American Medical Association
Physicians dedicated to the health of America

HIPAA

POLICIES & PROCEDURES DESK REFERENCE

MICHAEL W. HUBBARD, JD
KAREN E. GLOVER, JD
CAROLYN P. HARTLEY, MLA

HIPAA Policies and Procedures Desk Reference

Printed in the United States of America.

Internet address: www.ama-assn.org

Additional copies of this book may be ordered by calling 800 621-8335. Mention product number OP319602.

ISBN 1-57947-362-8

Library of Congress Cataloging-in-Publication Data

Hubbard, Michael W.
HIPAA policies and procedures desk reference / Michael W. Hubbard, Karen E. Glover, Carolyn P. Hartley.
p. cm.
ISBN 1-57947-362-8
1. Insurance, Health—Law and legislation—United States. 2. United States. Health Insurance Portability and Accountability Act of 1996. I. Glover, Karen E. II. Hartley, Carolyn P. III. Title.

KF1183.H83 2003
344.73’022—dc21

2003040325

BP02:02-P-062:02/03

For holding us up when our wings were worn out, we dedicate this book to Carrie, Kathryn, Taylor, Thad, Samantha, Evan, Chris, Kristen, and Laurie.

Preface

Physicians have long believed that privacy was a closely held tradition between patients and physician. Doors closed. Patients were free to talk and seek relief.

But then along came electronic files, e-mail messages with attached documents, managed care, 400-plus software programs to process billing and payments, repricing companies, quality assessments, peer reviews, electronic transcription services, and all of the other stuff that was supposed to make our jobs easier.

Everyone with a handheld device or Web site had a great idea about how to reduce information headaches while holding down the high cost of health care. But no one exactly explained how costs continued to rise while time with patients declined. Physicians tried to maintain that doctor-patient level of care and privacy, but electronic clutter ruled. It just wouldn't stop banging on the door, always demanding to see the doctor.

In the meantime, watchdog privacy groups didn't miss a beat on an emerging theme. Their polls told a concerning story. One in five Americans believed that a health care provider, insurance plan, government agency, or employer has improperly disclosed personal health information. Half of these people believed that it resulted in personal embarrassment or harm.[1] One in seven Americans has done something to keep personal medical information confidential, such as provide inaccurate information or "doctor-hop" to avoid a consolidated medical record or avoid care altogether.[2]

New privacy protections have come in the form of detailed federal rules under the Health Insurance Portability and Accountability Act of 1996 (HIPAA). The "portability" portion of that law helps a person maintain insurance when moving from one employer to the next. That portion of the law has already been implemented. When it comes to the privacy portion though, it's going to take a significant effort from everyone in health care to achieve compliance.

Congress called it "Administrative Simplification." It's anything but simple. The Privacy Rule, a component of HIPAA, sets specific guidelines for how the health care system will stabilize privacy issues. On August 14, 2002, final revisions to the Privacy Rule were published. Folded into that Rule is a mandate that covered entities (including many health care providers) establish policies and procedures to serve as a roadmap for how employees are to act and respond to privacy issues. Medical practices covered by HIPAA must put those policies and procedures in place by the April 2003 HIPAA privacy deadline.

More than a compliance standard, the policies and procedures need to drive behavior change. Physicians must adopt their own policies and procedures. The next step is to train everyone in the office so that everyone is clear about expectations.

In a recent informal poll among 13 hospital entities, 9 of 13 respondents said they believed the biggest challenge to complying with new privacy standards is changing

1. Survey conducted by Princeton Survey Research Associates, January 1999, for California HealthCare Foundation.
2. Ibid.

employee behavior. The group concluded that privacy and security training was more about change and culture management than it was about understanding HIPAA.[3]

With change and culture management on one side of our brain, and privacy regulations on the other, we brought together a team of legal, educational, and communication thinkers to develop the *HIPAA Policies and Procedures Desk Reference.*

ABOUT THIS BOOK

Chapter 1: How to Use This Book

If you are relatively new to HIPAA, this chapter is a must. Chapter 1 outlines how to approach this book based on what you do. In Chapter 1, you'll also find a Quick Reference Guide that points to the specific tasks to follow for many of the most common questions. For example, if you seek information on sending appointment reminders in compliance with to HIPAA, you would find a section that looks like this:

Appointment Reminder	Permission: Treatment or Operations	1.3
	Verify identity and authority of person requesting PHI	1.12
	Safeguards (it is okay to leave message on answering machine)	3.10 (AP9)
	Notice of Privacy Practices must mention appointment reminders	1.18

Chapter 2: Phase I Policies and Procedures

Chapter 2 presents a lighter version of HIPAA policies and procedures. If you are just starting to implement your policies and procedures, this chapter will help you get well on your way to showing a good faith compliance effort.

Chapter 3: Phase II Policies and Procedures

As you move deeper into HIPAA, you'll need the in-depth, comprehensive support presented in Chapter 3. The policies and procedures in Chapter 3 correlate with those in Chapter 2, but in this chapter, you'll find a more detailed approach.

Chapter 4: Workforce Training Tips

This chapter provides pointers about conducting training and how your Practice can use this book itself as a training tool.

Forms

To make your job easier, we've designed over 50 forms, from Authorization to Workforce Log. Each form is contained in its own Microsoft Word document on the CD-ROM at the end of this book for you to open and customize for your practice. Through a copyright provision included in this book, you have permission to use these forms to develop for your practice's use only. You may keep a copy of each form in this Policies and

3. Poll conducted by North Carolina Health Information and Communications Privacy and Security Officer's Training subgroup, September 2002.

Procedures Desk Reference and otherwise use this book as proof of your practice's compliance measures.

Appendix A: Privacy Rule Summary

You'll want to read the Privacy Rule Summary located on the CD-ROM that accompanies this book in the Privacy Rule Summary folder. The Privacy Rule Summary contains details from the final Privacy Rule and also from recent guidances and comments issued by the U.S. Department of Health and Human Services. For ready reference, you may also print this document and place it behind the tab for the Privacy Rule Summary, at the end of this book.

Appendices B and C

When you need to refer to the specific Privacy Rule provision on which each policy is based, turn to Appendix B to find a Crosswalk of Polices and Procedures to Privacy Rule Provisions. Appendix C gives you selected HIPAA definitions that have been reprinted from the final Privacy Rule. Make yourself familiar with these terms. Many of them will become part of your daily routine.

We acknowledge that as comprehensive as this Desk Reference might seem, it isn't complete. We've done extensive legal legwork to help you comply with federal regulations, but your state is likely to have stricter privacy laws. You also may find other federal laws that apply to your situation. Consult with an attorney to be certain state and other laws have been included in your policies and procedures customized for your needs.

Our highest vision is that we've given you a rock solid start to work from. Let us know how you're doing.

Mike Hubbard

Kari Glover

Carolyn Hartley

Overview of the Privacy Rule

HIPAA Privacy Rule

The Privacy Rule contains a number of standards that establish: (i) federally mandated policies regarding how health information can be used and disclosed, (ii) new individual rights, and (iii) new administrative requirements, including record-keeping requirements. The Privacy Rule contains a number of "implementation specifications," which provide further detail regarding how the various standards must be addressed. Most "covered entities" are required to comply with the Privacy Rule by April 14, 2003. However, "small health plans" (those having annual receipts of $5 million or less) have to comply by April 14, 2004.

Key Terms To Know

At its most basic level, the Privacy Rule regulates the use and disclosure of "protected health information" by "covered entities." These key terms are defined as follows:

- **Protected Health Information (PHI)**: Generally defined in the Privacy Rule as individually identifiable health information that is maintained or transmitted by a "covered entity" in any form or medium. Information is considered to be "individually identifiable" if (i) it identifies the individual or (ii) there is a reasonable basis to believe that the information can be used to identify the individual. In addition to clinical information, individually identifiable health information may include demographic characteristics, such as name, address, and age, or payment and billing details such as procedure code and diagnosis.
- **Covered Entity**: Generally defined to include: (i) health plans, (ii) health care clearinghouses, and (iii) health care providers who conduct electronic transactions for which HIPAA standard transactions have been adopted. If a medical practice conducts electronically any HIPAA transactions, it is a "covered entity" under the Privacy Rule.

The three categories of covered entities are described below.

- **Providers**: "Health care providers" include providers of medical or health services, or any person or organization who furnishes, bills, or is paid for health care in the normal course of business. Providers include, among many others, physicians, hospitals, pharmacies, nursing homes, durable medical equipment suppliers, dentists, optometrists, and chiropractors, if they conduct HIPAA standard transactions electronically. A health care provider is a covered entity under the HIPAA Privacy Rule only if it electronically conducts any transactions covered under the HIPAA "Transactions Rule." A provider is also a covered entity if someone else conducts such transactions for the provider. Examples could include a billing service company, a hospital billing department, or billing another medical practice that is doing the billing for a part-time physician who is sharing office space.
- **Plans**: "Health Plan" includes an individual or group plan that provided or pays for the cost of medical care. This includes health insurance companies, HMOs, and many employer-sponsored group health plans. Many medical practices sponsor group health plans. These medical practices also need to consider HIPAA privacy from the perspective of sponsors and fiduciaries of employee group health plans.

- **Clearinghouses**: "Health care clearinghouses" are companies that "translate" or facilitate translation of electronic transactions between the "standard" formats and code sets required under HIPAA and non-standard formats and code sets. Clearinghouses can include companies providing traditional electronic data interchange (EDI) services as well as billing/repricing services involving facilitation of the translation between standard and non-standard formats. Many billing companies have contractual relationships with clearinghouses.

Other Key Privacy Rule Concepts

- **New patient rights**: The Privacy Rule establishes new patient rights with respect to PHI, including patient rights of access to and amendment of records, and obtaining an accounting of certain disclosures of health information about them.
- **New administrative requirements**: Covered entities must adopt, implement, and enforce a number of written policies and procedures to ensure compliance with these requirements. The Practice must appoint a "Privacy Official" or privacy contact who is responsible for (i) developing written policies and procedures and systems, (ii) training the Practice's physicians and staff, and (iii) overseeing the required documentation relating to Privacy Rule compliance.
- **New restrictions on information flow**: The Privacy Rule imposes comprehensive regulatory restrictions on uses and disclosures of PHI. These are restrictions on how PHI can flow inside and outside a covered entity. The Privacy Rule prohibits any "use" and/or "disclosure" by a covered entity that does not fit under an applicable permission or requirement under the rule.
- **"Use" and "disclosure" are defined very broadly**: "Use" means what happens inside your Practice. "Use" includes looking at PHI. "Disclosure" means sharing PHI outside your Practice. In simplified terms, a Practice cannot look at or analyze PHI within its own office, or divulge or provide access to the information to any outsiders, except as the Privacy Rule permits or requires. In many cases, even where a type of use or disclosure falls within a particular permission under the Privacy Rule, the Privacy Rule imposes additional layers of requirements on how the use or disclosure may be accomplished.

More Restrictive State Laws

More restrictive state privacy laws can still apply. The Practice's legal counsel should assist in preparing modifications or additional policies and procedures to reflect applicable state laws and other laws.

For example, most states have laws that are more protective of privacy than HIPAA where the PHI involves mental health issues, HIV/AIDS or sexually transmitted disease status, or chemical dependency.

Penalties

A Practice's failure to comply with the Privacy Rule can result in civil and criminal penalties. The HIPAA statute provides that knowingly disclosing PHI to another person in violation of HIPAA triggers potential criminal penalties of up to a $50,000 fine and imprisonment for up to one year. If the offense is committed with the intent to sell, transfer, or use PHI for commercial advantage or personal gain, a person faces potential fines up to $250,000 and a sentence up to 10 years.

Current information handling practices that many covered entities view today as acceptable conduct could technically become criminal conduct when the HIPAA Privacy Rule compliance deadline arrives in April 2003. Although most medical practices take patient privacy very seriously, they are not accustomed to the level of compliance detail that the Privacy Rule imposes.

Acknowledgments

To the thinkers, planners, researchers, legal counselors, and friends who helped us write this comprehensive desk reference, we are deeply grateful to you. Our thanks go to the attorneys at Smith, Anderson Blount, Dorsett, Mitchell & Jernigan, L.L.P. and to the attorneys at Preston Gates Ellis L.L.P. for bringing their rich health care experiences and depth of knowledge to this project. From Smith Anderson, we thank Candice Murphy-Farmer, Dana Simpson, Bo Bobbitt, and Jane Langdell and from Preston Gates, we thank Tamara Watts, Anthony Miles, Mark Lamb, and a lively group of summer associates. For their technology and intellectual property advice, we thank Kevin Swan and Amber Beckman, and for employment advice, Lynn Du Bey, from Preston Gates Ellis L.L.P.

For exercising enormous diplomacy under word processing duress, we thank Gail Nolan from Preston Gates and Sheryl Roberts from Smith Anderson. They interpreted our handwriting, coordinated review copies, developed spreadsheets, and put in extra hours to help us get this book into your hands.

We humbly thank Holt Anderson, executive director of North Carolina Healthcare Information and Communications Alliance, Inc. (www.nchica.org), for being one of our strongest advocates and for offering us encouragement.

Thank you to Laura Lippman, MD, for her intelligent and thoughtful review and comments and for her friendship and support. Thank you to Margie Satinsky for her incisive comments and suggestions.

And last, we want to recognize the skill and patience handed to us from experienced editorial and marketing teams at AMA Press. Warmest thanks goes to Marsha Mildred, Katharine Dvorak, and Shelley Benson.

About the Authors

Michael W. Hubbard, JD

Mike Hubbard is a partner with Smith, Anderson, Blount, Dorsett, Mitchell and Jernigan, L.L.P., in Raleigh, North Carolina. He practices principally in the area of health and insurance law, including mergers and acquisitions, HIPAA compliance, and health informatics. He is co-author of the American Medical Association's *Field Guide to HIPAA Implementation*. He is a member of the Virginia State Bar, the North Carolina State Bar, the Section Council of the North Carollina Bar Association's Health Law Section, the Board of Directors of the North Carolina Society of Healthcare Attorneys, Inc, and he is Assistant Secretary of the North Carolina Healthcare Information and Communications Alliance, Inc. He received a B.S. degree in chemistry from Randolph-Macon College and a J.D. degree from the University of Virginia School of Law.

Karen (Kari) E. Glover, JD

Kari Glover is a senior partner in the law firm of Preston Gates Ellis, L.L.P., based in the Seattle office. She is leader of the Healthcare Practice Group at Preston Gates and practices principally in the area of health law, including health information and health technology, mergers and acquisitions, and executive compensation and benefits. Recently, Kari advised Microsoft in the development of a health information portal for its employees. Together with the Healthcare Practice Group, she advises a number of other technology and Internet health care entities with respect to compliance with regulatory requirements in the health care industry. In addition to other medical practice clients, she has acted as general counsel to the faculty practice plan at the University of Washington School of Medicine since 1984. In that capacity, she rendered advice on the development of the primary care network related to the University of Washington School of Medicine and clinical affiliations between the School of Medicine and Children's Hospital and Regional Medical Center, Fred Hutchinson Cancer Research Center, Seattle Cancer Care Alliance, and other entities with which the School of Medicine's faculty maintains clinical affiliations. Among her current activities, Kari is a member of the board of directors of a health care information systems company; was a luncheon speaker on bioinformatics at the American Health Lawyers Association conference on health care technology in December 2001 (see "Collisions at the Intersection: Law and Bioinformatics," 11 *BNA Health Law Reporter* 233. February 7, 2002); and is currently working with an American Bar Association Health Law Section task force concerning the impact on biotechnology development of the World Health Organization's position on the international human right to health. Kari graduated magna cum laude from Whitman College and received her J.D. degree, cum laude, from Harvard University. Kari serves on the Board of Trustees of Whitman College, currently chairing the board's Diversity Task Force.

Carolyn P. Hartley, MLA

Carolyn Hartley is Senior Vice-President of Development and Communications with Healthcare Training Strategies, L.L.C., and is also co-author of AMA's *Field Guide to HIPAA Implementation*, along with Mike Hubbard, Jan Root, PhD, and David C. Kibbe, MD, and of the *HIPAA Privacy Tool Kit*. Carolyn brings 25 years experience as a seasoned health care journalist, managing editor, and strategic marketing communications and crisis communications manager to this project. She also has co-authored and produced 26 nationally distributed books and video training courses, 11 of which are in health care and health information management. Carolyn has held significant appointments as Executive Producer, Healthcare Business Review; Vice-President, Center for Advanced Media Studies; Media and Publications Director, Mayer Hoffman McCann's Professional Resources Division; and Vice-President with Fleishman Hillard where she served as an advisor on new product-to-market programs for pharmaceutical and health information management clients. Her clients have appeared in proactive and confrontational situations on morning news shows and in hundreds of consumer and trade publications including *The Wall Street Journal, New York Times, Forbes, Bloomberg Radio, AP, USA Today, Universal Press Syndicate, Associated Press,* Dateline, 60 Minutes, 20/20, The Early Show, and Good Morning America. She holds an undergraduate degree in education and a Master of Liberal Arts degree from Baker University where she also has been an adjunct professor in the MBA and MLA programs.

Contents

Preface v
Overview of the Privacy Rule ix
Acknowledgments xi
About the Authors xiii

Chapter 1: How to Use This Book

Section 1.1 The Way You Use This Book Depends on What You Do 1
Section 1.2 Reference Tool for Everyone 2
How to Confirm Privacy Compliance of a PHI Use or Disclosure 3
Quick Reference Guide 4
What to Do When… 6
Verification Procedure Guide 13
Process for Determining Personal Representative Status with Respect to Adults and Emancipated Minors 16
Process for Determining Personal Representative Status with Respect to Deceased Individuals 17
Process for Determining Personal Representative Status with Respect to Unemancipated Minors 18
Process for Determining Whether Practice May or Must Disclose to a Parent or Provide Access to a Parent Under Express State Law 19
Process for Determining Whether Practice May Disclose to a Parent or Provide Access to a Parent Where State Law is Silent 20
Examples of Common Safeguards 21
Index of Phase I Policies and Procedures 22
Index of Forms 24
Section 1.3: Reference Tool for Practice Owners and Managers 27
Section 1.4: Reference Tool for Privacy Official 29
How to Develop and Implement Privacy Policies and Procedures 30
How to Develop and Implement Safeguards Policies and Procedures 31

Chapter 2: Phase I Policies and Procedures

Overview 33
Index of Phase I Policies and Procedures 34
PHI: Permissions 35
Introduction 35
Required Disclosures 35
Disclosures to the Patient 35

Our Treatment, Payment, Operations 35
Others' Treatment, Payment, Operations 36
Operations of Organized Health Care Arrangement 36
Family, Friends, and Disaster Relief Organizations 36
Incidental Disclosures 37
Public Purpose 37
Authorization 37
De-Identification 38
Limited Data Set 38
PHI: Special Requirements 39
Introduction 39
Verification 39
Minimum Necessary 39
Business Associates 39
Personal Representatives 40
Marketing 41
Psychotherapy Notes 41
Consistent with Notice of Privacy Practices 42
Consistent with Other Documents 42
Consent (State or Other Law) 42
Patient Rights 43
Introduction 43
General Policy 43
Access 43
Amendment 43
Accounting 44
Alternative Communications 45
Further Restrictions 45
Complaints 45
Privacy Management 47
Introduction 47
General Policy 47
Privacy Official/Privacy Contact 47
Notice of Privacy Practices—Development and Distribution 47
Policies and Procedures 48
Documentation 48
Workforce Training 48
Internal Sanctions 49
Mitigation 49
No Retaliation 49
No Waiver 49
Safeguards 50

Chapter 3: Phase II Policies and Procedures

How to Use This Chapter 51
Index of Phase II Policies and Procedures 52

PHI Use and Disclosure 53
PHI Use and Disclosure (PP1.0) 53
PHI Permissions Process Chart 56
Permissions 57
Required Disclosures (PP1.1) 57
Disclosures to the Patient (PP1.2) 59
Our Treatment, Payment, Operations (PP1.3) 61
Others' Treatment, Payment, Operations (PP1.4) 69
Operations of Organized Health Care Arrangement (PP1.5) 77
F1.5: Organized Health Care Arrangements 81
Family, Friends, and Disaster Relief Organizations (PP1.6) 83
Incidental Disclosures (PP1.7) 87
Uses and Disclosures for a Public Purpose (PP1.8) 89
F1.8A: State Law Required Disclosures 103
F1.8B-4: Sate Law Notification of Requirements: Spread of Disease 104
F1.8C: State Law Notification Requirements: Victims of Abuse 105
F1.8D: State Law Notification Requirements: Health Oversight Activities 106
F1.8O: State Law Workers' Compensation Laws 107
Authorization (PP1.9) 109
F1.9: Authorization for Use or Disclosure of Health Information 118
De-Identification (PP1.10) 121
F1.10: De-Identification "Safe Harbor" Checklist 122
Limited Data Set (PP1.11) 123
Special Requirements 125
Verification (PP1.12) 125
Minimum Necessary (PP1.13) 137
F1.13A: Minimum Necessary Workforce Form 146
F1.13B: Minimum Necessary Worksheet—Routine PHI Uses 147
F1.13C: Minimum Necessary Worksheet—Routine PHI Disclosures 148
F1.13D: Minimum Necessary Worksheet—Routine PHI Requests 149
Business Associates (PP1.14) 151
F1.14A: Medical Practice HIPAA Business Associate Amendment Terms and Conditions 153
F1.14B: Business Associate Amendment Log 158
F1.14C: Business Associate Amendment Termination Form 159
Personal Representatives (PP1.15) 161
F1.15A: State Laws Governing Personal Representatives 167
F1.15B: Process for Determining Personal Representative Status with Respect to Adults and Emancipated Minors 168
F1.15C: Process for Determining Personal Representative Status with Respect to Deceased Individuals 169
F1.15D: Process for Determining Personal Representative Status with Respect to Unemancipated Minors 170
F1.15E: Process for Determining Whether Practice May or Must Disclose to a Parent or Provide Access to a Parent Under Express State Law 171
F1.15F: Process for Determining Whether Practice May Disclose to a Parent or Provide Access to a Parent Where State Law is Silent 172
Marketing (PP1.16) 173
Psychotherapy Notes (PP1.17) 177

Consistent with Notice of Privacy Practices (PP1.18) 181
Consistent with Other Documents (PP1.19) 183
Consent (State or Other Law) (PP1.20) 185
F1.20A: State Law Consent Requirements 186
F1.20B: Federal Law Consent Requirements 187
Patient Rights 189
Patient Rights (PP2.0) 189
Access (PP2.1) 191
F2.1A: Designated Record Set Log 201
F2.1B: Request for Access to Records 203
F2.1C: Access Request Log 204
F2.1D: Response to Request for Access to Records 205
F2.1E: Access Denial Review Log 207
F2.1F: Access Request Review: Decision of Reviewing Official 208
Amendment (PP2.2) 209
F2.2A: Request to Amend Records 218
F2.2B: Amendment Request Log 219
F2.2C: Accepted Amendment Form 220
F2.2D: Response to Request to Amend Records 221
F2.2E: Amendment Notification Confirmation 224
Accounting (PP2.3) 225
F2.3A: Practice Protected Health Information Disclosure Log 237
F2.3B: Business Associate Protected Health Information Disclosure Log 238
F2.3C: Research Disclosure Log 239
F2.3D: Request for Disclosure Accounting 240
F2.3E: Accounting Request Log 241
F2.3F: Response to Request for Disclosure Accounting 242
F2.3G: Summary Information Accounting 244
F2.3H: Research Disclosure Accounting 245
Alternative Communications (PP2.4) 247
F2.4A: Request for Alternative Communications 253
F2.4B: Alternative Communications Request Log 254
F2.4C: Response to Request for Alternative Communications 255
Further Restrictions (PP2.5) 257
F2.5A: Request to Restrict Uses and Disclosures of Protected Health Information 265
F2.5B: Further Restriction Request Log 266
F2.5C: Response to Request to Restrict Uses and Disclosures of Protected Health Information 267
F2.5D: Termination of Agreed Restriction on Uses and Disclosures of Protected Health Information 268
F2.5E: Letter Terminating Agreed Restriction without Consent 269
Complaints (PP2.6) 271
F2.6A: Privacy Complaint 274
Privacy Management 275
General Policy (PP3.0) 275
Privacy Official/Privacy Contact (PP3.1) 277
F3.1A: Privacy Official Job Description 278

Notice of Privacy Practices—Development and Distribution (PP3.2) 279
F3.2A: Notice of Privacy Practices 286
F3.2B: Notice of Privacy Practices Receipt 292
F3.2C: Notice of Privacy Practices Provision Log 293
Policies and Procedures (PP3.3) 295
F3.3A: Checklist of Phase II Policies and Procedures 296
F3.3B: Policy/Procedure Modification Form 298
Documentation (PP3.4) 299
Workforce Training (PP3.5) 301
F3.5A: Workforce Log 303
F3.5B: Workforce Exclusions Log 304
F3.5C: Personal HIPAA Training Profile 305
F3.5D: Training Session Documentation Form 306
F3.5E: Confidentiality Agreement 307
Internal Sanctions (PP3.6) 309
Mitigation (PP3.7) 319
No Retaliation (PP3.8) 325
No Waiver of Rights (PP3.9) 327
Safeguards (PP3.10) 329
F3.10A: Safeguards Development and Documentation 337
F3:10B: Sample Questionnaire for Safeguards Vendors 377
Safeguards Glossary 379

Chapter 4: Workforce Training Tips

Training Tips 383

Appendix A: Privacy Rule Summary (On the CD-ROM)

How to Use This Privacy Rule Summary 389
Lesson 1: Origin and Purpose of the HIPAA Privacy Rule 391
Lesson 2: Notice of Privacy Practices (§164.502(i), §164.520) 397
Lesson 3: Patient Rights 405
Lesson 4: New Administrative Requirements (§164.530) 413
Lesson 5: Overview of New Restrictions on the Flow of PHI 418
Lesson 6: Permitted Uses and Disclosures: To the Patient; Treatment, Payment, and Health Care Operations; Family and Friends, Disaster Relief, and Facility Directories; Incidental Disclosures; and Authorizations 424
Lesson 7: Public-Good Uses and Disclosures (§164.512) 433
Lesson 8: Minimum Necessary (§164.502(b); §164.514(d)) 442
Lesson 9: Business Associates (§164.502(e); §164.504(e)) 446
Lesson 10: Other Special Requirements 451
Lesson 11: Other Laws, Preemption, and Enforcement 462
Lesson 12: Privacy Implementation 465

Appendix B: Crosswalk of Policies and Procedures to Privacy Rule Provisions 469

Appendix C: Glossary of Selected HIPAA Definitions 471

chapter 1

How to Use This Book

SECTION 1.1: THE WAY YOU USE THIS BOOK DEPENDS ON WHAT YOU DO

Introduction

Everyone has a role in privacy as defined in the Health Insurance Portability and Accountability Act of 1996 (HIPAA). We all must comply with the law. Each person within the Practice has particular responsibilities that involve patient information.

What you do should guide your reading of this book. To get started, follow the recommendations below based on your role in the Practice.

Later, keep reading about HIPAA. Read Appendix A, Privacy Rule Summary, to get a better appreciation for what HIPAA privacy is all about.

Everyone

Section 1.2 describes how everyone in the Practice should use this book. Each person in your workforce who handles patient information must follow the Practice's policies and procedures, including:

- Employed physicians
- Locum tenens physicians
- Clinical staff
- Business and administrative staff
- Trainees
- Volunteers
- Temporary employees

Section 1.2 also contains a Quick Reference Guide. The Quick Reference Guide helps you locate the policies and procedures that apply to a particular task or job function.

Practice Owners and Managers

Section 1.3 explains how Practice owners and managers should use this book.

Privacy Official

The Privacy Official plays a crucial role in a practice's successful HIPAA compliance program. Section 1.4 describes how the Privacy Official should use this book.

SECTION 1.2: REFERENCE TOOL FOR EVERYONE

Introduction

Your Practice's success in complying with the Privacy Rule depends on everyone in the Practice. Each person should take personal responsibility for assuring that his or her behavior and work meet the requirements of the Privacy Rule and the Practice's policies and procedures. One of the most critical aspects of compliance is having a thorough understanding of those requirements. Active participation in the Practice's privacy training and appropriate use of the Privacy Official as a resource will promote this understanding.

Learn Some Privacy Rule Basics

- Read Lesson 1 of Appendix A.
- Read through once the Phase I Policies and Procedures in Chapter 2. This will give you a good overview of what HIPAA privacy means to Practice operations. Chapter 2 contains shorter versions of policies and procedures. Chapter 3 contains more detailed versions of the same policies and procedures as well as from documents.
- Study carefully the policies and procedures assigned to you as identified on Form F3.5C, "Your Personal HIPAA Profile," which is to be completed by the Privacy Official (these may include Chapter 2 or Chapter 3 policies and procedures, as the Privacy Official deems appropriate).
- For additional background information, read the other lessons in Appendix A that relate to the policies and procedures assigned to you.

Actively Participate in Training

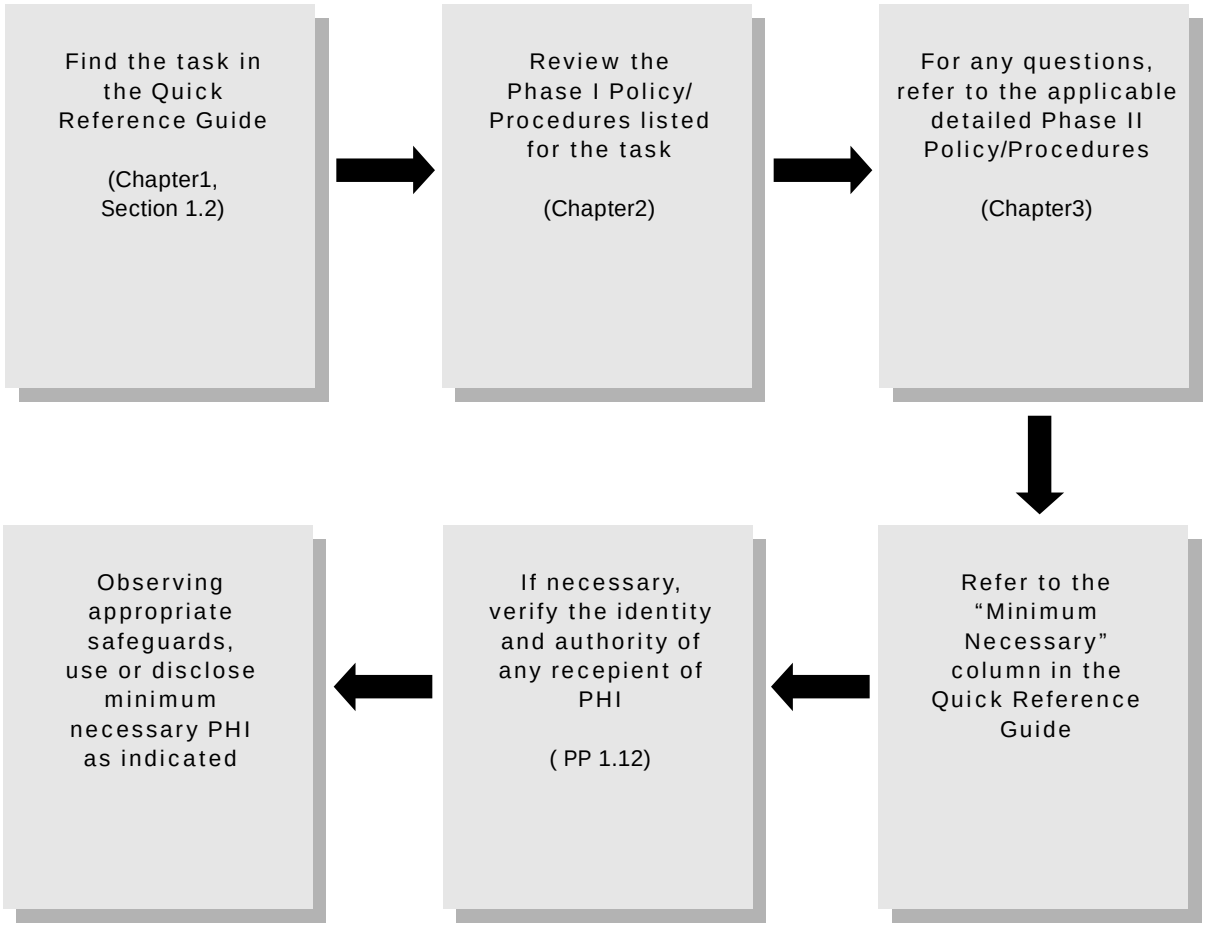
The Privacy Rule requires that the Practice's workforce be adequately trained on its privacy policies and procedures. Your participation in training is not only important to your understanding of the requirements—it is required.

Quick Reference Guide

The next pages contain a flow chart describing how to perform a task using or disclosing protected health information (PHI), an index of Phase I policies and procedures, and the "Quick Reference Guide." The Quick Reference Guide is your "road map" to policies and procedures. It helps you identify and locate policies and procedures that apply to a particular task or job function. It is not intended to reference all policies and procedures that may apply, just common ones. The Privacy Official will complete and then revise the Quick Reference Guide from time to time to fit the needs of your Practice and to improve compliance with the Privacy Rule.

How to Confirm Privacy Compliance of a PHI Use or Disclosure

If you are performing a task for our Practice that involves using or disclosing protected health information (PHI):



Name of Practice:

Address:

Privacy Official:

Telephone:

Last Updated: _____

QUICK REFERENCE GUIDE

Introduction

Use this Guide after you have reviewed some HIPAA basics. This Guide is designed to be the focus of your HIPAA training as you develop and implement your Practice's policies and procedures.

How to Use This Quick Reference Guide

Use the Quick Reference Guide to locate information about what privacy protection actions you need to take to do your job.

First, find the category of activity or description of the task or function you want to perform. If you have questions or do not find what you need, review our policies and procedures or contact our Privacy Official.

Second, review the things you need to do. As needed, read the listed policies and procedures to learn or to refresh your memory. This step includes making sure which "Permission" applies and satisfying the conditions of that Permission. It also includes complying with "Special Requirements."

The "P" numbers refer to the Phase I policies and procedures in Chapter 2 ("HIPAA Light" policies and procedures), and the "PP" numbers refer to Phase II policies and procedures in Chapter 3 ("HIPAA Heavy" policies and procedures). A Phase II "PP" policy and procedure provides more detail and contains forms for the same topic addressed by the Phase I "P" policy and procedure with the same number.

The "Minimum Necessary" Special Requirement is addressed in the "Minimum Necessary" column of the Quick Reference Guide "What to do when" chart. With the help of Practice professionals, the Privacy Official will follow the Minimum Necessary Policies and Procedures (PP1.13) to complete the Minimum Necessary column in the Quick Reference Guide for each listed task or function.

Note that to save space some Special Requirements are not listed repeatedly in the Quick Reference Guide because they are commonly applicable to many tasks or functions. Specifically, these include the following Special Requirements:

- Incidental Disclosures (P1.7);
- Verification (P1.12);
- Personal Representatives (P1.15);
- Consistent with Notice of Privacy Practices (P1.18);
- Consent (State or Other Laws) (P1.20);
- Safeguards (P3.10).

As a reminder of their importance, these Special Requirements are listed at the bottom of each page of the Quick Reference Guide. Always keep these Special Requirements in mind when you are making a PHI use or disclosure. For example, a basic safeguard is not to talk more loudly about patients than necessary if others can hear.

Third, ask the Privacy Official for clarification and assistance when you have questions about what you need to do to comply with the Practice's policies and procedures.

Quick Reference Guide Features

The Quick Reference Guide is organized as follows:

- "What to do when," which is a list of common tasks and functions involving PHI, with cross-referenced policies and procedures and "Minimum Necessary" guidance.
- List of permitted Incidental Disclosures.
- List of vendors with whom we have Business Associate Amendments.
- Verification Procedure Guide.
- Personal Representatives Flow Charts (how to determine when you can disclose to a parent, etc.).
- Safeguards examples, which are examples of commonly applicable (and common sense) protections for PHI.
- Index of Phase I Policies and Procedures.
- Index of forms.

Keep in mind that the Privacy Official will regularly revise and update the Quick Reference Guide, so make sure you review the most up-to-date version.

QUICK REFERENCE GUIDE

What to do when...

Task/Function	Permissions and Requirements for PHI Use or Disclosure or Request*	P/PP No.	Minimum Necessary** (PP1.13)
Pre-visit			
Initial Scheduling: Call from Referring Provider, Call from Patient	Permission: Treatment, Operations	1.3	Note: Minimum Necessary is not applicable (N/A) for disclosures to or requests by a health care provider for treatment purposes or disclosures to the patient
Eligibility Verification: Medical Necessity, Health Plan Coverage, Appropriateness of Care, Pre-Approval of Charges	Permission: Payment	1.3	
	Verify identity and authority of person requesting PHI	1.12	
Appointment Reminder	Permission: Treatment or Operations	1.3	
	Verify identity and authority of person requesting PHI	1.12	
	Safeguards (it is okay to leave message on answering machine)	3.10 (AP9)	
	Notice of Privacy Practices must mention appointment reminders	1.18	
Visit			
Pull Medical Record	Permission: Treatment	1.3	
Set Up Patient Accounts	Permission: Treatment, Payment, Operations	1.3	
Arrival and Check-In ■ New patient form	Permission: Disclosures to Patient	1.2	
	Permission: Our Treatment, Payment, Operations	1.3	
	Provide NPP on first visit after 4/13/03 and ask for signed receipt	3.2	
	Keep Notice of Privacy Practices receipt for file. Confirm in Log (#F3.2C)	3.4	

* This list is a beginning list of alternative Permissions and some relevant policies and procedures. The list is to be revised and maintained by the Privacy Official to make it most relevant to our Practice (including listing particular facts that trigger a particular alternative Permission). It is not intended to be exhaustive nor does it refer in all cases to certain broadly applicable policies and procedures (P/PP): Incidental Disclosures (1.7), Verification (1.12), Personal Representatives (1.15), Consistent with Notices of Privacy Practices (1.18), Consent (State or Other Law) (1.20), and Safeguards (3.10). Because these requirements are applicable to so many situations, you need to make it "second nature" to consider these requirements in just about all situations. Other guidance is included in the Quick Reference Guide to help you analyze the application of some of these policies and procedures—examples of permitted Incidental Disclosures, a list of OHCA participants, and a list of Business Associates are included at the end of the Quick Reference Guide chart of tasks ("What to do when…"), a Verification Procedures Guide follows the chart of tasks, and flow charts regarding Personal Representatives come next. Finally, examples of common Safeguards are also included.

** The Privacy Official will complete and maintain this column regarding the Minimum Necessary (PP1.13) requirements, with the help of professionals in the Practice. All of this Quick Reference Guide will be revised from time to time by the Privacy Official to make its contents most relevant to our Practice.

Task/Function	Permissions and Requirements for PHI Use or Disclosure or Request*	P/PP No.	Minimum Necessary** (PP1.13)
Call Patient to Exam Room	Permission: Treatment	1.3	Note: N/A for disclosures to or requests by a health care provider for treatment purposes or disclosures to the patient
	Permission: Family, Friends	1.6	
	Permission: Incidental Disclosures (OK to call name of patient if only necessary information is used)	1.7	
Patient in Exam Room	Permission: Treatment	1.3	Note: N/A for disclosures to or requests by a health care provider for treatment purposes or disclosures to the patient
	Permission: Disclosures to the Paitent	1.2	
	Permission: Family, Friends	1.6	
	Safeguards (OK to put chart in hallway if facing away from inadvertent observation or otherwise covered)	3.10	
Clinical Staff-Patient Interaction (physician, nurse, technicians, care coordinators)	Permission: Treatment	1.3	Note: N/A for disclosures to or requests by a health care provider for treatment purposes or disclosures to the patient
	Permission: Disclosures to the Paitent	1.2	
	Permission: Incidental Disclosures (OK to discuss PHI at nursing stations if low voices are used)	1.7	
	Safeguards (staff should take reasonable precautions not to be overhead discussing PHI)	3.10	
Check-Out	Permission: Our Treatment, Payment, Operations	1.3	
Post-visit			
Outside Lab and Other Tests	Permission: Treatment	1.3	Note: N/A for disclosures to or requests by a health care provider for treatment purposes or disclosures to the patient
	Permission: Others' Treatment, Payment, Operations	1.4	
Clinical Follow-Up Contacts With Patient	Permission: Required Disclosures	1.1	Note: N/A for disclosures to or requests by a health care provider for treatment purposes or disclosures to the patient
	Permission: Disclosures to Patient	1.2	
	Permission: Treatment	1.3	
	Permission: Incidental Disclosures (OK to leave message on answering machine if only necessary information is used)	1.7	
	Possible: Alternative Communications	2.4	
Clinical Follow-Up Contacts With Other Providers	Permission: Treatment	1.3	Note: N/A for disclosures to or requests by a health care provider for treatment purposes
	Permission: Others' Treatment, Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangement	1.5	
Billing and Collection	Permission: Payment, Operations	1.3	
	Permission: Others' Treatment, Payment, Operations	1.4	
	Other Permission: Operations of Organized Health Care Arrangement	1.5	

Task/Function	Permissions and Requirements for PHI Use or Disclosure or Request*	P/PP No.	Minimum Necessary** (PP1.13)
Special Disclosures Requested by Patient (life insurance; disclosure to employer for ADA, FMLA, etc; school physical)	Permission: Authorization	1.9	Note: N/A for uses or disclosures pursuant to a valid valid patient Authorization
Referrals			
Care Coordination/ Referral Coordination	Permission: Treatment, Operations	1.3	Note: N/A for disclosures to or uses by a health care provider for treatment purposes
	Permission: Others' Treatment, Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangment	1.5	
Referrals from Other Providers	Permission: Treatment, Payment, Operations	1.3	Note: N/A for disclosures to or uses by a health care provider for treatment purposes
	Permission: Others' Treatment, Payment, Operations	1.4	
Referrals to Other Providers	Permission: Treatment, Operations	1.3	Note: N/A for disclosures to or uses by a health care provider for treatment purposes
	Permission: Others' Treatment, Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangment	1.5	
Receiving Requests for Medical Records	Permission: Required Disclosures	1.1	Note: N/A for disclosures to or uses by a health care provider for treatment purposes, disclosures to the patient, or disclosures pursuant to a valid patient Authorization. Absent documented justification, delivering entire medical record can be a presumptive violation of the Privacy Rule.
	Permission: Disclosures to the Patient	1.2	
	Permission: Our Treatment, Payment, Operations	1.3	
	Permission: Others' Treatment, Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangement	1.5	
	Permission: Uses and Disclosures for Public Purpose	1.8	
	Permission: Authorization	1.9	
	Permission: De-Identification	1.10	
	Permission: Limited Data Set	1.11	
	Special Requirements: Verification	1.12	
	Special Requirements: Marketing	1.16	
	Special Requirements: Psychotherapy Notes	1.17	

Task/Function	Permissions and Requirements for PHI Use or Disclosure or Request*	P/PP No.	Minimum Necessary** (PP1.13)
Requesting Medical Records From Others	Permission: Treatment, Payment, Operations	1.3	Note: N/A for disclosures to or uses by a health care provider for treatment purposes or disclosures pursuant to a valid Authorization. Requesting entire medical record can be a presumptive violation of the Privacy Rule.
	Permission: Others' Treatment, Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangement	1.5	
	Permission: Authorization	1.9	
	Special Requirement: Marketing	1.16	
	Special Requirement: Psychotherapy Notes	1.17	
Referral/Service Authorizations	Permission: Treatment, Payment, Operations	1.3	Note: N/A for disclosures to or uses by a health care provider for treatment purposes or disclosures pursuant to a valid Authorization.
	Permission: Others' Treatment, Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangement	1.5	
	Permission: Authorizations	1.9	
Claim Submission	Permission: Payment, Operations	1.3	
	Permission: Others' Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangement	1.5	
	Permission: Authorization	1.9	
Claim Processing			
Claim Attchments	Permission: Payment, Operations	1.3	
	Permission: Others' Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangement	1.5	
	Permission: Authorization	1.9	
Claim Status Check	Permission: Payment, Operations	1.3	
	Permission: Others' Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangement	1.5	
	Permission: Authorization	1.9	
Remittance Advice and Payment Receipt	Permission: Payment, Operations	1.3	
	Permission: Others' Payment, Operations	1.4	
	Permission: Operations of Organized Health Care Arrangement	1.5	
	Permission: Authorization	1.9	

Task/Function	Permissions and Requirements for PHI Use or Disclosure or Request*	P/PP No.	Minimum Necessary** (PP1.13)
Practice Administration			
Business and Strategic Planning	Permission: Payment, Operations	1.3	
	Permission: Business Associates	1.14	
	Policies and Procedures	3.3	
	Workforce Training	3.5	
Legal	Permission: Payment, Operations	1.3	
	Permission: Operations of Organized Health Care Arrangement	1.5	
	Permission: Public Purpose	1.8	
	Special Requirements: Business Associates	1.14	
	Patient Rights: Complaints	2.6	
	Internal Sanctions	3.6	
	Mitigation	3.7	
HIPAA Privacy Rule Compliance	Permission: Operations	1.3	
Accounting/Bookkeeping	Permission: Payment, Operations	1.3	
	Permission: Operations of Organized Health Care Arrangement	1.5	
	Special Requirements: Business Associates	1.14	
Licensing/Regulation	Permission: Payment, Operations	1.3	
	Permission: Public Purpose	1.8	
Marketing	Special Requirements	1.16	Note: N/A for disclosures subject to a valid patient Authorization
	Permission: Authorization	1.9	
Vendor/Supplier Relationshipss	Permission: Treatment, Payment, Operations	1.3	Note: N/A for disclosures to or requests by a health care provider for treatment purposes or pursuant to a valid patient Authorization. Sharing of Minimum Necessary PHI with vendors or suppliers is a particularly sensitive area and deserves careful monitoring.
	Permission: Others' Treatment, Payment, Operations	1.4	
	Permission: Authorization	1.9	
	Permission: De-Identification	1.10	
	Permission: Limited Data Set	1.11	
	Special Requirements: Business Associates	1.14	
	Special Requirements: Marketing	1.16	
	Special Requirements: Psychotherapy Notes	1.17	
	Special Requirements: Consent	1.20	
	Possible: Patients: Further Restrictions	2.5	
	Workforce Training	3.5	
	Safeguards	3.10	

Task/Function	Permissions and Requirements for PHI Use or Disclosure or Request*	P/PP No.	Minimum Necessary** (PP1.13)
Exercise of Patient HIPAA Rights			
Requests for Access	Access	2.1	
	Permission: Our Operations (compliance with Privacy Rule)	1.3	
	Permission: Disclosures to Patient	1.2	
	Verification	1.12	
Requests for Amendment	Amendment	2.2	
	Permission: Our Operations	1.3	
	Permission: Disclosures to Patient	1.2	
	Verification	1.12	
Requests for Alternative Communications	Alternative Communications	2.4	
	Permission: Our Operations	1.3	
	Permission: Disclosures to Patient	1.2	
	Verification	1.12	
Requests for Disclosure Accounting	Accounting	2.3	
	Permission: Our Operations	1.3	
	Permission: Disclosures to Patient	1.2	
	Verification	1.12	
Further Restriction Request	Further Restrictions	2.5	
	Permission: Our Operations	1.3	
	Permission: Disclosures to Patient	1.2	
Complaints	Complaints	2.6	
	Privacy Official/Privacy Contact	3.1	
	Documentation	3.4	
	Permission: Our Operations	1.3	
	Permission: Disclosures to Patient	1.2	
	Internal Sanctions	3.6	
	Mitigation	3.7	
	No Retaliation	3.8	
Public Purpose			
Workers' Compensation Disclosures Regarding Patient Condition	Permission: Public Purpose (Workers' Compensation)	1.8	
	Log disclosures for disclosure accounting purposes	2.3	

Task/Function	Permissions and Requirements for PHI Use or Disclosure or Request*	P/PP No.	Minimum Necessary** (PP1.13)
Other			
Response to Emergency Requests	Permission: Disclosures to Patients	1.2	
	Permission: Treatment, Payment, Operations	1.3	
	Permission: Others' Treatment, Payment, Operations	1.4	
	Permission: Family, Friends and Disaster Relief Organizations	1.6	
	Public Purpose	1.8	
Response to Requests from Government	Family, Friends and Disaster Relief Organizations	1.6	
	Public Purpose	1.8	
	Verify the identity and authority of the requestor	1.12	

Examples of Permitted Incidental Disclosures (PP1.7)

1. Health care services may be coordinated orally by staff at nursing stations—if appropriately low voices are used.
2. Nurses or other staff may discuss the patient's condition by telephone, or may discuss treatment of the patient with another provider by telephone, if such discussions on the telephone are conducted in low voices and away from other potential listeners, if possible.
3. Lab results may be discussed with patients or other professionals in a joint treatment area if reasonable precautions are taken.
4. Messages containing information for patients may be left on answering machines or with family members if the information is reasonably limited to the amount necessary for the purpose.
5. Sign-in sheets may be used, and patient names called, in waiting rooms—if only the information needed for the purpose is used.
6. A public address system may be used to announce (a) patient names and limited information or (b) a request for the patient to contact a specific individual or location for more information.
7. X-ray light boards may be used at nursing stations that are not publicly accessible.
8. Patient charts may be placed outside exam rooms if reasonable precautions are taken, such as facing charts to the wall or providing a cover that conceals the chart when it is in place.

Organized Health Care Arrangements (PP1.5)

[Privacy Official to include a summary of F1.5 for quick reference]

List of Business Associates (PP1.14)

1. Transcription Company: _____
2. Practice Management System Vendor: _____
3. [Other] _____

QUICK REFERENCE GUIDE

Verification Procedure Guide (PP1.12)

Note: If the identity and the authority of the person requesting PHI are not already known.

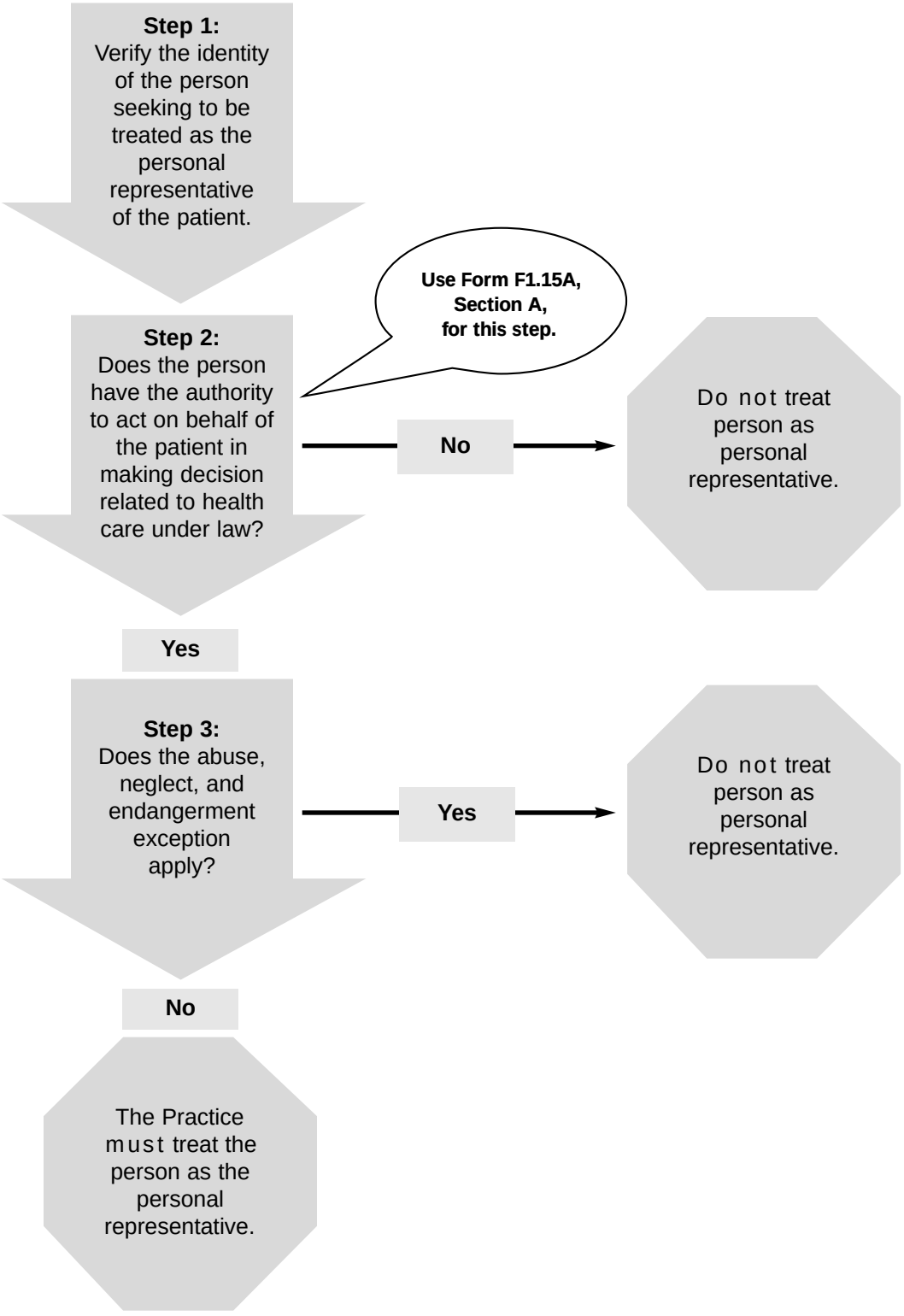
Step	If the person requesting PHI is…	Then…
A	**Claiming to be the patient and in person**	■ Require a driver's license, a passport, a state identification, or similar evidence of identity. ■ Request his/her social security number or other personal information that can be verified from his/her medical record. ■ The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith.
B	**Claiming to be the patient, but not in person**	■ Request his/her social security number or other personal information that can be verified from his/her medical record. ■ Send the PHI to a recognizable organizational mailing address. ■ Call the requestor back through the main organization switchboard rather than through a direct dial number to verify the instructions if the PHI is to be transmitted by fax or telephone or e-mail. ■ Use some other appropriate common-sense means of verifying that the person making the request is in fact the patient. ■ The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith.
C	**Not the patient, but in person with the patient**	■ Generally, if the patient is known to us or his or her identity is verified, and if the patient is with the person and identifies the person as someone entitled to receive the patient's PHI, that is sufficient Verification of the person's identity and authority. ■ If the patient is known to our Practice, that is sufficient Verification of the patient. If the patient is not known or recognized, verify the patient's identity under B above.
D	**Not the patient, but in person without the patient**	Use reasonable means to verify the person's *identity:* ■ Require a driver's license, a passport, a state identification, or similar evidence of identity. ■ The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith. Use reasonable means to verify the person's *authority.* ■ Require a copy of a power of attorney, a letter on official letterhead, a subpoena, or similar official document to evidence authority. ■ If the Permission (PP1.1 through PP1.11) you have identified for the use or disclosure of PHI requires particular documentation, statements, or representations by the person requesting PHI, request the required items and determine whether the evidence offered is sufficient. ■ In making this determination, our Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements—if our reliance is reasonable under the circumstances and is in good faith.

		■ For certain disclosures required by law, the condition of the Permission can be met by administrative subpoena or similar process or by a separate written statement that, on its face, shows the requirements have been met. Note: No Verification of identity or authority is required if the person requesting PHI is permitted to receive the PHI because he or she is a family member or someone involved in the patient's care or is picking up prescription medications or otherwise permitted to receive the PHI under Family, Friends, and Disaster Relief Organizations, PP1.6.
E	**Not the patient and not in person**	Use reasonable means to verify the person's identity by: ■ Sending the PHI to a recognizable organizational mailing address, or ■ Calling the requestor back through the main organization switchboard rather than through a direct dial number to verify the instructions, if the PHI is to be transmitted by fax or telephone or e-mail, or ■ Using some other appropriate common-sense means of verifying that the person making the request is in fact the person authorized to receive the patient's PHI. Use reasonable means to verify the person's *authority.* Require a copy of a power of attorney, a letter on official letterhead, a subpoena, or similar official document to evidence authority. ■ If the Permission (PP1.1 through PP1.11) you have identified for the use or disclosure of PHI requires particular documentation, statements, or representations by the person requesting PHI, request the required items and determine whether the evidence offered is sufficient. ■ In making this determination, our Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements—if our reliance is reasonable under the circumstances and is in good faith. ■ For certain disclosures required by law, the condition of the Permission can be met by administrative subpoena or similar process or by a separate written statement that, on its face, shows the requirements have been met.
F	**Claiming to be patient's personal representative**	Use reasonable means to verify the person's *identity* and *authority* to act for the patient as follows: ■ Examine a copy of the personal representative's court appointment as executor of a deceased patient's estate, or other reasonable evidence of the personal representative's authority. ■ Examine a copy of the power of attorney for a personal representative of an adult patient or a copy of the court appointment if the personal representative has been appointed by the court, or other reasonable evidence of the personal representative's authority to act for the patient. ■ Ask questions to determine that an adult acting for a young child has the requisite relationship to the child to support his or her status as personal representative to the child. Note: Where disclosure depends on personal representative status, this step applies in addition to any of the other steps described in this chart.

G	**Claiming to be a public official or acting on behalf of a public official**	If it is reasonable under the circumstances to do so, our Practice may rely on the following to verify the *identity* of a public official or a person acting on behalf of a public official: ■ If the request is in person, presentation of an agency identification badge, other official credentials, or other proof of government status; ■ If the request is in writing, the request is on appropriate government letterhead; or ■ If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official. If it is reasonable under the circumstances to do so, our Practice may rely on the following to verify the *authority* of a public official or a person acting on behalf of a public official: ■ A written statement of the legal authority under which the information is requested or, if a written statement of legal authority under which the information is requested would be impracticable, an oral statement of such legal authority; or ■ If the request is made pursuant to a legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

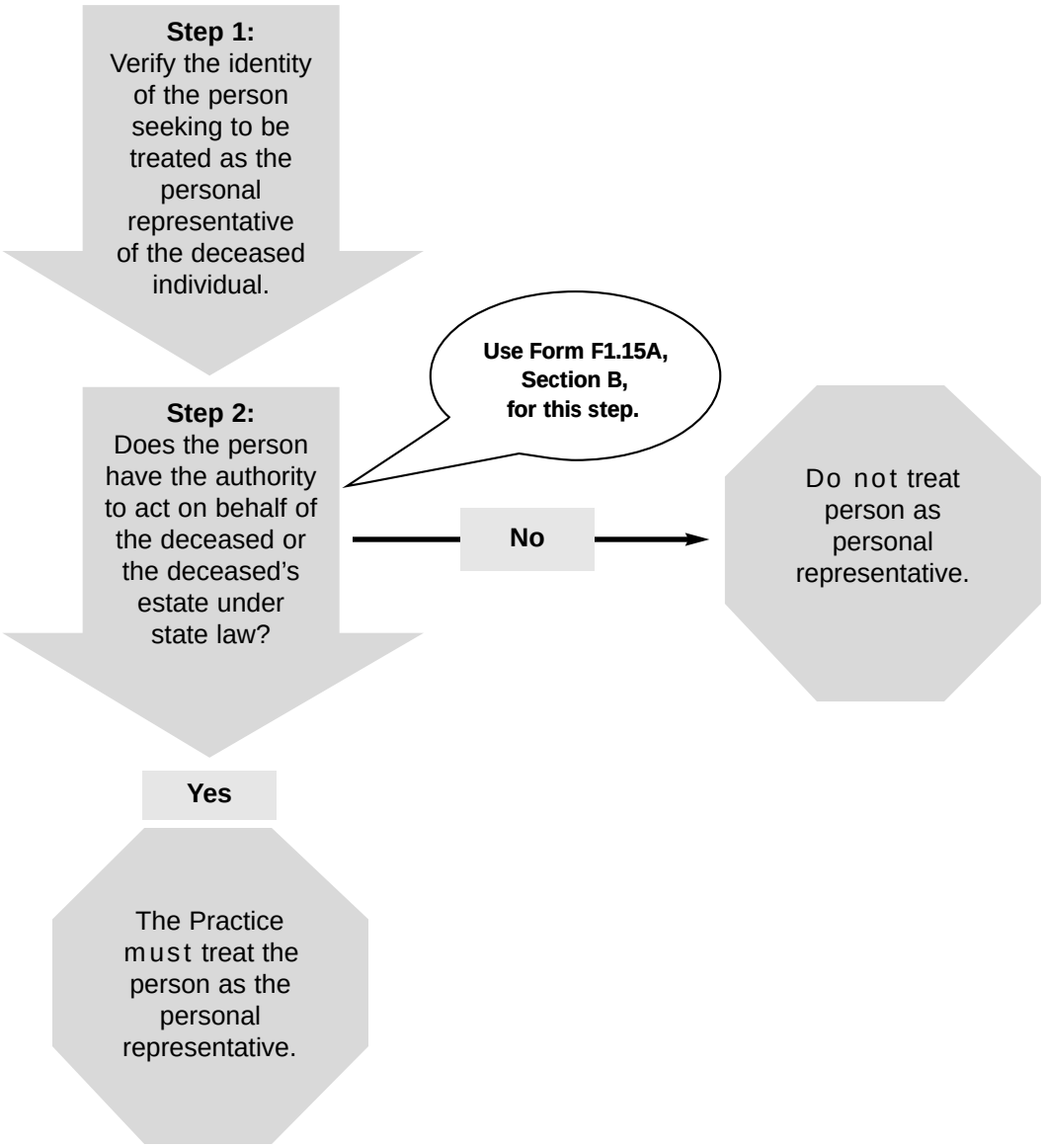
Quick Reference Guide

Process for Determining Personal Representative Status with Respect to Adults and Emancipated Minors (F1.15B)



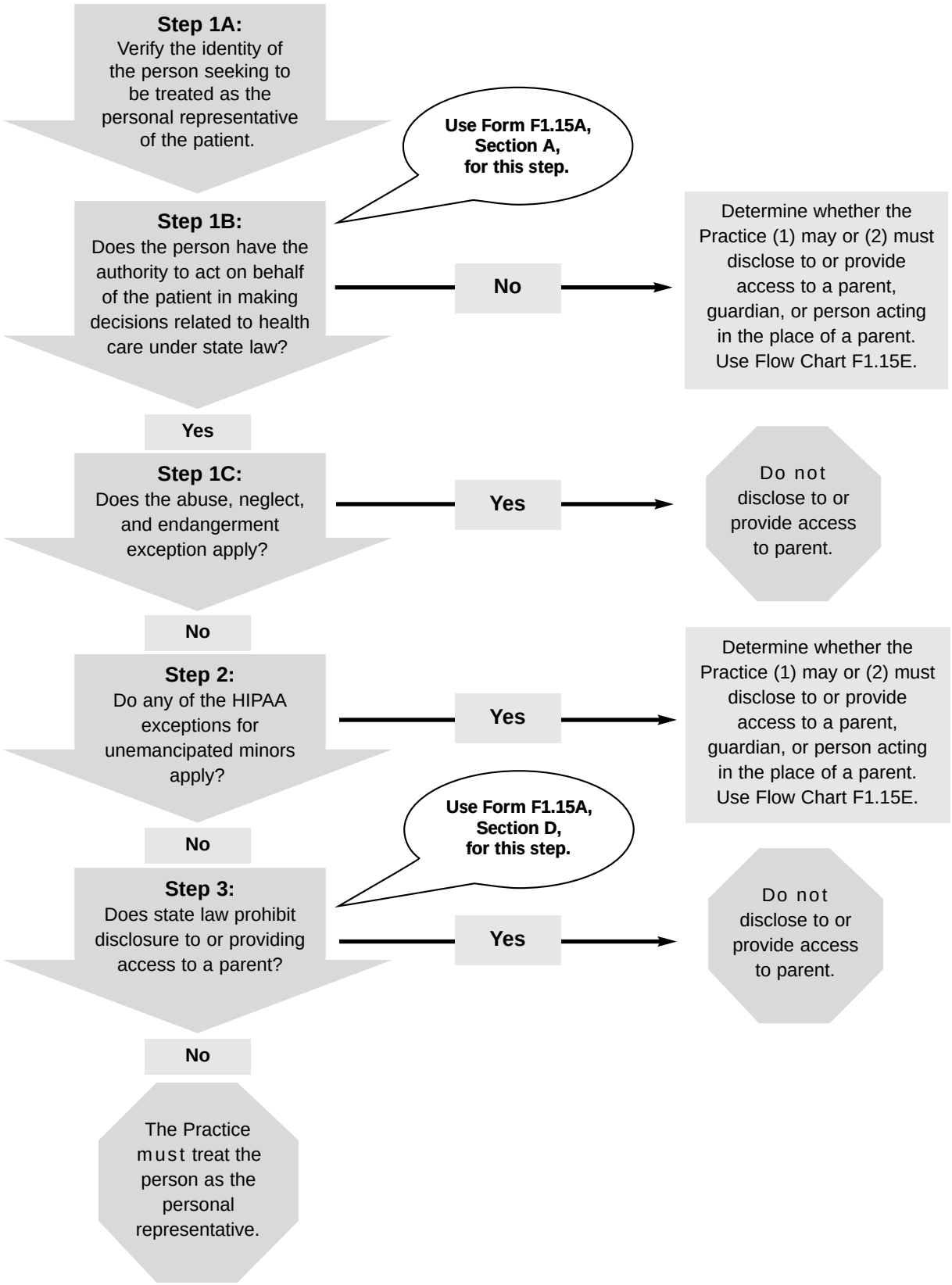
Quick Reference Guide

Process for Determining Personal Representative Status with Respect to Deceased Individuals (F1.15C)



Quick Reference Guide

Process for Determining Personal Representative Status with Respect to Unemancipated Minors (F1.15D)

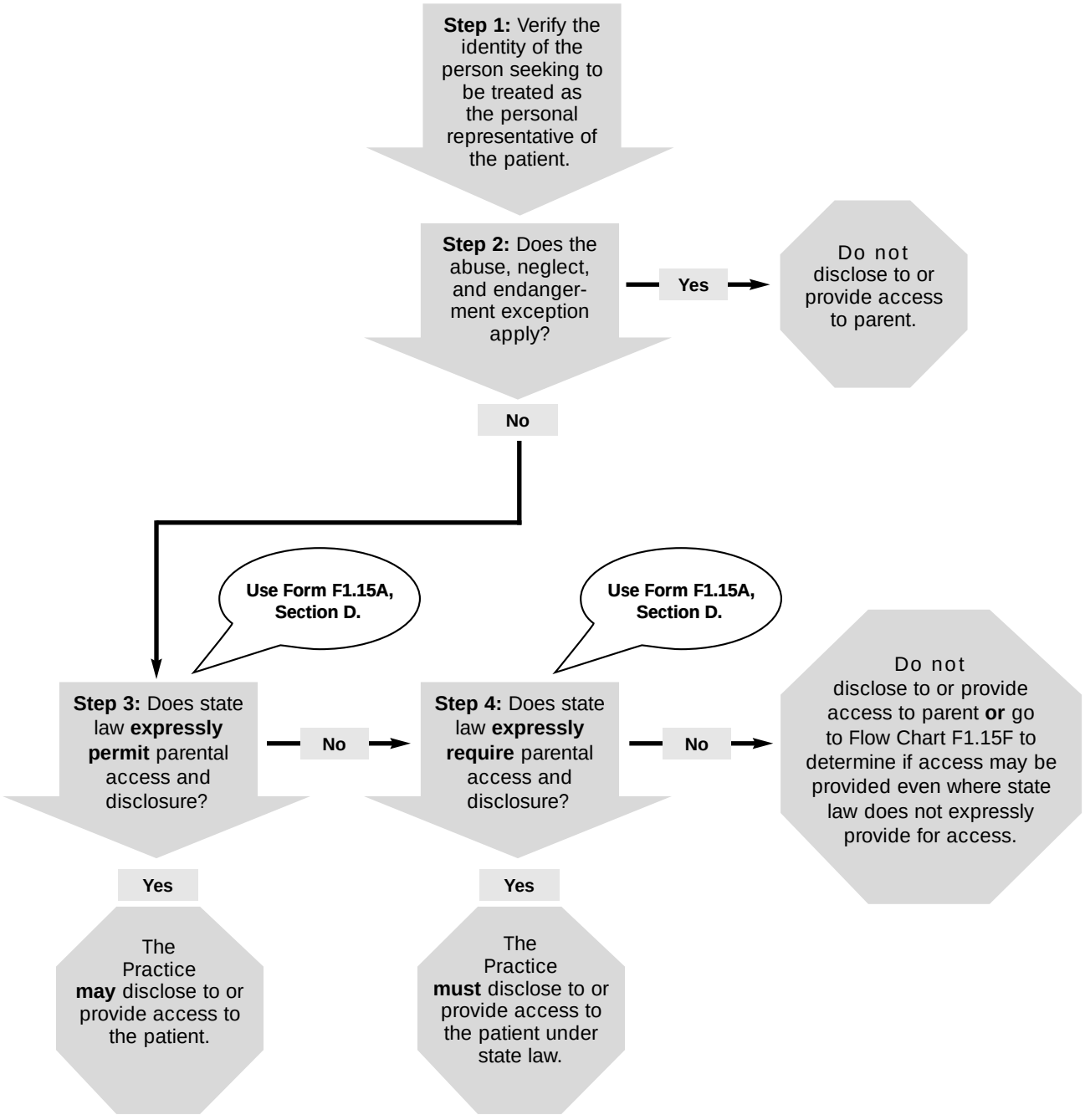


Quick Reference Guide

Process for Determining Whether Practice May or Must Disclose to a Parent* or Provide Access to a Parent Under Express State Law (F1.15E)

Note

It is only necessary to use this Flow Chart where the parent, guardian, or person acting in the place of a parent **does not** otherwise qualify as a personal representative of the unemancipated minor under HIPAA (see Flow Chart F1.15D).



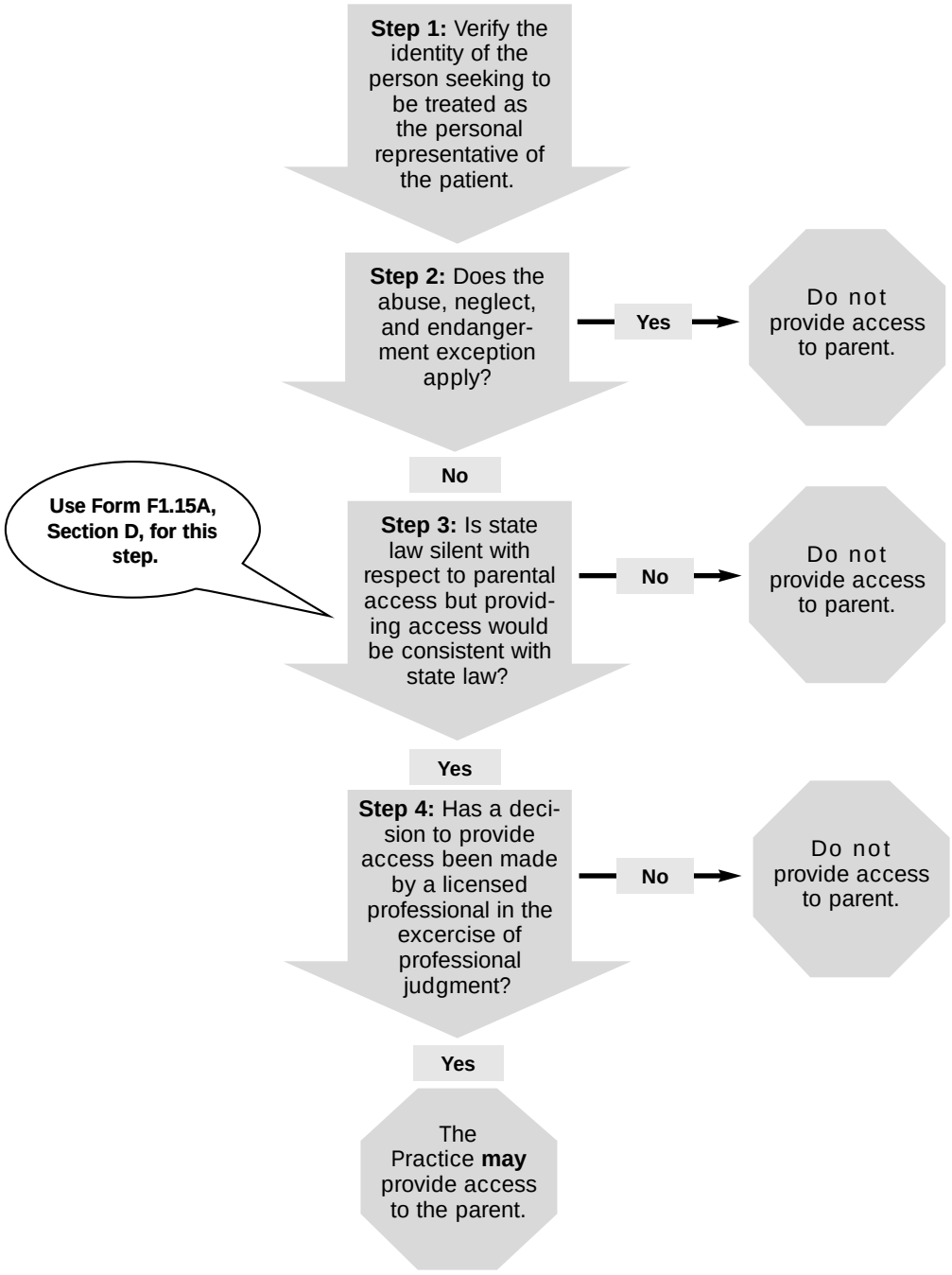
*Note: The term "parent" has been used collectively in this flow chart to refer to a parent, guardian, or a person acting in the place of a parent.

Quick Reference Guide

Process for Determining Whether Practice May Disclose to a Parent* or Provide Access to a Parent Where State Law is Silent (F1.15F)

Note

It is only necessary to use this Flow Chart where the parent, guardian, or person acting in the place of a parent **does not** otherwise qualify as a personal representative of the unemancipated minor under HIPAA (see Flow Chart F1.15D) and where disclosure is not permitted or required by **express** state law (see Flow Chart F1.15E).



*Note: The term "parent" has been used collectively in this flow chart to refer to a parent, guardian, or a person acting in the place of a parent.

QUICK REFERENCE GUIDE

Examples of Common Safeguards

No.	Safeguard Category	Examples of Safeguards
AP	Administrative Procedures	
AP1	Safeguard Documentation	Written designation of Security Official, and other written security policies and procedures
AP2	Security Management Process	Controls for installation/maintenance of equipment Inventory of hardware and software assets Workstation policies/mandatory password change Periodic virus checking policy/procedure
AP3	Certification of Compliance	Certification review by self or third party expert
AP4	Contingency Plans	Arrangements for disaster recovery and emergency mode services
AP5	Formalized Record Processing	Designating a secure fax machine to receive PHI
AP6	Access Control/Personnel Security/ Termination Procedures	Maintain access/authorization records Personnel/security clearance—background/reference checks Sanctions and termination policies and procedures for security violations
AP7	Internal Audit	Regular review of access activity records Regular inventories of storage media for PHI Security incident response procedures
AP8	Workforce Security Training	Orientation/regular workforce security training
AP9	Common Sense Protections	Staff to talk in low voices when discussing PHI Procedures for loud speaker communications *See* Permitted Incidental Disclosures in Quick Reference Guide
PS	Physical Security	
PS1	Assigned Security Responsibility	Written designation of Security Official Allocation of responsibility between Privacy and Security Officials if not the same person
PS2	Media Controls	Locked doors, cabinets, drawers Data backup, storage, and disposal procedures
PS3	Physical Access Controls	Facility security plan Visitor sign-in/escort requirements
PS4	Workstation Policy and Guidelines	Automatic logoff/screen time-out requirements Secure workstation locations
TS	Technical Security	
TS1	Data Integrity Controls	Firewalls/virus protection/alarm
TS2	Computer Access, Audit, and Authorization Controls	Access controls and audit trail Encryption
TS3	Data and Entity Authentication	Unique user identifier Automatic logoff/screen time-out requirements Password/personal identification number (PIN)

QUICK REFERENCE GUIDE

Index of Phase I Policies and Procedures

Note: These policies and procedures are in Chapter 2.

Policy/Procedure	Section Number
PHI Permissions and Special Requirements	
General Policy	P1.0
Permissions	
Required Disclosures	P1.1
Disclosures to the Patient	P1.2
Our Treatment, Payment, Operations	P1.3
Others' Treatment, Payment, Operations	P1.4
Operations of Organized Health Care Arrangement	P1.5
Family, Friends, and Disaster Relief Organizations	P1.6
Incidental Disclosures	P1.7
Public Purpose	P1.8
Authorization	P1.9
De-Identification	P1.10
Limited Data Set	P1.11
Special Requirements	
Verification	P1.12
Minimum Necessary	P1.13
Business Associates	P1.14
Personal Representatives	P1.15
Marketing	P1.16
Psychotherapy Notes	P1.17
Consistent with Notice of Privacy Practices	P1.18
Consistent with Other Documents	P1.19
Consent (State or Other Law)	P1.20
Patient Rights	
General Policy	P2.0
Access	P2.1
Amendment	P2.2
Accounting	P2.3
Alternative Communications	P2.4
Further Restrictions	P2.5
Complaints	P2.6

Privacy Management	Section Number
General Policy	P3.0
Privacy Official/Privacy Contact	P3.1
Notice of Privacy Practices—Development and Distribution	P3.2
Policies and Procedures	P3.3
Documentation	P3.4
Workforce Training	P3.5
Internal Sanctions	P3.6
Mitigation	P3.7
No Retaliation	P3.8
No Waiver	P3.9
Safeguards	P3.10

QUICK REFERENCE GUIDE

Index of Forms

Note: Except where noted, these forms are at the end of the "PP" policies and procedures in Chapter 3 with the same number (for example, Form F1.5 is in PP1.5). These forms are also on the CD-ROM that accompanies this book.

Form #	Title	Purpose
QRG	Quick Reference Guide	QRG appears in Chapter 1, Section 1.2. It provides quick reference to policies and procedures that apply to particular tasks and functions performed in our Practice.
F1.5	Organized Health Care Arrangements	Use to list the participants in each OHCA in which our Practice participates
F1.8A	State Law Required Disclosures	Use to describe the circumstances in which state law requires disclosure of confidential medical information
F1.8B-4	State Law Notification Requirements: Spread of Disease	Use to describe the circumstances in which state law requires our Practice to report confidential medical information regarding the spread of disease
F1.8C	State Law Notification Requirements: Victims of Abuse	Use to describe the circumstances in which state law requires our Practice to report confidential medical information regarding victims of abuse
F.8D	State Notification Requirements: Health Oversight Activities	Use to describe the circumstances in which state law requires our Practice to report confidential medical information regarding health oversight activities
F1.8O	State Law Workers' Compensation Laws	Use to describe state workers' compensation and other similar programs
F1.9	Authorization for Use or Disclosure of Health Information	Use to obtain patient authorization for use or disclosure of PHI
F1.10	De-Identification "Safe Harbor" Checklist	Use to determine if health information has been de-identified under the "safe harbor" method of de-identification
F1.13A	Minimum Necessary Workforce Form	Use to identify the workforce persons or classes of persons who need access to PHI and the categories of PHI to which such persons or classes of persons need access
F1.13B	Minimum Necessary Worksheet Routine PHI Uses	Use to identify uses routinely made by the Practice
F1.13C	Minimum Necessary Worksheet Routine PHI Disclosures	Use to identify disclosures routinely made by the Practice
F1.13D	Minimum Necessary Worksheet Routine PHI Requests	Use to identify requests routinely made by the Practice
F1.14A	Medical Practice HIPAA Business Associate Amendment	Use to develop Business Associate Amendment form
F1.14B	Business Associate Amendment Log	Use to Track the Practice's Business Associates and the status of Business Associate Amendments
F1.14C	Business Associate Amendment Termination Form	Use to document reason for Business Associate Amendment termination, and disposition of PHI
F1.15A	State Laws Governing Personal Representatives	Use to describe various state laws governing personal representatives and the disclosures of medical information that may be made to personal representatives
F1.20A	State Law Consent Requirements	Use to describe the circumstances in which state law requires a consent or notice for the disclosure of confidential medical information

Form #	Title	Purpose
F1.20B	Federal Law Consent Requirements	Use to describe the circumstances in which federal laws require a consent or notice for the disclosure of confidential medical information
F2.1A	Designated Record Set Log	Use to describe the designated record sets maintained by the Practice
F2.1B	Request for Access to Records	Form to be provided to patient for the patient to make written request for access to records
F2.1C	Access Request Log	Use to document access requests made by patients
F2.1D	Response to Request for Access to Records	Use to respond to access request made by patient
F2.1E	Access Denial Review Log	Use to document reviews of patient access denials
F2.1F	Access Request Review: Decision of Reviewing Official	Use to notify patient of the results of an access denial review
F2.2A	Request to Amend Records	Form to be used by patient to make a request to amend medical records
F2.2B	Amendment Request Log	Use to document amendment requests made by patients
F2.2C	Accepted Amendment Form	Use to document an amendment to patient medical record
F2.2D	Response to Request to Amend Records	Use to respond to patient request to amend records
F2.2E	Amendment Notification Confirmation	Use to document notification of amendment to patient's medical records
F2.3A	Practice Protected Health Information Disclosure Log	Use to describe disclosures of PHI made by Practice
F2.3B	Business Associate Protected Health Information Disclosure Log	Business Associate uses this form to document disclosures of PHI made by the Business Associate
F2.3C	Research Disclosure Log	Use to describe certain disclosures made for research purposes
F2.3D	Request for Disclosure Accounting	Form to be used by patient to request an accounting of disclosures of PHI
F2.3E	Accounting Request Log	Use to document patients' requests for an accounting of disclosures of PHI
F2.3F	Response to Request for Disclosure Accounting	Use to respond to a patient's request for an accounting of disclosures of PHI
F2.3G	Summary Information Accounting	Use to provide summary information about multiple disclosures of PHI
F2.3H	Research Disclosure Accounting	Use to provide summary information about disclosures of PHI made by the Practice for research purposes that did not require an authorization
F2.4A	Request for Alternative Communications	Patient uses this form to make a request to the Practice that the Practice communicate with the patient by alternative means or at alternative locations
F2.4B	Alternative Communications Request Log	Use to document patients' requests for alternative communications
F2.4C	Response to Request for Alternative Communications	Use to respond to a patient request for alternative communications
F2.5A	Request to Restrict Uses and Disclosures of Protected Health Information	Patient uses this form to request that the Practice agree to additional restrictions on the uses and disclosures of PHI
F2.5B	Further Restriction Request Log	Use to document requests for further restrictions by patient

Form #	Title	Purpose
F2.5C	Response to Request to Restrict Uses and Disclosures of Protected Health Information	Use to respond to patient request for further restriction
F2.5D	Termination of Agreed Restriction on Use and Disclosure of Protected Health Information	Use to document patient consent to terminate the additional restrictions on the use and disclosure of PHI that were previously agreed to by Practice
F2.5E	Letter Terminating Agreed Restriction Without Consent	Use to provide notice to patient that the Practice is terminating an additional restriction on the use and disclosure of PHI
F2.6A	Privacy Complaint	Use to document privacy complaints
F3.1A	Privacy Official Job Description	Use to describe Privacy Official responsibilities and duties
F3.2A	Notice of Privacy Practices	Use to develop form Notice of Privacy Practices
F3.2B	Notice of Privacy Practices Receipt	Use for patient acknowledgment that patient was provided with a Notice of Privacy Practices
F3.2C	Notice of Privacy Practices Provision Log	Use to document provision of Notice of Privacy Practices to patients
F3.3A	Checklist of Phase II Policies and Procedures	Use to document dates that policies and procedures were adopted and/or modified
F3.3B	Policy/Procedure Modification Form	Use to document and describe modifications to a policy and procedure
F3.5A	Workforce Log	Use to document the names of persons included in the Practice's workforce
F3.5B	Workforce Exclusions Log	Use to describe the circumstances in which a Practice employee provides services not as a member of the Practice's workforce
F3.5C	Personal HIPAA Training Profile	Use to describe the policies and procedures for which a particular employee needs training
F3.5D	Training Session Documentation Form	Use to document attendees at policies and procedures training session
F3.5E	Confidentiality Agreement	Use to develop form Employee Confidentiality Agreement
F3.10A	Safeguards Development and Documentation	Use to record development of safeguards and documentation of safeguards
F3.10B	Sample Questionnaire for Safeguards Vendors	Use to evaluate vendors of safeguards software and products

SECTION 1.3: REFERENCE TOOL FOR PRACTICE OWNERS AND MANAGERS

How to Use This Book

Introduction

If you are a Practice owner or manager, you play a critical HIPAA compliance role. You provide the leadership, management, and resources. You also make or approve key decisions. Use this book to plan and manage your Practice's HIPAA privacy program.

If you are also the Privacy Official, read Section 1.4, Reference Tool for Privacy Officials: How to Use This Book.

Step 1: Learn Some Privacy Rule Basics

Take one step at a time. Don't be intimidated by thinking you have to learn everything at once. Focus on what you need to learn first for your particular roles and responsibilities in the Practice. First learn what you need to get started.

- Read Lessons 1 and 5 of Appendix A.
- For additional background on HIPAA privacy planning, read Chapter 4 of the *Field Guide to HIPAA Implementation.* (AMA Press; www.amapress.org)

Step 2: Appoint Privacy Official

Use Policy/Procedure P3.1 or PP3.1 to appoint the Privacy Official. Also, adopt a job description for the Privacy Official position.

Step 3: Consult With Legal Counsel

Discuss HIPAA compliance, including the following topics, with your lawyer.

- State and other privacy laws that may be stricter and still apply
- Notice of Privacy Practices
- Business Associate Agreements
- Vendor agreements
- Attorney-client privilege

Step 4: Board Action

Your board of directors (or other governing body) should approve and adopt resolutions regarding the Practice's commitment to HIPAA compliance. The board should:

- empower and motivate staff to implement HIPAA compliance, and
- receive periodic status reports from the practice manager or chief executive and the Privacy Official. The Board should approve key decisions.

Step 5: Lead by Example

In their personal actions, Practice leaders need to set the tone for HIPAA privacy implementation in the Practice. Lead by example. Set a positive tone and emphasize the benefits that HIPAA can bring to the Practice.

Step 6: Continue Learning About HIPAA

Step 6 never ends! Everyone's HIPAA education will continue. Over time, parts of HIPAA will become second nature. But we all need to stay abreast of developments in how the U.S. Department of Health and Human Services (HHS) and the courts apply HIPAA, and how the health care industry evolves in protecting patient privacy.

Chapter 4 contains tips for educating your Practice's staff about patient privacy.

Step 7: Address Own Group Health Plan

Your Practice may purchase group health insurance for Practice employees. If so, the Practice likely sponsors a "health plan" that is a "covered entity" under the HIPAA Privacy Rule. "Health plan" includes an individual or group plan that provides, or pays the cost of, medical care. For purposes of HIPAA, a health plan does not include coverage for accident or disability insurance, liability insurance or a supplement to liability insurance, workers' compensation or similar insurance, automobile medical payment insurance, credit-only insurance, coverage for on-site medical clinics, and other similar insurance coverage under which benefits for medical care are secondary or incidental to other insurance benefits.

Your Practice's health plan is likely a covered entity under HIPAA. This is true even if it is a fully-insured plan. What employers have to do for HIPAA compliance depends in part on what plan information the employer gets and for what purpose. The Privacy Rule's impact on health plans is a complex subject and beyond the scope of this desk reference, which is intended for physician practices. That said, if your plan is insured or if you have a professional third-party administrator, it is important to coordinate who is responsible for what HIPAA Privacy requirements. The fiduciary of your Practice's health plan should coordinate with the insurer or administrator to assure himself or herself, in consultation with the plan administrator or with plan counsel, that the applicable HIPAA requirements with respect to the plan are being met.

SECTION 1.4: REFERENCE TOOL FOR PRIVACY OFFICIAL

How to Use This Book

Introduction

Congratulations! You were selected, and you have agreed to be the Privacy Official of your Practice. You will play a critical role in your Practice's ability to survive in a new era of privacy in health care. There is a lot to learn and monitor continuously. You will be well served to start early. Your mission, much of which you've already accepted, is to learn a lot about the Privacy Rule and its implications for your Practice. With that knowledge, you can prepare your practice for compliance.

You will do more to protect the privacy and security of patient information than you ever thought possible. You will also become an even more valuable asset to your Practice. You will not only assure that all of the many detailed aspects of compliance are met, but you will serve as an invaluable resource to your Practice when new and unexpected compliance challenges arise.

Step 1: Learn Some Privacy Rule Basics

- For additional privacy and information security background, read the American Medical Association's *Field Guide to HIPAA Implementation* (AMA Press; www.amapress.org), Chapters 4, 6, and 7.
- Read all of Appendix A, Privacy Rule Summary.

Step 2: Advise Management

Owner or management approval is needed to take certain actions regarding HIPAA compliance. That means you have to "teach" others about HIPAA.

Step 3: Policy and Procedure Adoption

- Consult with legal counsel about state law privacy requirements that still apply.
- Use this book to adopt HIPAA privacy policies and procedures. (See Flow Chart "How to Build Policies and Procedures" following this section.)
- Modify the sample policies and procedures as appropriate for your Practice's needs and requirements under state and other laws, as applicable.
- Adopt other policies and procedures to fit your needs and the requirements of state and other laws, as applicable.
- Review Safeguards Policy and Procedure (PP3.10) to develop and implement safeguards appropriate for your Practice's operations. (See Flow Chart "How to Develop Safeguards" following this section.)

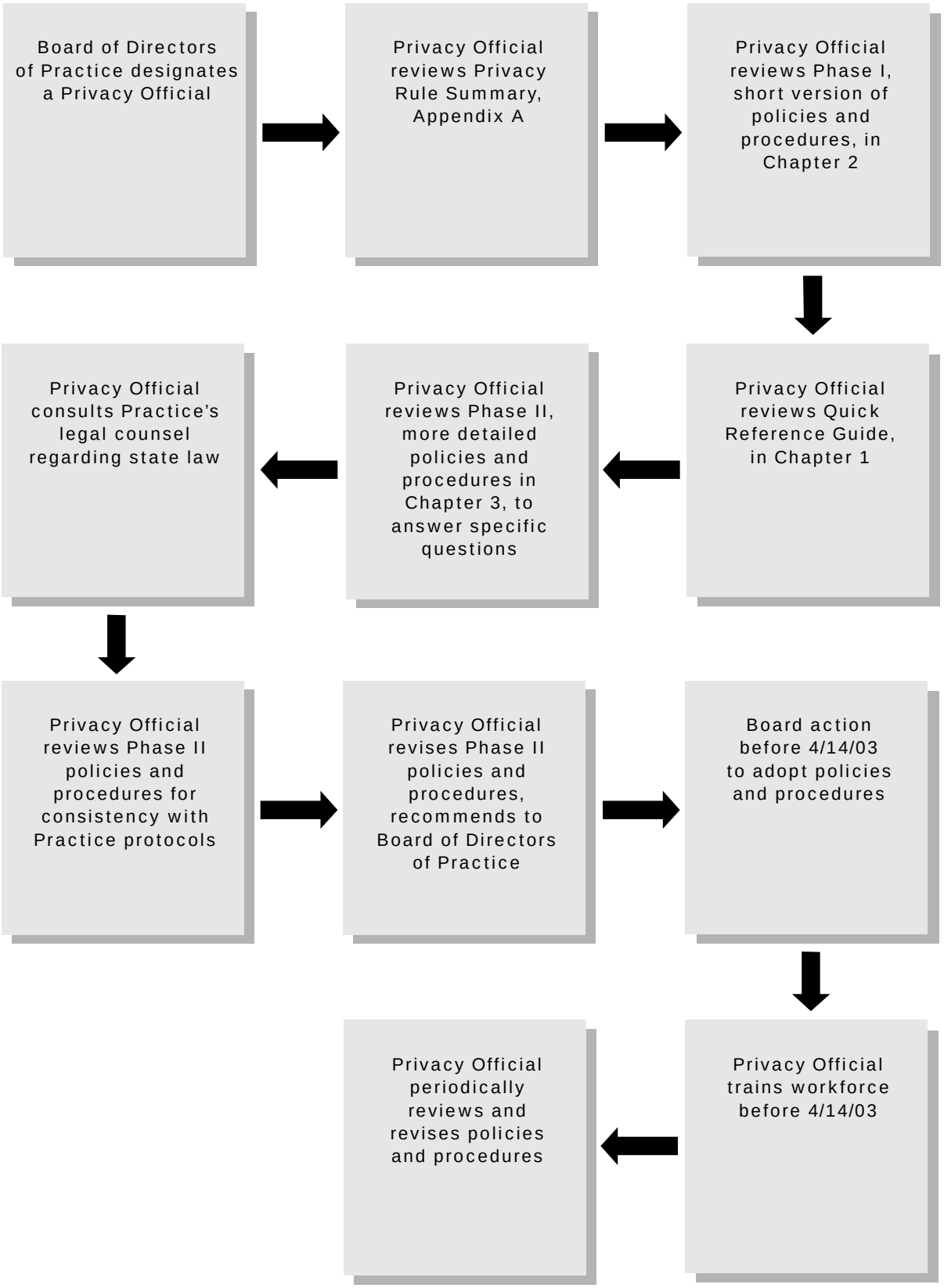
Step 4: Policy and Procedure Documentation

HIPAA requires documentation of policies and procedures. You can use this book as a place to document and keep your Practice's HIPAA privacy policies and procedures.

Step 5: Training

You can use this book to train your Practice's workforce. Assign particular policies and procedures to specific persons based on their job responsibilities, and train them on these assignments. This book contains Workforce Training Policies and Procedures (PP3.5). Chapter 4 contains additional tips for educating the Practice's staff on patient privacy.

Quick Reference Guide
How to Develop and Implement Privacy Policies and Procedures



Quick Reference Guide
How to Develop and Implement Safeguards Policies and Procedures

chapter 2

Phase I Policies and Procedures

OVERVIEW

Introduction

Compliance with HIPAA is a lot of work. Start with Phase I, or "HIPAA Light" in this chapter. Then, as you are ready, tackle Phase II, or "HIPAA Heavy" in Chapter 3.

Note

We are not saying that by implementing "HIPAA Light" you will comply with the Privacy Rule as of April 14, 2003. We offer you this two-phased approach so that you have the option of first addressing the major HIPAA requirements in shorter policies and procedures, and then building toward a more detailed compliance program as the material becomes more familiar.

The numbering of Phase I "P" policies and procedures is the same as Phase II "PP" policies and procedures. So, for example, P1.10 addresses the same topic as PP1.10—PP1.10 is just more detailed. If you need more information about how a "P" policy is applied, you can flip over to the "PP" version.

How to Use This Chapter

- Consult with legal counsel regarding HIPAA and state law impacts on your Practice.
- Adopt Phase I policies and procedures.
- Document your Phase I policies and procedures in this book.
- Modify the Quick Reference Guide in Chapter 1 to identify policies and procedures that apply to specific tasks or functions in your Practice.
- Use Chapter 2 as a "portal" into Phase II policies and procedures. Over time, adopt Phase II policies to meet the needs of your Practice.

List of Phase I Policies and Procedures

Phase I policies and procedures are organized into the following categories:

Policy/Procedure	Description	Section Number
PHI Permissions	Restrictions on using and disclosing patient information.	P1
Patient Rights	Patient rights with respect to patient information.	P2
Privacy Management	Policies relating to the administrative aspects of protecting patient privacy.	P3

INDEX OF PHASE I POLICIES AND PROCEDURES

Policy/Procedure	Section Number
PHI Permissions	
General Policy	P1.0
Permissions	
Required Disclosures	P1.1
Disclosures to the Patient	P1.2
Our Treatment, Payment, Operations	P1.3
Others' Treatment, Payment, Operations	P1.4
Operations of Organized Health Care Arrangement	P1.5
Family, Friends, and Disaster Relief Organizations	P1.6
Incidental Disclosures	P1.7
Public Purpose	P1.8
Authorization	P1.9
De-Identification	P1.10
Limited Data Set	P1.11
Special Requirements	
Verification	P1.12
Minimum Necessary	P1.13
Business Associates	P1.14
Personal Representatives	P1.15
Marketing	P1.16
Psychotherapy Notes	P1.17
Consistent with Notice of Privacy Practices	P1.18
Consistent with Other Documents	P1.19
Consent (State or Other Law)	P1.20
Patient Rights	
General Policy	P2.0
Access	P2.1
Amendment	P2.2
Accounting	P2.3
Alternative Communications	P2.4
Further Restrictions	P2.5
Complaints	P2.6
Privacy Management	
General Policy	P3.0
Privacy Official/Privacy Contact	P3.1
Notice of Privacy Practices—Development and Distribution	P3.2
Policies and Procedures	P3.3
Documentation	P3.4
Workforce Training	P3.5
Internal Sanctions	P3.6
Mitigation	P3.7
No Retaliation	P3.8
No Waiver	P3.9
Safeguards	P3.10

PHI: PERMISSIONS

Introduction

Welcome to "HIPAA Light." This description of the PHI Permissions category of policies and procedures covers the basic requirements for the use and disclosure of PHI. You may refer to the "HIPAA Heavy" or Phase II policies and procedures in Chapter 3 for clarification or guidance. The Phase II policies and procedures have the same numbering scheme as the Phase I policies and procedures.

Forms to assist in complying with these policies and procedures are included in this book. The forms are listed in the Index of Forms at the end of Chapter 1. The forms are numbered to match the number of the applicable policies and procedures. The forms themselves are found in the Chapter 3 "Phase II" or "PP" Policies and Procedures (along with instructions on their use).

General Policy
P1.0

Our policy is to use and disclose PHI only in compliance with the HIPAA Privacy Rule and other applicable requirements. This means that three things must happen.

- First, the use or disclosure must fit under an applicable Privacy Rule Permission.
- Second, the use or disclosure must comply with the conditions of that Permission.
- Third, the use or disclosure must comply with "Special Requirements" under the Privacy Rule and other laws that may apply.

Required Disclosures
P1.1

It is our Practice's policy to disclose PHI as required by the Privacy Rule. The Privacy Rule requires us to provide a patient, when requested, access to his or her own PHI (pursuant to P2.1) or an accounting of disclosures of his or her PHI (pursuant to P2.3).

The Privacy Rule also requires that we permit the U.S. Department of Health and Human Services (HHS) to access our facilities, books, records, accounts, and other information, including PHI, that are relevant to HHS determining our compliance with the Privacy Rule.

Disclosures to the Patient
P1.2

Our Practice may disclose PHI to an individual who is the subject of such information. We may generally disclose such information to an individual's personal representative, unless exceptions apply (under Personal Representatives, P1.15, because the individual is an unemancipated minor, the Practice believes that the individual has been abused or neglected by the personal representative, or such disclosure may otherwise endanger the individual).

Our Treatment, Payment, Operations
P1.3

Our Practice's policy is to use and disclose PHI for our treatment, payment, and health care operations, *without obtaining consent or authorization from the patient,* as permitted by the Privacy Rule, except where a HIPAA "Authorization" is specifically required or other Special Requirements apply, such as when PHI is used for Marketing, when the PHI includes Psychotherapy Notes, or when state law may require patient permission to use or disclose.

The definitions of treatment, payment, and health care operations are extensive and are included in full in the Glossary.

"Treatment" generally means the provision, coordination, or management of health care and related services among health care providers or by a health care provider with a third party, consultation between health care providers regarding a patient, or the referral of a patient from one health care provider to another.

"Payment" generally encompasses the various activities of health care providers to obtain payment or be reimbursed for their services and of a health plan to obtain premiums, to fulfill its coverage responsibilities and provide benefits under the plan, and to obtain or provide reimbursement for the provision of health care.

"Health care operations" are certain administrative, financial, legal, and quality improvement activities of a covered entity that are necessary to run its business and to support the core functions of treatment and payment. These activities are limited to the specific activities listed in the definition of "health care operations" in the Glossary.

Others' Treatment, Payment, Operations P1.4

Our Practice's policy is that we may use and disclose PHI for the Treatment and Payment activities of other Health Care Providers, and for Payment activities and some Health Care Operations activities of other Covered Entities, *without consent or authorization from the patient*, as permitted by the Privacy Rule, except where an Authorization is specifically required or other special requirements apply, such as when PHI is used for Marketing, or when the PHI includes Psychotherapy Notes.

For purposes of our Practice's permitted uses and disclosures of PHI for the Health Care Operations of another, the applicable definition of Health Care Operations is more limited than in the case of our own Health Care Operations. Our Practice's uses and disclosures of PHI for certain Health Care Operations of another Covered Entity are permitted only if our Practice and the other Covered Entity have (or had) a relationship with the individual who is the subject of the PHI being requested, and the disclosure is:

(i) for a purpose related to (A) quality assessment and improvement, or (B) reviewing the competence of health care professionals and training—more specifically described in paragraphs (1) and (2) of the complete definition of Health Care Operations (see Glossary); or

(ii) for the purpose of health care fraud and abuse detection or compliance.

For example, a health care provider may disclose PHI to a health plan for the plan's HEDIS (Health Plan Employer Data and Information Set) purposes, provided the health plan has or had a relationship with the individual who is the subject of the information.

The definitions of "treatment" and "payment" for purposes of others' treatment and payment activities are the same as those definitions for purposes of our Practice's treatment and payment activities.

For example, a physician may send an individual's health plan coverage information to a laboratory that needs the information to bill for services it provided to the physician with respect to the individual.

Operations of Organized Health Care Arrangement P1.5

Generally, the Privacy Official or contact will determine if we participate in an Organized Health Care Arrangement (OHCA) and (if so) who the other participants in the OHCA are. The definition of an OHCA includes five types of related organizations, but the definitions most likely to apply to our Practice are:

- a clinically integrated care setting where individuals usually receive care from more than one provider; or
- an organized system of care in which more than one Covered Entity participates, and they: (1) hold themselves out to the public as a joint arrangement and (2) jointly conduct utilization review, quality assessment, or certain payment activities.

All uses and disclosures of PHI for Health Care Operations of the OHCA by or to another covered entity participating in an OHCA are permitted except where an Authorization is specifically required or other Special Requirements apply, such as when PHI is used for Marketing, or when the PHI includes Psychotherapy Notes.

Our practice may issue a joint Notice of Privacy Practices with other participants in an OHCA about use and disclosure of PHI as permitted by the Privacy Rule and as determined appropriate by our Privacy Official. Where our Practice discloses PHI for the Health Care Operations of an OHCA, we will give notice of those disclosures in our Notice of Privacy Practices.

Family, Friends, and Disaster Relief Organizations P1.6

Our Practice may disclose PHI related to a patient's current condition to a patient's family member or other relative, a close personal friend (or any other person identified by the patient) involved in the patient's care, or a disaster relief organization (for purposes of notifying a patient's family member or personal representative) if the patient:

(a) is given an opportunity to agree to or prohibit the use or disclosure of PHI, or

(b) is incapacitated or not present, but the disclosure is in the patient's best interests.

Incidental Disclosures
P1.7

Our Practice's policy is to limit the scope of PHI exposed to "Incidental Disclosures" by complying with the Privacy Rule's Minimum Necessary requirements (P1.13), and by taking reasonable steps to implement appropriate Safeguards (P3.10) to protect against such disclosures.

Incidental Disclosures are permitted under our Practice's policies only to the extent permitted under the Privacy Rule. The Privacy Rule permits only incidental uses and disclosures of PHI that occur as a by-product of another permissible or required use or disclosure, as long as our Practice has applied *reasonable safeguards* and implemented the *minimum necessary* standard, where applicable, with respect to the primary use or disclosure.

Examples of permitted Incidental Disclosures are included in the Quick Reference Guide in Chapter 1.

Public Purpose
P1.8

It is our Practice's policy to comply with federal, state, and local laws with respect to the use or disclosure of PHI, and to recognize those situations in which disclosure is required or permitted for public policy purposes or requirements under the Privacy Rule. Generally, the Privacy Official will determine whether a use or disclosure of PHI is for a public purpose permitted or required under the Privacy Rule (except for documented delegation of this task to properly trained persons).

Public purpose uses and disclosures permitted under specific limited circumstances described in the Privacy Rule include uses and disclosures of PHI:

- as required by law;
- for public health activities, including public health authority activities, and uses and disclosures related to child abuse, Food and Drug Administration, spread of disease, or to an employer;
- about victims of abuse, neglect, or domestic violence;
- for health oversight activities;
- in a judicial or administrative proceeding;
- for law enforcement purposes;
- with respect to a decedent;
- to facilitate organ donation;
- for research;
- to avoid serious threat to health or safety;
- regarding armed forces personnel;
- regarding national security and intelligence activities;
- to provide protective services for the President of the United States and other high state officials;
- about an individual in legal custody; or
- to comply with workers' compensation laws.

The rules for each of these categories of use or disclosure under the Public Purpose Permission are set forth in more detail in PP1.8 in Chapter 3.

Authorization
P1.9

Our Practice may not use or disclose PHI without a valid Authorization, unless such use or disclosure is otherwise permitted or required by the Privacy Rule. We will document and retain any Authorization pursuant to which we use or disclose PHI on the standard Authorization Form. The Practice's standard Authorization Form is attached as form F1.9.

The requirement for a patient's Authorization does not apply to uses and disclosures that comply with any of the following Permissions:

- Required Disclosures (P1.1)
- Disclosures to the Patient (P1.2)
- Our Treatment, Payment, Operations (P1.3)

- Others' Treatment, Payment, Operations (P1.4)
- Operations of Organized Health Care Arrangements (P1.5)
- Family, Friends, and Disaster Relief Organizations (P1.6)
- Incidental Disclosures (P1.7)
- Public Purpose (P.1.8)
- De-identification (P1.10)
- Limited Data Set (P1.11)

De-Identification P1.10

It is our Practice's policy to create de-identified information and disclose de-identified information only in compliance with the HIPAA Privacy Rule. Our policy is that PHI may be de-identified only in compliance with either the safe harbor method or the expert statistician method, both of which are described in the Privacy Rule. Questions regarding what is "de-identified information" and "protected health information" should be referred to the Privacy Official.

Limited Data Set P1.11

Our Practice is permitted to disclose a "Limited Data Set" to recipients who will use the information only for the purposes of research, public health, or health care operations. The Privacy Official will document compliance with "Limited Data Set" requirements. A "Limited Data Set" is PHI that excludes certain direct identifiers of the patient or of relatives, employees, or household members of the patient.

We may use or disclose a "Limited Data Set" only if we obtain a signed data use agreement that meets certain requirements, including assuring that the Limited Data Set recipient will only use or disclose the PHI for limited purposes.

If our Practice knows of a pattern of activity or practice of the Limited Data Set recipient that constitutes a material breach or violation of the data use agreement, we are required to take steps to cure the breach or end the violation. If such steps are unsuccessful, we are required to discontinue disclosure of PHI to the recipient and report the problem to the Secretary of HHS.

PHI: SPECIAL REQUIREMENTS

Introduction

P1.1 through P1.11 describe how PHI uses and disclosures are permitted (and in some cases required) under the Practice's policies and procedures. These policies and procedures track the permissions contained in the HIPAA Privacy Rule. All PHI uses and disclosures must fit in one of these permissions.

P1.12 through P1.20 describe "Special Requirements," which are additional requirements for using and disclosing PHI. These additional requirements may apply depending on the facts. We call these "Special Requirements." These are things you have to do in addition to fitting in one of the "Permission" policies and procedures.

Verification
P1.12

Our Practice's policy is to comply with the Privacy Rule requirement that, before releasing PHI to someone who has requested it, the Practice must:

(1) verify the *identity* of any person (if unknown to the Practice) who requests PHI, and

(2) verify the *authority* of any such person to have access to the PHI.

The Practice's policy is to obtain any documentation required for release of PHI from the person requesting the PHI.

A Verification Procedures Guide that summarizes the requirements for Verification is provided as part of the Quick Reference Guide in Chapter 1.

Minimum Necessary
P1.13

Our Practice's policy is to make reasonable efforts and implement reasonable Safeguards (P3.10) to limit uses, disclosures, and requests for disclosure of PHI to the minimum necessary amount of information to achieve the purpose of the use, disclosure, or request.

These efforts will include:

(a) limiting each staff member's access to the minimum amount of PHI necessary to carry out his or her duties; and

(b) taking reasonable steps to avoid incidental uses or disclosures that result from otherwise required uses or disclosures.

There are exceptions to the Minimum Necessary requirements. The Minimum Necessary standard does not apply to:

- disclosures to or requests by a health care provider for treatment purposes;
- disclosures to the patient of his or her own PHI;
- uses or disclosures made according to a patient Authorization;
- uses or disclosures to comply with HIPAA;
- disclosures to HHS for Privacy Rule enforcement purposes; and
- uses or disclosures required by other law.

Business Associates
P1.14

It is our Practice's policy to enter into a Business Associate Agreement with all Business Associates (as defined in and required by the Privacy Rule) before disclosing PHI to a Business Associate or allowing a Business Associate to create or receive PHI on behalf of the Practice.

The Standard Business Associate Amendment (F1.14A) will be used for all Business Associates of the Practice. The Privacy Official must approve any change to this Standard Amendment. The Privacy Official will seek advice from legal counsel regarding any deviations from this Standard Amendment, as appropriate.

If the Practice becomes aware of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligations under the Business Associate Agreement, the Practice will take reasonable steps to:

- cure the breach or end the violation;
- terminate the contract; or
- report the problem to the Secretary of HHS.

The policy of the Practice is to mitigate, to the extent practicable, any harm that results from a privacy breach or violation by a Business Associate.

Personal Representatives P1.15

It is our policy to treat the "Personal Representative" of a patient just as we would the patient with respect to disclosures of PHI, access to PHI, and exercise of patient HIPAA rights, except as otherwise provided by this policy. However, a Personal Representative will only be treated as a Personal Representative with respect to PHI that is relevant to that particular representation. Our Practice will follow both HIPAA requirements and applicable state law in this area.

> **Note**
>
> The application of this Personal Representative Policy and Procedure in a particular state will be highly dependent on relevant state laws. The Privacy Official, consulting with legal counsel as appropriate, will use Form F1.15A, sections A through D to describe applicable state laws.

The Privacy Rule specifies who may act as a Personal Representative for the following three categories of persons:

If the patient is . . .	**then the personal representative is . . .**
■ a deceased individual (or the deceased individual's estate)	the executor, administrator, or other person who has the authority under state law to act on behalf of the deceased individual or the individual's estate
■ an adult or emancipated minor	the person who has the authority under state law to act on behalf of the adult or emancipated minor **in making decisions related to health care**
■ an unemancipated minor	the parent, guardian, or a person acting in the place of a parent who has the authority under applicable state law to act on behalf of an unemancipated minor in making decisions related to health care

The state law definitions for emancipated and unemancipated minors are described in Form F1.15A, Section E (Privacy Official to complete this form in consultation with legal counsel).

The Privacy Rule contains special permissions regarding who can be a Personal Representative of *unemancipated minors.* A person may not be a Personal Representative of an unemancipated minor, and the minor has the authority to act as the individual with respect to PHI pertaining to a health care service, if:

- the minor consents to such health care service; no other consent to such service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as a personal representative.
- the minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in the place of a parent; and the minor, a court, or another person authorized by law consents to such health care service; *or*
- a parent, guardian, or other person acting in the place of a parent assents to an agreement of confidentiality between a covered health care provider and the minor with respect to such health care service.

Even when a parent, guardian, or person acting in the place of a parent does not qualify as a Personal Representative, the Practice may still disclose PHI to or provide access to PHI to a parent where state law *expressly* grants *permission*. Where state law requires disclosure or access, the Practice *must* comply.

When state law does not *expressly* provide for access, the Practice may still provide access to a parent, guardian, or person acting in the place of a parent if the following criteria are met:

- there are no specifically applicable access provisions under state law;
- giving access would be *consistent* with state law; *and*
- the decision to provide access is made by a licensed health care professional in the exercise of professional judgment.

These applicable state laws are described in Form F1.15A, Sections A through D.

Notwithstanding any other policy described above in this P1.15, including applicable state law, our Practice *may elect* not to treat a person as a Personal Representative if the Practice has a reasonable belief that:

- the individual has been or may be subjected to domestic violence, abuse, or neglect by such person or treating such person as the Personal Representative could endanger the individual; and
- the Practice, in the exercise of professional judgment, decides that it is not in the best interests of the individual to treat the person as the individual's Personal Representative.

Marketing
P1.16

It is the policy of this Practice to obtain a specific Authorization for any disclosure of an individual's PHI for Marketing purposes, except as otherwise permitted by the Privacy Rule. A Marketing communication is allowed without an Authorization if the communication is (a) a face-to-face communication made by the Practice to an individual, or (b) a promotional gift of nominal value provided by the Practice.

"Marketing" means making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service. Certain PHI uses and disclosures are excluded from this part of the "Marketing" definition under the Privacy Rule:

- describing (a) health-related products or services, or (b) payments for health-related products or services, that are provided by or included in a benefits plan of the Practice;
- for treatment of that individual;
- uses for case management or care coordination for that individual; or
- directing or recommending alternative treatments, therapies, health care providers, or settings of care to that individual.

Marketing also means an arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

For example, a drug manufacturer receives a list of patients from a Covered Entity and provides remuneration, then uses that list to send discount coupons for a new antidepressant medication directly to the patients. This is a Marketing disclosure by the Covered Entity under the second definition of Marketing.

Psychotherapy Notes
P1.17

Our Practice's policy is to abide by the Privacy Rule and not use or disclose Psychotherapy Notes without an Authorization from the patient, except as described below.

The only exceptions under the Privacy Rule to this requirement for a patient Authorization before releasing Psychotherapy Notes are:

- uses by the originator of the Psychotherapy Notes for treatment purposes;
- uses or disclosures by our Practice for our training programs;
- uses or disclosures by our Practice to defend ourselves in legal actions or other proceedings brought by the individual;

- disclosures to the individual as required by HIPAA;
- disclosures to the Secretary of HHS as required by HIPAA;
- uses or disclosures that are required by law;
- disclosures to health oversight agencies with respect to oversight of the originator of the Psychotherapy Notes;
- uses and disclosures that are by or to a coroner or medical examiner for certain purposes; and
- uses and disclosures that are necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public *and* to a person reasonably able to prevent or lessen the threat.

Consistent with Notice of Privacy Practices
P1.18

It is our Practice's policy that we will not use or disclose PHI in a manner inconsistent with our Practice's Notice of Privacy Practices (NPP).

If you have any questions about the NPP or whether a use or disclosure is consistent with the NPP, contact the Privacy Official.

Our Practice will not engage in any of the following activities unless the Practice's NPP includes a separate statement that:

- the Practice may contact the patient to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the patient; or
- the Practice may contact the patient to raise funds for the Practice.

Consistent with Other Documents
P1.19

It is our Practice's policy that we will use and disclose PHI consistent with any limitations placed on the use or disclosure of such PHI by other documents or agreements entered into by the Practice.

Examples of documents or agreements that may contain additional limitations on uses or disclosures of PHI include:

- Authorizations (P1.9);
- Agreements to further restrict uses and disclosures of PHI (P2.5);
- Alternative Communications agreements (P2.4);
- Amendments (or Amendment denials) (P2.2); and
- Privacy or confidentiality provisions in contracts entered into by the Practice.

Consent (State or Other Law)
P1.20

There are circumstances in which state or other federal laws will require some form of consent or notice for certain uses or disclosures of PHI even where HIPAA does not require an Authorization. Also, other laws may provide a greater right of access to PHI. In our state, a consent or notice is required in the circumstances described in Form F1.20A, State Law Consent Requirements. The circumstances in which our state laws provide a greater right of access to PHI are also described in Form F1.20A. Federal laws require a consent in the circumstances described in the form Federal Law Consent Requirements (F1.20B). The Privacy Official will oversee the completion of and updates to these forms.

PATIENT RIGHTS

Introduction

The HIPAA Privacy Rule gives patients new rights with respect to PHI that relates to them. This Patient Rights category of policies and procedures covers what the Practice must do when patients exercise these rights.

General Policy
P2.0

It is our policy to comply with patient rights requirements of the Privacy Rule as further detailed below. Every employee should recognize when a patient is exercising these rights. Subject to further direction from the Privacy Official on procedures, you should generally refer a patient request to the Privacy Official for handling. If you have questions, contact the Privacy Official.

Access
P2.1

It is our Practice's policy to comply with the Privacy Rule regarding a patient's right to request to have access to and obtain copies of PHI about the patient maintained by or for the Practice in a Designated Record Set. Designated Record Sets include billing records, medical records, and other records used to make decisions regarding a patient.

The HIPAA right to access does not apply to (1) Psychotherapy Notes; (2) PHI compiled in reasonable anticipation of or for use in a civil, criminal, or administrative action; and (3) any laboratory reports or other related information that are exempt from the Clinical Laboratory Improvement Amendments (CLIA).

A request to inspect or obtain a copy of PHI must be made in writing (refer to form F2.1A). The Practice has a specified number of days to respond to such a request, depending on whether the PHI is maintained on-site or off-site.

The Practice may deny a request for access for several different reasons. The types of permitted denials are divided into two categories: those for which our Practice must provide a review process and those for which a review is not required (refer to policy PP2.1). If a denial is reviewable, the patient has the right to have the denial reviewed by a licensed health care professional who did not participate in the original decision to deny access.

If the Practice denies a request for access it must:

- send a timely written denial to the individual,
- provide other PHI after excluding the information to which there is a ground to deny access, and
- be helpful in informing the patient where else to direct a request for access.

If the Practice grants a request for access, it must:

- provide the patient with access to the PHI in the form or format requested by the patient, if it is readably producible in such format. If it is not, the PHI must be provided in a readable, hard copy form or another format agreed to by the patient. If the patient agrees, the Practice can provide a summary of the PHI requested in lieu of providing access.
- arrange with the patient a convenient time and place to inspect or obtain a copy of the PHI. The PHI can also be mailed to the patient. The Practice may recoup the reasonable cost of copies it makes in response to a request for access.

Form F1.20A describes applicable state laws or other laws that still apply and that require us to do other or different things than what the HIPAA Privacy Rule requires regarding patient access to records.

Amendment
P2.2

It is our Practice's policy to comply with the Privacy Rule and applicable state laws regarding a patient's request that our Practice amend PHI about the patient in a Designated Record Set. Designated Record Sets include billing records, medical records, and other records used to make decisions regarding a patient.

There are *four* separate grounds for permitted denials of an Amendment Request.

1. We may deny a patient's Amendment Request if we determine that the PHI was not created by our Practice, unless the patient provides to us a reasonable basis to believe that the originator of the PHI is no longer able to act on the requested amendment.

2. We may deny a patient's Amendment Request if we determine that the PHI is not part of a Designated Record Set.
3. We may deny a patient's Amendment Request if we determine that the PHI is accurate and complete.
4. We may deny a patient's Amendment Request if we determine that the PHI would not be available for inspection under the patient's HIPAA right to inspect and copy PHI (refer to policy P2.1).

An Amendment Request must be made in writing and must provide a reason to support the requested amendment (refer to form F2.2A). The Practice has 60 days to respond to such a request, but may seek an additional 30-day extension.

If the Practice grants an Amendment Request it must make the appropriate amendment to the PHI that is the subject of the request for amendment. The Practice must also inform the patient that the requested amendment has been accepted. The Practice, with the consent of the patient, must also inform others about the accepted amendment, including persons whom the patient identifies as having received the PHI subject to the amendment and persons the Practice knows have such PHI and may have relied or could foreseeably rely on it to the detriment of the patient.

If the Practice denies an Amendment Request it must:

- send a timely written denial to the patient, and
- explain the basis for the denial and explain that the patient may submit a statement of disagreement or complain to the Practice or Secretary of HHS about the denial.

If the patient submits a statement of disagreement, the Practice may prepare its own written rebuttal.

If a statement of disagreement is submitted, the Practice must include all materials related to the Amendment Request and its denial with any subsequent disclosure of PHI to which the disagreement relates. If no statement of disagreement is submitted, the patient may still request the Practice to include the Amendment Request and the Practice's denial with subsequent disclosures.

If the Practice is informed by another covered entity about an amendment to an individual's PHI, the Practice must amend the affected PHI in its own Designated Record Sets and notify the individual about the amendment.

Accounting
P2.3

It is our Practice's policy to comply with the Privacy Rule regarding a patient's right to receive an accounting of disclosures of PHI made by our Practice in the 6-year period preceding the date on which the accounting is requested. Such an accounting does not include disclosures:

- to carry out treatment, payment, or health care operations;
- to the patient who is the subject of the disclosed PHI;
- pursuant to a HIPAA-compliant authorization;
- for a facility directory or to persons involved in the patient's care, or for other notification purposes;
- of "Limited Data Set" data in compliance with our Limited Data Set Policies and Procedures (P1.11);
- as "Incidental Disclosures" in compliance with our policies and procedures for incidental disclosures;
- for national security or intelligence purposes;
- to correctional institutions or law enforcement officials having lawful custody of a patient; or
- made prior to April 14, 2003.

A request for an accounting must be made in writing (refer to form F2.3A). The Practice has 60 days to respond to such a request, unless it seeks a 30-day extension.

An accounting must include the following information: (1) the date of the disclosure; (2) the name of the entity or person receiving the information and, if known, the address

of the entity or person; (3) a brief description of the PHI disclosed; and (4) a brief statement of the purpose of the disclosure. Special rules apply for summarizing multiple disclosures to the same person or entity for the same purpose and for providing summary information about high-volume disclosures made for research purposes that do not require an authorization (refer to policy PP2.3).

The Practice must provide the first accounting to a patient in any 12-month period without charge. Thereafter, the Practice may impose a reasonable cost-based fee for each subsequent request within the same 12-month period, so long as it informs the patient in advance of the fee.

Our Practice may temporarily suspend a patient's right to receive an accounting of disclosures that were made to a health oversight agency or a law enforcement official. The length of such a temporary suspension will depend on whether the request for the suspension by the agency or official was made in writing or orally, as specified in the Privacy Rule.

Alternative Communications P2.4

It is our Practice's policy to accommodate reasonable requests by patients to receive communications of PHI from our Practice by alternative means or at alternative locations.

Such accommodation is subject to the following conditions:

- It is our policy to require that a patient make an Alternative Communications Request in writing.
- Our Practice may, when appropriate, condition its accommodation of an Alternative Communications Request on receiving information as to how payment will be handled.
- Our Practice may, when appropriate, condition its accommodation of the patient's Alternative Communications Request on the patient's specifying an alternative address or other means of contact.

Our Practice will not require a patient to explain the basis for an Alternative Communications Request as a condition of our accommodating the request.

Further Restrictions P2.5

It is our Practice's policy to permit a patient to request that our Practice agree to additional restrictions that go beyond what the Privacy Rule requires for uses and disclosures of PHI for treatment, payment, and health care operations. A patient may also request further restrictions for "opt-out" disclosures to family and friends involved in the patient's care. Such requests are called "Further Restriction Requests."

Our Practice is not required to agree to a Further Restriction Request. It is our policy generally not to agree to Further Restriction Requests. We will only agree to such requests when exceptional circumstances exist, when the Practice can reasonably accommodate the request, and when the Privacy Official (or an authorized physician) determines that we should agree to the request.

If our Practice agrees to a Further Restriction Request, we must document and comply with that agreement. Even if our Practice agrees to a Further Restriction Request, that agreement is not effective under the Privacy Rule to prevent uses or disclosures: (1) to the patient, (2) for facility directories, (3) for any "public purpose" disclosure (defined in P1.8), or (4) to treat the patient in an emergency.

If our Practice agrees to a Further Restriction Request, the agreed restriction can only be terminated if: (1) the patient agrees to or requests the termination in writing; (2) the patient orally agrees to the termination and the oral agreement is documented; or (3) the Practice informs the patient that it is terminating the agreement to the restriction, except that such termination is only effective with respect to PHI created or received after the Practice has informed the patient of the termination of the restriction.

Complaints P2.6

It is the Practice's policy to provide a process whereby individuals may make complaints concerning the Practice's privacy policies and procedures, compliance with those policies and procedures, and compliance with the requirements of the HIPAA Privacy Rule. The

Practice acknowledges that documenting and responding to privacy complaints is an important aspect of monitoring the Practice's compliance efforts with respect to the privacy of health information.

Any staff member who is presented with a privacy complaint by any person should refer the individual to the Privacy Official or contact who will document the complaint on the Privacy Complaint Form (F2.6A). The Privacy Official will respond, in writing, after the Practice has reviewed and investigated the complaint.

All Privacy Complaint Forms and any other documentation related to a privacy complaint, the investigation, or the disposition of the complaint shall be kept in the Privacy Official's files for such length of time as is required under the policy and procedure for Documentation (PP3.4).

Communications that are subject to the attorney-client privilege shall be maintained as directed by legal counsel, including in separate files as appropriate.

PRIVACY MANAGEMENT

Introduction

Managing the Practice's HIPAA compliance comes with many administrative tasks. This set of policies and procedures addresses the management and administrative aspects of protecting patient privacy.

General Policy
P3.0

It is our policy to comply with administrative requirements of the Privacy Rule as further detailed below. If you have questions, contact the Privacy Official.

Privacy Official/Privacy Contact
P3.1

As required by the HIPAA Privacy Rule, our Practice has designated a Privacy Official or contact who is responsible for developing and implementing the privacy policies and procedures of our Practice. The designation is as follows:

Privacy Official Name: _____

Effective Date of Appointment: _____

Our Privacy Official is also designated as the contact person who is responsible for receiving complaints and who will provide further information about matters covered by our Practice's NPP.

Notice of Privacy Practices—Development and Distribution
P3.2

It is our policy to provide adequate notice of:

- the uses and disclosures of PHI that may be made by the practice,
- an individual's right with respect to PHI, and
- the Practice's legal duties with respect to PHI.

The Practice will not use or disclose PHI in a manner inconsistent with the NPP.

The NPP will be distributed to the following persons at the following times:

Make the NPP available to . . .	**when . . .**
■ persons with whom we have a direct treatment relationship	no later than the first time of service delivery after April 14, 2003; or as soon as reasonably practicable after an emergency treatment situation
■ persons with whom we have an indirect treatment relationship	upon request
■ any person, whether a patient or not	upon request
■ individuals who first receive health care service electronically	automatically and simultaneously in response to the individual's first request for service
■ individuals who first receive health care service by phone	by mail on the day that service by phone was provided

Our NPP must contain certain information specified by the Privacy Rule. The NPP that will be used for our Practice is Notice of Privacy Practices Form (F3.2A), as it may be amended with the approval of the Privacy Official.

If we maintain a Web site about our Practice, we will post the NPP prominently on our Web site. We will also post the NPP prominently at each physical treatment delivery site that we maintain.

Where the Practice has a direct treatment relationship with a patient, the patient will be asked to acknowledge his or her receipt of our NPP.

Documentation regarding the NPP should also be maintained in compliance with the policy and procedure for Documentation (P3.4).

Policies and Procedures
P3.3

It is our policy to implement policies and procedures with respect to PHI that are reasonably designed to ensure compliance with the standards, implementation specifications, or other requirements of the HIPAA Privacy Rule. These policies and procedures shall also be consistent with applicable state law and other laws that are not preempted by HIPAA.

All policies and procedures will be documented in either written or electronic format. Documentation of policies and procedures will be in compliance with the policy and procedure for Documentation (P3.4).

Changes to the Practice's policies and procedures will be made when necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of the HIPAA Privacy Rule. When such changes in the law occur, the Practice will promptly revise and implement the affected policy or procedure using the Policy/Procedure Modification Form (F3.3B).

When revisions to the Practice's policies and procedures affect a practice stated in the NPP (F3.2A), the NPP must be revised accordingly. Revisions to the NPP will be made in accordance with Notice of Privacy Practices—Development and Distribution (P3.2). The effective date of a revised policy and procedure may not be prior to the effective date of the revised NPP.

The Practice hereby adopts the policies and procedures in this Chapter 2 as of the effective date specified below.

Adopted by: _____ (print name and title)

Signature: _____

Date: _____

Effective Date of Chapter 2 Policies and Procedures (April 14, 2003, unless otherwise specified): _____

Documentation
P3.4

It is our policy to comply with the documentation requirements contained in the HIPAA Privacy Rule.

Where the Privacy Rule requires a communication to be in writing, our Practice must maintain a written or electronic copy as documentation.

If an action, activity, or designation is required by the Privacy Rule to be documented, our Practice must maintain a written or electronic record of that action, activity, or designation.

Our Practice must maintain the policies and procedures required under the Privacy Rule in written or electronic form.

Our Practice will maintain the required documentation for 6 years from the later of the date the record was created or the date when the record was last in effect.

We will keep records and submit compliance reports, in such time and manner containing such information, as the Secretary of HHS may determine to be necessary to enable HHS to determine whether we have complied or are complying with the Privacy Rule.

We will permit access by HHS during normal business hours to our facilities, books, records, accounts, and other sources of information that are pertinent to the Secretary's determining compliance with the Privacy Rule. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, we must permit access by the Secretary at any time and without notice.

Workforce Training
P3.5

It is the Practice's policy to train all members of its workforce on the policies and procedures with respect to PHI as necessary and appropriate for the members of the workforce to carry out their functions within the Practice. "Workforce" members include employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Practice, is under the direct control of the Practice, whether or not they are paid by the Practice. Training will also be provided on any material changes in the

Practice's policies and procedures. Training will be documented as stated in the policy and procedure on Documentation (P3.4).

Internal Sanctions
P3.6

Our Practice's policy is to take disciplinary action (Internal Sanctions), if appropriate and as approved by our President or governing board (or other person designated by our president or governing board to take action), against any member of our workforce who has violated our Practice's privacy policies and procedures or HIPAA or state privacy law requirements.

As required by the Privacy Rule, no Internal Sanctions will be applied against whistleblowers, workforce member crime victims, or others by reason of conduct that is in good faith and protected from retaliation.

Circumstances that might give rise to a need for Internal Sanctions will be reviewed and investigated by the Privacy Official, or by another person designated by the Privacy Official, the president of our Practice, or our governing board, as appropriate, to "stand in the shoes" of the Privacy Official if he or she is absent or unable to act. The Privacy Official or the designated person may choose to consult with counsel for our Practice. The final decision regarding Internal Sanctions will be made by an individual (Review Official) appointed by the president of our Practice or our governing board, as appropriate to the severity of the issue, the employees or workforce members involved, and the structure of our Practice.

Business Associates also may be reviewed under the policies and procedures for Internal Sanctions.

Mitigation
P3.7

Our Practice will mitigate, to the extent practicable, any harmful effect that is known to the Practice of a use or disclosure of PHI by the Practice or its Business Associates in violation of the Practice's privacy policies and procedures or in violation of requirements of the Privacy Rule.

Any employee or workforce member may report to the Privacy Official or Practice management the employee's concerns or questions regarding whether our Practice and its workforce are complying with our privacy policies and procedures or applicable legal requirements.

The Privacy Official, the president of our Practice, and our governing board will be responsible for responding to such complaints, inquiries, or concerns, including determining and implementing mitigation where warranted.

No Retaliation
P3.8

It is our Practice's policy to not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient for the exercise of any rights under the Privacy Rule, including filing a complaint.

It is our Practice's policy to not intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient or other person for:

- Filing a complaint with the Secretary of HHS;
- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or
- Opposing any act or practice made unlawful by the Privacy Rule, provided the patient or other person (1) has a good faith belief that the practice is unlawful and (2) the manner of opposition is reasonable and does not involve the disclosure of PHI in violation of the Privacy Rule.

No Waiver
P3.9

It is our Practice's policy that we will not require an individual to waive his or her rights under the Privacy Rule, including the right to make a complaint to the Secretary of HHS, as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.

Safeguards
P3.10

Our Practice's policy is to document and implement appropriate administrative, technical, and physical Safeguards to protect against reasonably anticipated (1) threats or hazards to the security or integrity of PHI, and (2) unauthorized uses or disclosures of PHI in violation of the Privacy Rule or our Practice's privacy policies and procedures.

Safeguards implemented by our Practice will include assigned responsibility for managing and supervising the use of security measures to protect data and workforce-member conduct relating to data security, as well as policies and procedures that protect PHI from unauthorized access, use, or disclosure. Policies and procedures implemented by our Practice will be directed to establishing administrative processes, limiting physical access, and providing technical mechanisms to achieve the following with respect to PHI:

- Manage the routine and nonroutine receipt, use, or disclosure of PHI;
- Establish and maintain the integrity of PHI received, stored, used, or disclosed by the Practice;
- Provide for verifiable and secure transmission of PHI;
- Provide for access to and protection of PHI in an emergency situation;
- Control access to facilities, storage locations, storage media, computer work stations, networks, and actual PHI;
- Monitor activity relating to access, use, and disclosure of PHI;
- Identify and correct abnormalities, weaknesses, or malfunctions in computer or other data access, manipulation, or transmission systems;
- Identify and remedy privacy breaches; and
- Provide for ongoing assessment and improvement of existing protections.

Our Practice's decisions about implementing Safeguards will be guided by a risk analysis that balances the anticipated direct and indirect costs of a particular Safeguard against the anticipated benefits and the likelihood and severity of the threat the Safeguard is intended to prevent. Our assessment of the costs of a safeguard will include measures of its effect on (a) efficient treatment practices; (b) quality of patient care; and (c) administrative burden of compliance. Where available and appropriate, our Practice also may take advantage of Safeguards available from vendors.

The Quick Reference Guide in Chapter 1, Section 1.2, contains examples of Safeguards of common application.

chapter 3

Phase II Policies and Procedures

HOW TO USE THIS CHAPTER

Introduction

Congratulations! You have adopted and implemented Phase I policies and procedures. You have "HIPAA Light" under control. Now you are ready for "HIPAA Heavy!" These Phase II policies and procedures cover the same topics as Phase I—but more detail is provided to guide compliance decisions.

The Phase II policies and procedures also contain forms to help you implement the policies and procedures.

Phase II Policies and Procedures

Phase II policies and procedures are grouped into the same categories as Phase I Policies and Procedures and follow the same numbering system, except that Phase II Policies and Procedures have the "PP" prefix.

Policy/Procedure	Description	Section Number
PHI Permissions	Restrictions on using and disclosing patient information.	PP1
Patient Rights	Patient rights with respect to patient information.	PP2
Privacy Management	Policies relating to the administrative aspects of protecting patient privacy.	PP3

Adopt Your Own Modifications

Adopt policies and procedures to fit your Practice's needs. HIPAA compliance is not "one size fits all." These policies and procedures are not the final word on what your Practice should do. Review these policies and procedures with your lawyer. Understand how laws in your state, and other laws (federal, tribal, local, etc.) can affect what you can and cannot do with patient information. Think about how to make HIPAA implementation work in *your* Practice.

Maintain Your Policies and Procedures

HIPAA requires your Practice to document its policies and procedures. This book can serve as the place to keep your documentation. PP3.3 describes in more detail how to use this chapter to adopt your more detailed HIPAA policies and procedures.

INDEX OF PHASE II POLICIES AND PROCEDURES

Policy/Procedure	Section Number
PHI Permissions	
General Policy	PP1.0
Permissions	
Required Disclosures	PP1.1
Disclosures to the Patient	PP1.2
Our Treatment, Payment, Operations	PP1.3
Others' Treatment, Payment, Operations	PP1.4
Operations of Organized Health Care Arrangement	PP1.5
Family, Friends, and Disaster Relief Organizations	PP1.6
Incidental Disclosures	PP1.7
Public Purpose	PP1.8
Authorization	PP1.9
De-Identification	PP1.10
Limited Data Set	PP1.11
Special Requirements	
Verification	PP1.12
Minimum Necessary	PP1.13
Business Associates	PP1.14
Personal Representatives	PP1.15
Marketing	PP1.16
Psychotherapy Notes	PP1.17
Consistent with Notice of Privacy Practices	PP1.18
Consistent with Other Documents	PP1.19
Consent (State or Other Law)	PP1.20
Patient Rights	
General Policy	PP2.0
Access	PP2.1
Amendment	PP2.2
Accounting	PP2.3
Alternative Communications	PP2.4
Further Restrictions	PP2.5
Complaints	PP2.6
Privacy Management	
General Policy	PP3.0
Privacy Official/Privacy Contact	PP3.1
Notice of Privacy Practices—Development and Distribution	PP3.2
Policies and Procedures	PP3.3
Documentation	PP3.4
Workforce Training	PP3.5
Internal Sanctions	PP3.6
Mitigation	PP3.7
No Retaliation	PP3.8
No Waiver	PP3.9
Safeguards	PP3.10

PHI USE AND DISCLOSURE PP1.0

Introduction

This policy provides an overview of our Practice's policies and procedures regarding use and disclosure of protected health information (PHI) under the HIPAA Privacy Rule. For more background basics on what the Privacy Rule requires regarding patient privacy protection, read Appendix A, Privacy Rule Summary, Lesson 5.

General Policy

Our policy is to use and disclose PHI only in compliance with the HIPAA Privacy Rule and other applicable requirements. This means that three things must happen.

- Step 1: Confirm that the use or disclosure fits under an applicable Permission.
- Step 2: Confirm that the use or disclosure complies with the conditions of that Permission.
- Step 3: Determine what Special Requirements the use or disclosure triggers, and confirm compliance. These include Special Requirements under the Privacy Rule and under other privacy laws (including applicable state laws).

What is PHI?

These policies and procedures only apply to "protected health information" or PHI. Follow these steps to determine whether information is PHI.

Step 1: Is the Information Health Information?

Determine whether the information requested or to be used or disclosed is consistent with the following:

- Created or received by a health care provider, health plan, employer, or health care clearinghouse; *and*
- Relates to the past, present, or future diagnosis or treatment of a physical or mental condition; **or**
- Relates to a payment claimed or paid for a past, present, or future diagnosis or treatment of a physical or mental condition.

Information that meets the above criteria is health information and may be PHI if it is individually identifiable. **Proceed to Step 2** to determine whether the information is individually identifiable.

Information that does not meet any of the above criteria is not PHI and is not subject to these policies and procedures unless otherwise noted.

Step 2: Is the Information Individually Identifiable?

Determine whether the information requested identifies or reasonably could be used to identify an individual by determining whether it contains any of the following identifiers of the individual or of relatives, employers, or household members of the individual:

- Name
- Geographic subdivisions smaller than a state, except for initial three-digit zip codes containing more than 20,000 people
- Any element of a date
- Telephone numbers
- Fax numbers
- Electronic mail addresses

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers, including license plate numbers
- Device identifiers and serial numbers
- URLs
- IP addresses
- Biometric identifiers including finger and voice prints
- Full-face photographic images and comparable images
- Any other identifying number, characteristic, or code

Information that contains one or more of the above identifiers may be individually identifiable, and unless the Privacy Official has instructed otherwise, should be treated as PHI.

Information that does not contain any of the above identifiers constitutes De-Identified Information and is not PHI (assuming our Practice does not have actual knowledge that the information could be used to identify an individual). See De-Identification (PP1.10).

Permissions

To determine whether a use or disclosure of PHI complies with our policies and procedures, the first step is to determine the applicable Permission for the use or disclosure. No use or disclosure of PHI may occur unless it fits within an applicable Permission and meets the conditions of that Permission.

The following is the list of our policies for Permissions for a use or disclosure of PHI.

Permission	Section
General Policy	PP1.0
Required Disclosures	PP1.1
Disclosures to the Patient	PP1.2
Our Treatment, Payment, Operations	PP1.3
Others' Treatment, Payment, Operations	PP1.4
Operations of Organized Health Care Arrangement	PP1.5
Family, Friends, and Disaster Relief Organizations	PP1.6
Incidental Disclosures	PP1.7
Public Purposes	PP1.8
Authorization	PP1.9
De-Identification	PP1.10
Limited Data Set	PP1.11

First, identify the applicable Permission. Then, confirm that the conditions of that Permission are met. If not, confirm whether any other Permission may apply and whether conditions of the other Permission can be met. In most cases, an Authorization is a Permission of last resort, but it is a Permission that may nonetheless work.

Special Requirements

Even if after you identify the applicable Permission and determine that the conditions of that Permission are met, other requirements may still apply. We call these Special Requirements.

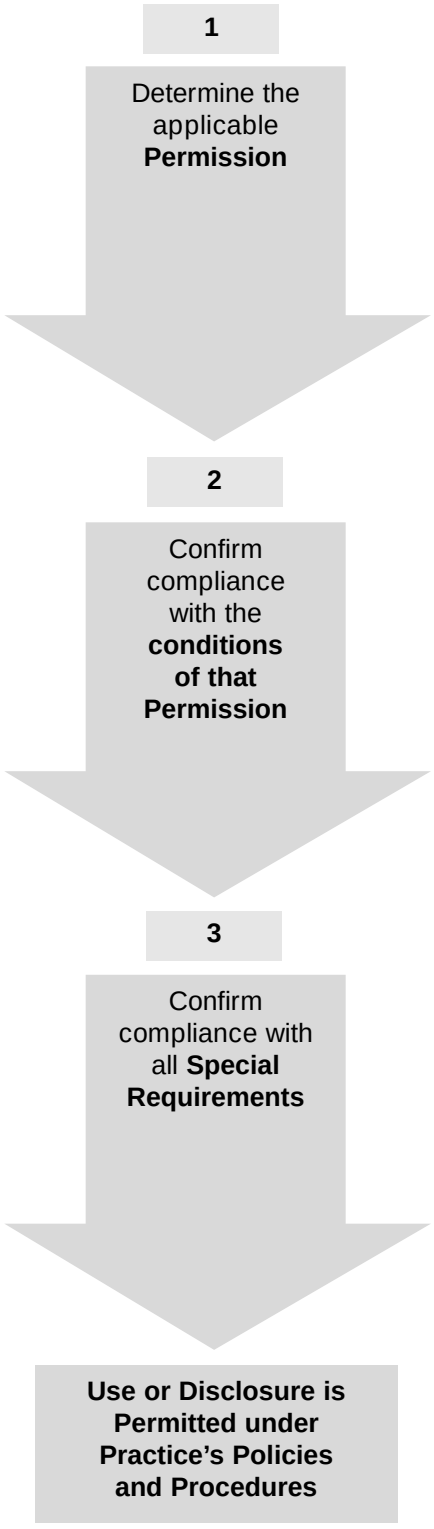
The following is a list of our policies and procedures for these Special Requirements.

Special Requirements	Section
Verification	PP1.12
Minimum Necessary	PP1.13
Business Associates	PP1.14
Personal Representatives	PP1.15
Marketing	PP1.16
Psychotherapy Notes	PP1.17
Consistent with Notice of Privacy Practices	PP1.18
Consistent with Other Documents	PP1.19
Consent (State and Other Laws)	PP1.20

Note

The use or disclosure must meet the conditions of all applicable Special Requirements. This is different from the Permission compliance step, in which the use or disclosure only needs to comply with one type of Permission.

PHI Permissions Process Chart



PERMISSIONS: REQUIRED DISCLOSURES PP1.1

General Policy	It is our Practice's policy to disclose PHI as required by the Privacy Rule.
Scope of Policy	This policy applies to disclosures of PHI required by the Privacy Rule, including those to the patient and those required by HHS. PP1.8 describes our Practice's policies regarding Uses and Disclosures for a Public Purpose, including disclosures required by laws other than the Privacy Rule.
Disclosures to Patients	It is our Practice's policy to provide a patient, when requested, access to his or her own PHI or an accounting of disclosures of his or her PHI, when required by the Privacy Rule. PP2.1 describes our Practice's policies for responding to Access Requests. PP2.3 describes our Practice's policies relating to Disclosure Accounting Requests. PP2.3 describes our Practice's policies for tracking and logging disclosures that are subject to the patient's right to make Disclosure Accounting Requests.
Disclosures to HHS	It is our Practice's policy to permit HHS access to our facilities, books, records, accounts, and other sources of information, including PHI, that are relevant to HHS determining our compliance with the Privacy Rule. It is our policy generally to permit such access during normal business hours; however, if HHS determines that circumstances requiring immediate action exist, we will permit HHS such access at any time and without notice.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PERMISSIONS: DISCLOSURES TO THE PATIENT PP1.2

Introduction

The Privacy Rule permits the Practice to disclose PHI to the patient who is the subject of such information.

General Policy

The Practice may disclose PHI to an individual who is the subject of such information. The Practice also may generally disclose such information to an individual's personal representative; however, exceptions may apply if the individual is an unemancipated minor, or if the Practice believes that the individual has been abused or neglected by the personal representative or that such disclosure may otherwise endanger the individual.

> **Note**
>
> Disclosures to the patient of the patient's PHI are not subject to the minimum necessary requirements described in PP1.13, Minimum Necessary.

Other Policies and Procedures

PP1.1, Required Disclosures, describes our Practice's policies and procedures regarding disclosures to the patient that are required by the Privacy Rule.

PP1.15, Personal Representatives, describes our Practice's policies and procedures regarding disclosures to a patient's personal representative.

PP1.12, Verification, describes our Practice's policies and procedures regarding verifying the identity of someone who requests PHI.

Contact Person

Our Privacy Official is designated to be the contact person for questions relating to disclosures to the patient of his or her own PHI and our compliance with the Privacy Rule related to such disclosures.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PERMISSIONS: OUR TREATMENT, PAYMENT, OPERATIONS PP1.3

Overview

Introduction

The HIPAA Privacy Rule permits our Practice to use or disclose PHI for our Treatment, Payment, and Health Care Operations (TPO) *without any consent or authorization from the patient* except where an Authorization is specifically required or other Special Requirements apply, such as when PHI is used for Marketing, or when the PHI includes Psychotherapy Notes, or when state law requires a consent from the patient.

The scope of the TPO permission is principally determined by the Privacy Rule's definitions of Treatment, Payment, and Health Care Operations.

How This Policy/ Procedure Works

Use this policy to confirm whether a PHI use or disclosure falls within Our Treatment, Payment, Operations Permission.

Contact Person

Our Privacy Official is designated to be the contact person for questions, suggestions, or complaints relating to use or disclosure of PHI for our Treatment, Payment, or Health Care Operations and our compliance with the Privacy Rule related to use or disclosure of PHI for our Treatment, Payment, or Health Care Operations.

Note

In PP3.1, Privacy Official/Privacy Contact, we designate the person who is our Privacy Official. That policy also contains the description of the Privacy Official's responsibilities.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PERMISSIONS: OUR TREATMENT, PAYMENT, OPERATIONS PP1.3

General Policy

General Policy

Our Practice's policy is to use and disclose PHI for our Treatment, Payment, and Health Care Operations, *without consent or authorization from the patient*, as permitted by the Privacy Rule, except where an Authorization is specifically required or other special requirements apply, such as when PHI is used for Marketing, or when the PHI includes Psychotherapy Notes, or when state law requires a consent from the patient.

Definitions

Health Care Operations. The definition of health care operations is long (*see* Glossary for full definition). It includes a wide range of activities that make up the typical functions of a medical practice, including quality assessment and improvement, protocol development, case management, peer review, health plan performance evaluation, training programs, legal and auditing services, and other managerial and administrative functions. The definition of Health Care Operations also includes due diligence for merger, transfer, or consolidation of our Practice, as well as certain uses for fundraising for the benefit of our Practice.

Payment. Refers to:

1. The activities undertaken by:

(i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or

(ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and

2. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:

(i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;

(ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following PHI relating to reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of health care provider and/or health plan.

Treatment. Refers to the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

Procedure

To evaluate whether a disclosure of PHI is being made for Our Treatment, Payment, or Health Care Operations, go to PP1.3, Our Treatment, Payment, Operations—Index of Procedures.

PERMISSIONS: OUR TREATMENT, PAYMENT, OPERATIONS PP1.3

Index of Procedures

Introduction

Whether an activity comes within the TPO permission is determined by the definitions of Treatment, Payment, and Health Care Operations.

The Privacy Official will assist as appropriate in the analysis involved in Step 2.

Inquiry/Action Steps

Use these procedures in connection with our Practice's Treatment, Payment, or Health Care Operations:

Step	Inquiry/Action
1	Determine whether the PHI is to be used or disclosed for our Treatment, Payment, or Health Care Operations.
2	Determine whether Special Requirements apply.

Step1: Determine Whether the PHI Is to be Used or Disclosed for Our Treatment, Payment, or Health Care Operations

Introduction

The terms Treatment, Payment, and Health Care Operations have broad definitions under HIPAA and include a range of uses and disclosures related to treating patients, securing reimbursement, and conducting health care operations in our Practice. Treatment, Payment, and Health Care Operations represent a majority of our Practice's disclosures of PHI. Accordingly, the Privacy Official and other employees of the Practice should invest the time to understand the full definitions here and in the Glossary.

Step 1.1

Review Quick Reference Guide

Review the Quick Reference Guide to see if a task or function is listed as permitted for our Treatment, Payment, and Health Care Operations. The Privacy Official will use the Quick Reference Guide to maintain and update a list of activities typically undertaken by the Practice for our Treatment, Payment, and Health Care Operations (Quick Reference Guide).

Step 1.2

Is the PHI to be Used and Disclosed for Treatment, Payment, or Health Care Operations?

If the intended use or disclosure of PHI is listed in the Quick Reference Guide as permitted for Our Treatment, Payment, or Health Care Operations, and you do not have any questions, you may proceed to Step 2.

If the intended use or disclosure of PHI is not in the Quick Reference Guide, or if you have questions, proceed to Steps 1.3 through 1.5 to determine whether the intended use of PHI is for Treatment (Step 1.3), Payment (Step 1.4), or Health Care Operations (Step 1.5). A use or disclosure only needs to fit in one category, so first review the category you think most closely applies.

Step 1.3

Using Definition of Treatment, Is the Intended Use for Treatment?

Step A If the intended use of PHI is not in the Quick Reference Guide, determine whether the intended use of PHI is for a purpose in the definition of Treatment, ie,

- providing, coordinating, and/or managing health care and related services;
- consultations between providers about patient care; or
- referrals of patients for care from one health care provider to another.

Step B If yes, **proceed to Step 2.**

Step C If no, **proceed to Step 1.4.**

Step 1.4

Using Definition of Payment, Is the Intended Use for Payment?

Step A If the intended use of PHI is not in the Quick Reference Guide, determine whether the intended use of PHI is for an activity or purpose undertaken by our Practice to obtain or provide reimbursement for the provision of health care, including:

- ■ determinations of eligibility or coverage;
- ■ risk adjusting amounts due based on enrollee health status and demographic characteristics;
- ■ billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing;
- ■ review of health care activities with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- ■ utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and
- ■ disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name and address, date of birth, social security number, payment history, account number, and name and address of the health care provider and/or health plan.

Step B If yes, **proceed to Step 2.**

Step C If no, **proceed to Step 1.5.**

Step 1.5

Using the Definition of Health Care Operations, Is the Intended Use for Our Health Care Operations?

Step A If the intended use of PHI is not in the Quick Reference Guide, determine whether the intended use of PHI is for an activity or purpose in the definition of Health Care Operations set forth below.

Health Care Operations would include any of the following activities by our Practice to the extent related to our covered functions:

- ■ conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, and related functions that do not include treatment;
- ■ reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance and health plan performance; conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; and accreditation, certification, licensing, or credentialing activities;
- ■ underwriting, premium rating, and other activities relating to the creation, renewal or replacement of a contract of health insurance or health benefits; and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care;
- ■ business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating our Practice, including formulary development and administration and development or improvement of methods of payment or coverage policies; and
- ■ business management and general administrative activities of our Practice, including, but not limited to,
- □ management activities relating to implementation of and compliance with HIPAA;

- ☐ customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that PHI is not disclosed to such policy holder, plan sponsor, or customer;
- ☐ resolution of internal grievances;
- ☐ sale, transfer, merger, or consolidation of all or part of our Practice with another covered entity, or an entity that following such activity will become a covered entity, and due diligence related to such activity; and
- ☐ creating de-identified health information or a limited data set and fundraising for the benefit of our Practice.

Step B If yes, **proceed to Step 2.**

Step C If no, **proceed to Step 1.6.**

Step 1.6

Consult with Privacy Official

If you cannot determine if the use or disclosure is for Treatment, Payment, or Health Care Operations, consult with the Privacy Official (or determine whether any other Permission applies). **Proceed to Step 1.7.**

Step 1.7

Privacy Official Determination

Step A Where there is uncertainty, the Privacy Official is responsible for making the final judgment concerning whether a use or disclosure of PHI by our Practice is for our Treatment, Payment, or Health Care Operations.

Step B If the Privacy Official determines that the use or disclosure of PHI is for Treatment, Payment, or Health Care Operations, **proceed to Step 2.**

Step C If the Privacy Official determines that the use or disclosure of PHI is not for Treatment, Payment, or Health Care Operations, **proceed to Step 1.8.**

Step 1.8

Secure an Authorization

If the intended use or disclosure of PHI does not fit within this permission for Our Treatment, Payment, Operations, and if no other Permission applies (see PP1.1 through PP1.11), **proceed to Authorization, PP1.9,** and secure an Authorization from the patient for our Practice to use or disclose the PHI for the intended use.

Step 2: Confirm Compliance with Applicable Special Requirements

---

Introduction

Even if the use or disclosure of PHI is for Treatment, Payment, or Health Care Operations, the procedures in this Step 2 should be followed to determine whether any Special Requirements apply to the use or disclosure of PHI by our Practice and to confirm compliance with any applicable Special Requirements.

Step 2.1

Do Special Requirements Apply?

The Quick Reference Guide briefly identifies Special Requirements that may apply to various PHI uses and disclosures, including the Minimum Necessary amount of information. If a use or disclosure is not on the list, or if you have questions about a use or disclosure that is on the list, review additional policies and procedures listed below. Review the following policies and procedures as appropriate to determine whether one or more of these Special Requirements applies to a particular use or disclosure of PHI by our Practice.

- Verification, PP1.12
- Minimum Necessary, PP1.13
- Business Associates, PP1.14
- Personal Representatives, PP1.15
- Marketing, PP1.16
- Psychotherapy Notes, PP1.17
- Consistent with Notice of Privacy Practices, PP1.18

- Consistent with Other Documents, PP1.19
- Consent, PP1.20

Step 2.2

If Yes, Use Applicable Policies and Procedures

If one or more of the Special Requirements applies, proceed to review and comply with the applicable Special Requirements policies and procedures before making the use or disclosure.

Step 2.3

If No, Proceed to Use or Disclose PHI

If none of the Special Requirements applies, you may proceed to use and disclose PHI for our Practice's Treatment, Payment, or Health Care Operations.

PERMISSIONS: OTHERS' TREATMENT, PAYMENT, OPERATIONS PP1.4

Overview

Introduction

The HIPAA Privacy Rule permits our Practice to use or disclose PHI *without any consent or authorization from the patient:*

- for the Treatment activities of another Health Care Provider;
- to another Health Care Provider or Covered Entity for the Payment activities of the entity receiving the PHI; and
- to another Covered Entity (including covered Health Care Providers) for Health Care Operations activities of the entity that receives the information, if our Practice and the other entity both have (or had) a relationship with the individual who is the subject of the PHI being requested, and the disclosure is:
  - (i) for a purpose related to (A) quality assessment and improvement, or (B) reviewing the competence of health care professionals and training more specifically described in paragraphs (1) and (2) of the definition of Health Care Operations (see Glossary); *or*
  - (ii) for the purpose of health care fraud and abuse detection or compliance.

Policies and Procedures

PP1.4 describes our policies and procedures relating to disclosure of PHI for Treatment, Payment, or Health Care Operations of another entity.

Contact Person

Our Privacy Official is designated to be the contact person for questions, suggestions, or complaints relating to disclosure of PHI for Treatment, Payment, or Health Care Operations of another entity and our compliance with the Privacy Rule related to use or disclosure of PHI for Treatment, Payment, or Health Care Operations.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PERMISSIONS: OTHERS' TREATMENT, PAYMENT, OPERATIONS PP1.4

General Policy

General Policy

Our Practice's general policy is to use and disclose PHI for the Treatment activities of Health Care Providers, for Payment activities of other Health Care Providers or other Covered Entities, and for some Health Care Operations of other Covered Entities (including covered Health Care Providers), without consent or authorization from the patient, as permitted by the Privacy Rule, except where an Authorization is specifically required.

An Authorization for certain uses and disclosures under Special Requirements may apply, such as when PHI is used for Marketing, or when the PHI includes Psychotherapy Notes.

Definitions

Health Care Operations. The definition of Health Care Operations that applies in most situations is long (see Glossary for full definition). However, *only a limited subset of that definition applies for purposes of permitted uses and disclosures of Health Care Operations of others.* Only the following types of Health Care Operations are included in the Permission for the use or disclosure of PHI for the Health Care Operations of others:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities.
3. In addition, our Practice may use or disclose PHI for purposes of others' health care fraud and abuse detection or compliance activities.

Note

Our Practice may not use or disclose PHI for purposes of another entity's underwriting, legal and auditing services, and other managerial and administrative functions.

Payment. Payment is discussed in PP1.3, Our Treatment, Payment, Health Care Operations. The Privacy Rule definition of Payment is in the Glossary.

Treatment. Treatment is discussed in PP1.3, Our Treatment, Payment, Health Care Operations. The Privacy Rule definition of Treatment is in the Glossary.

Procedures

Use the Procedures described in Others' Treatment, Payment, or Health Care Operations—Index of Procedures, PP1.4, to determine whether a use or disclosure of PHI to another entity is permitted for that other entity's Treatment, Payment, or Health Care Operations.

PERMISSIONS: OTHERS' TREATMENT, PAYMENT, OPERATIONS PP1.4

Index of Procedures

Introduction

Analyzing PHI disclosure for Treatment, Payment, or Health Care Operations of another entity is a multi-step process.

Inquiry/Action Steps

Use the following steps to determine whether a use or disclosure of PHI is permitted for the Treatment, Payment, or Health Care Operations of another entity:

Step	Inquiry/Action
1	Determine whether the entity receiving the PHI is a Health Care Provider or a Covered Entity.
2	Determine whether the PHI is to be used or disclosed for another Health Care Provider's Treatment or Payment Activities or for another Covered Entity's Payment or Health Care Operations Activities.
3	Confirm compliance with applicable Special Requirements.

Note

A separate policy, PP1.5, describes our policies and procedures for uses or disclosures for the health care operations of an Organized Health Care Arrangement that we participate in.

Other Procedures

Use these other procedures as appropriate:

Our Treatment, Payment, Health Care Operations, PP1.3

Operations of Organized Health Care Arrangement, PP1.5

Authorization, PP1.9

Review the Quick Reference Guide

Step 1: Determine Whether the Entity Receiving the PHI Is a Health Care Provider or a Covered Entity

Introduction

Under the Privacy Rule, our Practice may disclose PHI to another Health Care Provider for its Treatment activities, to another Health Care Provider or another Covered Entity for its Payment activities, and to another Covered Entity (including a covered Health Care Provider) for some of its Health Care Operations. If the entity receiving the PHI is not a Health Care Provider or a Covered Entity, *the permission relating to TPO of others does not apply.*

Step 1.1

Determine Whether Receiving Entity is a Health Care Provider or a Covered Entity

Determine whether the intended recipient of the PHI is a Health Care Provider or a Covered Entity.

HIPAA Covered Entities are (1) health plans, (2) health care clearinghouses, and (3) health care providers, if the provider conducts any HIPAA transactions electronically (see Appendix A, Privacy Rule Summary). These terms are defined in the Glossary.

Step 1.2

If Recipient Is a Health Care Provider or Covered Entity

If the intended recipient of PHI is a Health Care Provider or a Covered Entity, **proceed to Step 2.**

Otherwise, **proceed to Step 1.3.**

Step 1.3

If Recipient Is Not a Health Care Provider or Covered Entity

If the intended recipient of PHI is not a Health Care Provider or a Covered Entity, *this PP1.4 does not apply.*

Step A Review other permissions for applicability (see PP1.1 through PP1.11).

Step B If no other permission applies, **proceed to Authorization, PP1.9.**

Also, **proceed to Step 3** to determine whether any special requirements apply.

Step 2: Determine Whether the PHI Is to be Used or Disclosed for the Other Entity's Treatment, Payment, or Health Care Operations

Introduction

The terms Treatment, Payment, and Health Care Operations have broad definitions under HIPAA and include a range of uses and disclosures related to treating patients, securing reimbursement, and conducting health care operations.

However, for purposes of permitted uses and disclosures of PHI for the Health Care Operations of others, only a part of the others' Health Care Operations may be taken into account—these are the Health Care Operations related to quality assessment and improvement, protocol development, case management, peer review, health plan performance evaluation, training programs, and similar activities. In addition, our Practice may use or disclose PHI for purposes of other Covered Entities' health care fraud and abuse detection or compliance activities.

This Permission in PP1.4 does not permit our Practice to use or disclose PHI for underwriting, legal and auditing services, and other managerial and administrative functions undertaken for the benefit of others.

Step 2.1

Review Quick Reference Guide for List of PHI Uses and Disclosures for Others' TPO

Using the Quick Reference Guide in Chapter 1, Section 1.2, of this book, the Privacy Official will create, update, and maintain a list of PHI uses and disclosures by the Practice for the benefit of others' Treatment, Payment, and Health Care Operations (using the more limited definition of Health Care Operations applicable for uses and disclosures of PHI for other Covered Entities' Health Care Operations).

Review the Quick Reference Guide to determine whether the intended use of PHI is:

- for Treatment activities of another Health Care Provider,
- for Payment activities of another Health Care Provider or another Covered Entity, or
- for permitted Health Care Operations of another Covered Entity (including a covered Health Care Provider).

If the intended PHI use or disclosure is identified as permitted for the Others' TPO, and you do not have any questions, **proceed to Step 3.**

If the intended use of PHI is not in the Quick Reference Guide, or if you have questions, **proceed to Steps 2.3 through 2.5** to determine whether the intended use of PHI is properly for another's Treatment (Step 2.2), Payment (Step 2.3), or permitted Health Care Operations (Step 2.4).

Note

If a recipient Health Care Provider is not a Covered Entity under HIPAA, the Permission to disclose for others' TPO does not apply to disclosures for the Health Care Operations of the non-Covered Entity Health Care Provider. Proceed next to consider the other Permission (Treatment, etc.) that you think most closely fits what you intend to do with the PHI.

Step 2.2

Is the Intended Use for Treatment?

Step A If the intended use of PHI is not in the Quick Reference Guide, determine whether the intended use of PHI is for a purpose listed in the definition of Treatment, ie,

- providing, coordinating, and/or managing health care and related services;
- consultations between providers about patient care; or
- referrals of patients for care from one health care provider to another.

Step B If yes, and if the intended recipient is a Health Care Provider, **proceed to Step 3.**

Step C If no, or if the intended recipient is a Covered Entity that is not a Health Care Provider, **proceed to Step 2.3.**

Step 2.3

Is the Intended Use for Payment?

Step A If the intended use of PHI is not in the Quick Reference Guide, determine whether the intended use of PHI is for an activity or purpose in the definition of Payment set forth below.

Payment means activities undertaken by a Covered Entity or a Health Care Provider to obtain or provide reimbursement for the provision of health care, including:

- determinations of eligibility or coverage;
- risk adjusting amounts due based on enrollee health status and demographic characteristics;
- billing, claims management, collection activities, obtaining payment under a contract for reinsurance, and related health care data processing;
- review of health care activities with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;
- utilization review activities, including precertification and preauthorization of services and concurrent and retrospective review of services; and
- disclosure to consumer reporting agencies of any of the following PHI relating to collection of premiums or reimbursement: name and address, date of birth, social security number, payment history, account number, and name and address of the health care provider and/or health plan.

Step B If yes, **proceed to Step 3.**

Step C If no, **proceed to Step 2.4.**

Step 2.4

Is the Intended Use for the Limited Types of Others' Health Care Operations That Qualify for This Permission?

Step A If the intended use of PHI is not in the Quick Reference Guide, determine whether the intended use of PHI is for an activity or purpose in the limited subset of Health Care Operations for purposes of the Permission for Health Care Operations of others.

Health Care Operations that fall within the Permission for Others' Health Care Operations include any of the following activities by another Covered Entity to the extent related to its covered functions:

- conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, population-based activities relating to improving health or reducing health care costs,

protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives, and related functions that do not include treatment;

- reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities; and
- health care fraud and abuse detection or compliance.

Step B If the use or disclosure of PHI is for another Covered Entity's permitted Health Care Operations, then determine:

- whether both our Practice and the requesting Covered Entity have, or have had, a relationship with the individual who is the subject of the PHI being requested; and
- whether the PHI pertains to such relationship.

Step C If both conditions in Step B are met, **proceed to Step 3**.

Step D If either condition in Step B is not met, or if the intended recipient is a Health Care Provider that is not a Covered Entity, **proceed to Step 2.5.**

Step 2.5

Consult with Privacy Official

If you cannot determine if the use or disclosure is for Treatment, Payment, or permitted Health Care Operations of others, consult with the Privacy Official. **Proceed to Step 2.6.**

Step 2.6

Privacy Official Makes Final Determination

Step A Where there is uncertainty, the Privacy Official is responsible for making the final judgment concerning whether a use or disclosure of PHI is for Treatment, Payment, or permitted Health Care Operations of others.

Step B If the Privacy Official determines that the use or disclosure of PHI is permitted for others' Treatment, Payment, or Health Care Operations, **proceed to Step 3.**

Step C If the Privacy Official determines that the use or disclosure of PHI is not permitted for others' Treatment, Payment, or Health Care Operations, **proceed to Step 2.7.**

Step 2.7

If the intended use or disclosure of PHI does not fit within this permission for Others' Treatment, Payment, Operations, and if no other permission applies (see PP1.1 through PP1.11), **proceed to Authorization, PP1.9,** and secure a proper Authorization from the patient for our Practice to use or disclose the PHI for the intended purpose.

Step 3: Determine Whether Special Requirements Apply

Introduction

Even if the use or disclosure of PHI is for Treatment, Payment, or permitted Health Care Operations of others, the procedures in this Step 3 should be followed to determine whether any Special Requirements applies to the intended use or disclosure of PHI.

Step 3.1

Review Special Requirements

Based on the terms of the following policies and procedures, determine whether one or more of these Special Requirements apply to an intended use or disclosure of PHI:

- Verification, PP1.12
- Minimum Necessary, PP1.13
- Business Associates, PP1.14
- Personal Representatives, PP1.15

- Marketing, PP1.16
- Psychotherapy Notes, PP1.17
- Consistent with Notice of Privacy Practices, PP1.18
- Consistent with Other Documents, PP1.19
- Consent (State or Other Law), PP1.20

Step 3.2

Confirm Compliance With Any Applicable Special Requirements

If none of the Special Requirements applies, or if applicable Special Requirements are met, proceed to use and disclose PHI for Treatment, Payment, or permitted Health Care Operations of others as intended.

If one or more of the Special Requirements applies, proceed to review the policies and procedures that apply and make the use or disclosure only in compliance with applicable policies and procedures.

PERMISSIONS: OPERATIONS OF ORGANIZED HEALTH CARE ARRANGEMENT PP1.5

Overview

Introduction

The HIPAA Privacy Rule permits covered entities that participate in an Organized Health Care Arrangement (OHCA) to disclose PHI about an individual to another covered entity that participates in the OHCA for any Health Care Operations activities of the OHCA. This gives such OHCA entities broader authority to share PHI for Health Care Operations with each other than non-OHCA entities.

OHCA List

The Privacy Official will list the participants (or classes of participants) in each OHCA in which our Practice participates on the OHCA List, Form F1.5, attached to this PP1.5. The Privacy Official may also maintain an OHCA section in the Quick Reference Guide in Chapter 1.

Policies and Procedures

PP1.4 describes our Practice's policies and procedures relating to use or disclosure of PHI for the Health Care Operations of others that are not participants in an OHCA. PP1.4 also permits use and disclosure of PHI for Treatment and Payment activities of others, including participants in an OHCA.

PP1.5 describes our Practice's policies and procedures relating to use or disclosure of PHI with participants in the OHCA for the Health Care Operations of the OHCA.

Contact Person

Our Privacy Official is designated to be the contact person for questions, suggestions, or complaints relating to use or disclosure of PHI to another participant in an OHCA.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PERMISSIONS: OPERATIONS OF ORGANIZED HEALTH CARE ARRANGEMENT PP1.5

General Policy

General Policy

It is our Practice's policy to recognize the special Privacy Rule Permission regarding an OHCA. The OHCA Permission allows for use and disclosure of PHI for all of the Health Care Operations of the OHCA rather than the limited definition of Health Care Operations generally permitted for others (see PP1.4).

Our Privacy Official will complete the OHCA List (Form F1.5) by listing or describing the participants of each OHCA in which our Practice participates. Our Practice may use and disclose PHI to other participants in the OHCA for all of the Health Care Operations activities of the OHCA.

Our practice will issue a joint Notice of Privacy Practices with other participants in the OHCA about use and disclosure of PHI for Health Care Operations of the OCHA as permitted by the Privacy Rule and as determined appropriate by our Privacy Official. See Notice of Privacy Practices—Development and Distribution, PP 3.2.

Definitions

Covered Entity. See Glossary.

Health Care Operations. The full definition applies, including underwriting, legal, and auditing services and other managerial and administrative functions. See Glossary.

Organized Health Care Arrangement. The Privacy Rule defines an Organized Health Care Arrangement as any one of the following five types of organizations or arrangements (the first two are most likely to apply to our Practice operations):

- a clinically integrated care setting where individuals usually receive care from more than one provider.
- an organized system of care in which more than one covered entity participates, and they: (1) hold themselves out to the public as a joint arrangement and (2) jointly conduct utilization review, quality assessment, or certain payment activities.
- a group health plan (but only with respect to certain individuals).
- a group health plan and one or more other group health plans, each maintained by the same plan sponsor.
- "same sponsor" group health plans and the insurance carriers or HMOs with respect to such plans (but only with respect to certain individuals).

The full definition is in the Glossary.

Procedure

Use this procedure to determine if a PHI disclosure is permitted under the OHCA Permission.

OHCA List

Our Practice's Privacy Official will complete OHCA Form F1.5 to identify each OHCA, if any, in which our Practice participates, the other participants in the OHCA, and the scope or boundaries of the joint activities of the OHCA.

Our Privacy Official should use the summary definition above and the full definition in the Glossary to determine if our Practice participates in an OHCA. The Privacy Official should consult with the Practice's legal counsel as appropriate in completing Form F1.5. **Proceed to Step 1.2.**

PERMISSIONS: OPERATIONS OF ORGANIZED HEALTH CARE ARRANGEMENT PP1.5

Index of Procedures

Introduction

Analyzing PHI disclosure for operations of an OHCA is a multi-step process. The Privacy Official should provide answers in advance to all employees with respect to Step 1 and assist in the analysis involved in Steps 2 and 3.

Inquiry/Action Steps

Follow these steps regarding use and disclosure of PHI with members of an OHCA:

Step	Inquiry/Action
1	Review the Quick Reference Guide
2	Is the requesting entity a covered entity that participates in our Practice's OHCA?
3	Confirm compliance with any Special Requirements

Step 1: Review the Quick Reference Guide

Introduction

To determine if a PHI use or disclosure qualifies for the OHCA Permission, first review the Quick Reference Guide to see if the use or disclosure is listed or you have questions. If it is listed, and if you do not have questions, follow the action steps listed in the Quick Reference Guide. If it is not listed in the Quick Reference Guide, **proceed to Step 2.**

Step 2: Is the Requesting Entity a Covered Entity That Participates In Our Practice's OHCA?

Introduction

The first step in applying the OHCA Permission is to determine whether the entity receiving the PHI is a covered entity that participates in an OHCA with our Practice. This procedure should be followed by any Practice employee to determine whether the requesting entity is a covered entity that participates in an OHCA with the Practice.

Step 2.1

Review the OHCA List

Look to the OHCA List, Form F1.5, as completed by our Privacy Official, to determine whether the requesting entity is a Covered Entity that participates in an OHCA with the Practice.

Step 2.2

If the receiving entity is not listed as a covered entity on the OHCA List, then contact the Privacy Official to determine whether the OHCA Permission applies to the intended PHI use or disclosure. If the receiving entity does not participate in an OHCA with the Practice, **proceed to Others' Treatment, Payment, Operations, PP1.4** as a possible permission for the PHI use or disclosure.

If the receiving entity is a Covered Entity that participates in our Practice's OHCA and such entity is receiving PHI for any Health Care Operations activities of the OHCA, **proceed to Step 3.**

Step 3: Confirm Compliance with Applicable Special Requirements

Introduction

Even if the use or disclosure of PHI is for Health Care Operations of an OHCA in which our Practice participates, the procedures in this Step 3 should be followed to determine whether any Special Requirements apply to the use or disclosure of PHI by our Practice. Follow the Practice's policies and procedures for each Special Requirement that applies.

Step 3.1

Do Special Requirements Apply?

For a PHI use or disclosure listed in the Quick Reference Guide, follow the policies and procedures for Special Requirements listed in the Quick Reference Guide. But also consider whether any other Special Requirements apply.

Whether or not a use or disclosure is in the Quick Reference Guide, make sure the use or disclosure complies with every Special Requirement that applies. Determine whether one or more of these Special Requirements apply to a use or disclosure of PHI by our Practice:

- Verification, PP1.12
- Minimum Necessary, PP1.13
- Business Associates, PP1.14
- Personal Representatives, PP1.15
- Marketing, PP1.16
- Psychotherapy Notes, PP1.17
- Consistent with Notice of Privacy Practice, PP1.18
- Consistent with Other Documents, PP1.19
- Consent (State or Other Law), PP1.20

Step 3.2

If Yes, Use Applicable Policies and Procedures

If one or more of the Special Requirements applies, proceed to review and follow the policies and procedures that apply.

Step 3.3

If No, Proceed

After confirming none of the Special Requirements applies, or confirming compliance with those that do apply, proceed to disclose PHI to other participants of our Practice's OHCA for the Health Care Operations activities of the OHCA.

F1.5

Name of Practice:

Address:

Privacy Official:

Telephone:

Organized Health Care Arrangements

OHCA	Participants	Scope of Joint Activities

Last Updated: _____

PERMISSIONS: FAMILY, FRIENDS, AND DISASTER RELIEF ORGANIZATIONS PP1.6

Overview

Introduction

Our Practice may disclose PHI related to a patient's current condition to a patient's family member, other relatives, a close personal friend, or any other person identified by the patient, involved in the patient's care (or payment for care). We may also make a PHI use or disclosure to a disaster relief organization (for purposes of notifying a patient's family member or personal representative). In both cases, this Permission applies if the patient (a) is given an opportunity to agree to or prohibit the use or disclosure of PHI, or (b) is incapacitated or not present, but the disclosure is in the patient's best interests.

> **Note**
>
> This policy and procedure may apply when the policy and procedure PP1.2, Disclosures to the Patient, does not apply. Sometimes, the person involved in a patient's care is a personal representative of the patient. In such cases, a disclosure to the person may qualify for the Disclosures to the Patient Permission because the personal representative status allows the person to be considered to be the patient for HIPAA privacy purposes.

Policies

PP1.6 describes our policies relating to disclosures of PHI to family, friends, and disaster relief organizations (for purposes of notifying a patient's family member or personal representative).

Contact Person

Our Privacy Official is designated to be the contact person for questions, suggestions, or complaints about our Practice's affairs relating to disclosures of PHI to family, friends, and disaster relief organizations (for purposes of notifying a patient's family member or personal representative) and our compliance with the Privacy Rule related to such disclosures.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

DISCLOSURES TO FAMILY AND FRIENDS PP1.6

Policies

General Policy

Our Practice's policy is to comply with the Privacy Rule and applicable state laws regarding disclosures of a patient's PHI to family members, relatives, close personal friends and others identified by the patient involved in the patient's care, and disaster relief organizations (for purposes of notifying a patient's family member or personal representative).

Scope of Policy

This policy applies to disclosures of PHI related to a patient's current condition to family members, close personal friends involved in the patient's care, and disaster relief organizations (for purposes of notifying a patient's family member or personal representative).

> **Note**
>
> This policy is not intended to provide a "loophole" for avoiding the Privacy Rule's other requirements and is not intended to allow disclosures to a broad range of individuals. Rather, this policy should be construed narrowly to allow limited disclosures of PHI to individuals who have close relationships with a patient.

Policy Regarding Disclosures to Family Members, Friends, and Others Involved in a Patient's Care or Payment Related to Care

It is our Practice's policy to disclose to a patient's family member, other relatives, close personal friend, or other person identified by the patient PHI directly relevant to the person's involvement with the patient's care or payment related to the patient's care if one of the following two conditions is met:

1. The patient is *present* and one of the following is true:
   - the patient agrees to the disclosure;
   - the patient is given the opportunity to object to the disclosure, but does not object; or
   - a Practice employee, exercising professional judgment, reasonably infers from the circumstances that the individual does not object to the disclosure.

> **Note**
>
> The Practice may orally present the patient with the opportunity to agree with or disagree with the disclosure and the patient may orally respond.

2. The patient is *not present* or is *incapacitated* or it is an emergency circumstance and both of the following are true:
   - a Practice employee, exercising professional judgment, determines that the disclosure is in the best interests of the patient, and
   - the disclosure is relevant to the person's involvement with the patient's health care.

> **Note**
>
> A Practice employee may use his or her professional judgment and experience with common practice to make reasonable decisions about the patient's best interest in allowing a person to act on behalf of the patient to pick up filled prescriptions, medical supplies, X-rays, or other similar forms of PHI.

Policy Regarding Notifying Family, Friends, or Personal Representatives of Patient's Condition

It is our Practice's policy to use or disclose limited PHI to notify, or assist in the notification of, a patient's family member, personal representative, or other person responsible for a patient's care of the patient's location, general condition, or death if one of the following three conditions is met:

1. The patient is present and one of the following is true:
   - the patient agrees to the disclosure.
   - the patient is given the opportunity to object to the disclosure, but does not object.

Note

The Practice may orally present the patient with the opportunity to agree with or disagree with the disclosure and the patient may orally respond.

   - a Practice employee, exercising professional judgment, reasonably infers from the circumstances that the individual does not object to the disclosure.
2. The patient is not present or is incapacitated or it is an emergency circumstance, and both of the following are true:
   - a Practice employee, exercising professional judgment, determines that the disclosure is in the best interests of the patient; and
   - the disclosure is relevant to the person's involvement with the patient's health care.
3. The Practice is disclosing PHI to an entity authorized by law or by its charter to assist in disaster relief efforts, for the purpose of coordinating notification efforts with such entity, and one of the following is also true:
   - condition 1 above is satisfied.
   - condition 2 above is satisfied.
   - a Practice employee, exercising professional judgment, determines that these requirements interfere with the Practice's ability to respond to the emergency circumstances.

Policy: Special Requirements Still Apply

Even if you confirm that a PHI use or disclosure qualifies for this Family and Friends Permission, you still need to confirm compliance with any applicable Special Requirements, which are the policies and procedures at PP1.13 through PP1.20. (The Verification Policy and Procedure (PP1.12) does not apply to disclosures under this Family and Friends Permission.)

PERMISSIONS: INCIDENTAL DISCLOSURES PP1.7

Introduction	The Privacy Rule permits uses and disclosures that occur incident to any use or disclosure that is permitted or required by HIPAA, so long as the covered entity implements safeguards to avoid such disclosures, and limits the scope of PHI exposed to such incidental disclosures by complying with the Minimum Necessary requirement.
General Policy	The Practice will take reasonable steps to avoid incidental disclosures by implementing appropriate safeguards, and will reduce the amount of PHI exposed to such incidental disclosures by complying with the Minimum Necessary requirement.
Policies and Procedures	Minimum Necessary, PP1.13, describes our Practice's policies and procedures for disclosing the Minimum Necessary PHI. Safeguards, PP3.10, Procedures PS2–PS4, TSS1, and TSM1, describe our Practice's policies and procedures for implementing reasonable Safeguards.
Examples of Incidental Disclosures	The Quick Reference Guide in Chapter 1, Section 1.2, contains examples of permissible Incidental Disclosures. This list includes examples from the United States Department of Health and Human Services (HHS). Our Privacy Official will also add items to the list as helpful and appropriate.
Contact Person	The contact person for information or other communications about Incidental Disclosures is the Privacy Official. The Privacy Official is also designated as the contact person regarding our compliance with the Privacy Rule with respect to Incidental Disclosures.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PERMISSIONS: USES AND DISCLOSURES FOR A PUBLIC PURPOSE PP1.8

Overview

Introduction

The HIPAA Privacy Rule states that our Practice may use or disclose an individual's PHI when such use or disclosure is for certain public health activities or other public purposes designated by HIPAA, or is otherwise required by law. These uses and disclosures do not require any consent or authorization from the patient.

> **Note**
>
> These uses and disclosures must be tracked. The patient is entitled to an accounting that includes uses and disclosures for a public purpose. See Accounting, PP2.3.

Policies and Procedures

PP1.8 describes our Practice's policies and procedures relating to PHI uses and disclosures for a public purpose.

Contact Person

Our Privacy Official is designated to be the contact person for questions relating to PHI uses and disclosures for a public purpose.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PERMISSIONS: USES AND DISCLOSURES FOR A PUBLIC PURPOSE PP1.8

General Policy

Policy

It is our Practice's policy to comply with federal, state, and local laws with respect to the use or disclosure of PHI, and to recognize those situations in which disclosure is required or permitted for public purposes set forth in our Practice's Procedure for Uses and Disclosures for a Public Purpose.

Generally, the Privacy Official will determine whether a use or disclosure of PHI is for a public purpose permitted or required under the Privacy Rule. However, this responsibility may be delegated to a properly trained person.

Satisfaction of Minimum Necessary Standard

The Practice is required to implement reasonable efforts to limit uses, disclosures, and requests for disclosures of PHI to the Minimum Necessary to achieve the purpose of the use, disclosure, or request. See Minimum Necessary, PP1.13.

These procedures apply to uses and disclosures made for a public purpose or otherwise required by law. Note that our Practice may rely on a requested disclosure as the Minimum Necessary for the following uses and disclosures made under this provision:

- disclosure to a public official, if the public official represents that the information requested is the Minimum Necessary for the stated purpose.
- documentation or representations complying with the requirements of the Research section below have been provided by a person requesting information for research purposes.

Procedure for Public Purpose

Follow the steps described in PP1.8, Procedure for Uses and Disclosures for a Public Purpose—Index of Procedures.

PERMISSIONS: USES AND DISCLOSURES FOR A PUBLIC PURPOSE PP1.8

Index of Procedures

Introduction

Our Practice may use or disclose an individual's PHI for certain public purposes or if the use or disclosure is required by law. Generally, the Privacy Official will determine whether a use or disclosure of PHI is for a public purpose permitted or required by the Privacy Rule.

Inquiry/Action Steps

These steps can be used to determine whether a use or disclosure of PHI is permitted for a public purpose:

Step	Inquiry/Action
1	Review the Quick Reference Guide
2	Review Public Purposes A through O for applicability
3	Confirm compliance with Special Requirements
4	Document disclosures of PHI
5	Provide disclosure documentation to Privacy Official

Step 1: Review the Quick Reference Guide

Introduction

There are many types of PHI uses and disclosures that are permitted for a public purpose. To determine whether a use or disclosure is permitted for a public purpose, our Practice will use these procedures.

Step 1.1

Review the Quick Reference Guide

First review the Quick Reference Guide to see if the intended use or disclosure is listed in the Public Purposes section of the Quick Reference Guide.

Step 1.2

Use or Disclosure Not in Quick Reference Guide

If you do not find the intended use or disclosure in the Quick Reference Guide, then review any of the following types of public purposes that may apply. Proceed to Step 2.

If the PHI is to be disclosed…	See Step 2
■ As required by law	Public Purpose A
■ For public health activities	Public Purpose B
☐ Public Health Authority, B-1	
☐ Relating to Child Abuse, B-2	
☐ FDA-Related, B-3	
☐ Relating to Spread of Disease, B-4	
☐ To an Employer, B-5	
■ About victims of abuse, neglect, or domestic violence	Public Purpose C
■ For health oversight activities	Public Purpose D
■ A judicial or administrative proceeding	Public Purpose E
■ For law enforcement purposes	Public Purpose F
■ With respect to a decedent	Public Purpose G
■ To facilitate organ donation	Public Purpose H
■ For research	Public Purpose I
■ To avoid serious threat to health or safety	Public Purpose J

■ Regarding armed forces personnel	Public Purpose K
■ Regarding national security and intelligence activities	Public Purpose L
■ To provide protective services for the President of the United States and other high state officials	Public Purpose M
■ About an individual in legal custody	Public Purpose N
■ To comply with workers' compensation laws	Public Purpose O

Step 2: Review Public Purposes A through O for Applicability

Public Purpose A—Required by Law

Introduction

The Privacy Rule permits uses and disclosure of PHI that are required by law.

Definition

The full definition of required by law is in the Glossary. Required by law basically means the law makes you use or disclose PHI—not that the law allows you to do so.

A-1: Disclose PHI as Required By Law

Our Practice may use and disclose PHI to the extent it is required by law, and provided the use or disclosure complies with and is limited to the relevant requirements of such law. Form F1.8A is attached to provide the Privacy Official with a place to note required state law disclosures and state law limits on what can be disclosed.

A-2: Follow Requirements for Specific Disclosures

Any use or disclosure made as a result of Step 1 must comply with the requirements described in one of the sections below if it relates to the subject of those sections:

- Victims of Abuse, Neglect, or Domestic Violence, B-1 or C-1
- Judicial and Administrative Activities, E
- Law Enforcement, F

Public Purpose B—Disclosures for Public Health Activities

Introduction

Our Practice may disclose PHI to the individuals listed in Steps 3.1 through 3.5 below for the purposes described.

Definition

The full definition of "public health authority" is in the Glossary. It basically means government agencies responsible for public health matters as part of their official mandate (including some contractors of such agencies).

B-1: Disclosing PHI to a Public Health Authority

Our Practice may disclose PHI to a public health authority authorized by law to collect or receive such information for the purpose of preventing or controlling disease, injury, or disability.

The Privacy Official will list below examples of these public health authorities under our local and state governments:

Public Health Authorities:

_____

_____

_____

_____

If the Practice is also a public health authority, our Practice may use PHI for the purposes described above.

At the direction of a public health authority, our Practice may also disclose PHI to an official of a foreign government agency that is acting in collaboration with a public health authority.

B-2: Disclosing PHI Relating to Child Abuse

Our Practice may disclose PHI to a public health authority or other appropriate government agency authorized by law to receive reports of child abuse or neglect.

B-3: FDA-Related Disclosures

Our Practice may disclose PHI to a person subject to the jurisdiction of the U.S. Food and Drug Administration (FDA) with respect to an FDA-related product or activity for which that person is responsible, for the purpose of activities related to the quality, safety, or effectiveness of the FDA-related product or activity.

B-4: Disclosing PHI Related to Spread of Disease

Our Practice may disclose PHI to a person who may have been exposed to a communicable disease, or is otherwise at risk of contracting or spreading a disease or condition, provided that the Practice is authorized by law to notify such person as necessary in the conduct of a public health intervention or investigation.

Form 1.8B is attached to provide the Privacy Official with a place to note state law that requires disclosure to state agencies regarding spread of disease.

B-5: Disclosing PHI to an Employer for Workplace Medical Surveillance

Our Practice may disclose PHI of an individual to his or her employer if:

- the Practice is a covered health care provider who is a member of the workforce of such employer who provides health care or who provides health care to the individual at the employer's request (a) to conduct an evaluation relating to medical surveillance of the workplace, or (b) to evaluate whether the individual has a work-related injury;
- the PHI disclosed consists of findings regarding a work-related illness or injury or a workplace-related medical surveillance;
- the employer needs the findings in order to comply with its state and legal obligations to record such illness or injury or carry out responsibilities for workplace medical surveillance; and
- the Practice provides written notice to the individual that PHI relating to medical surveillance of the workplace and work-related illnesses and injuries is disclosed to the employer (a) by giving a copy of the notice to the individual at the time the health care is provided, or (b) if the health care is provided on the employer's work site, by posting the notice in a prominent place at the site where such health care is provided.

Public Purpose C—Victims of Abuse, Neglect, or Domestic Violence

Introduction

Our Practice is permitted by the Privacy Rule to make appropriate disclosures about individuals who are victims of abuse, neglect, or domestic violence.

Note

This section does not apply to reports of child abuse or neglect, which are governed by the section on Disclosures for Public Health Activities in Public Purpose B-2 above.

C-1: Disclosing PHI About Victims of Abuse

Our Practice will disclose PHI about an individual whom the Practice reasonably believes to be a victim of abuse, neglect, or domestic violence to a government authority expressly authorized to receive reports of such abuse, neglect, or domestic violence if:

- the disclosure is required by law and complies with and is limited to the relevant requirements of such law;
- the individual agrees to the disclosure; or
- the disclosure is authorized by statute or regulation and either:
  - ☐ the Practice believes the disclosure is necessary to prevent serious harm to the individual or other potential victims; or
  - ☐ if the individual cannot agree due to incapacity, the Practice may make the disclosure if the person authorized to receive the report represents that the PHI will not be used against the individual, and that an immediate enforcement activity would be materially and adversely affected by waiting until the individual can agree.

Note

Form 1.8C is attached to provide the Privacy Official with a place to note state law that requires disclosure to state agencies regarding victims of abuse.

C-2: Do Not Inform the Individual or Personal Representative If Risky

Our Practice must promptly inform the individual of any disclosures made, *except if:*

- the Practice believes in its professional judgment that informing the individual would place him or her at risk of serious harm, or
- the Practice would be informing a personal representative whom the Practice believes to be responsible for the abuse, neglect, or other injury and the Practice reasonably believes in its professional judgment that informing such personal representative would not be in the individual's best interests.

Public Purpose D—Health Oversight Activities

Introduction

Our Practice may disclose PHI for health oversight activities.

Note

Form 1.8D is attached for the Privacy Official with a place to note state law-required notifications for health oversight activities.

Definition

The full definition of "health oversight agency" is in the Glossary. It includes agencies authorized by law to oversee the health care system.

D-1: Disclosing PHI to a Health Oversight Agency

Our Practice may disclose PHI to a health oversight agency for health oversight activities authorized by law, or other activities necessary for appropriate oversight of the following:

- the health care system;
- government benefit programs for which health information is relevant to beneficiary eligibility;
- entities subject to government regulatory programs for which health information is necessary for determining compliance with program standards; or
- entities subject to civil rights laws under which health information is necessary for determining compliance.

D-2: Certain Investigations or Activities Are Not Health Oversight Activities

The permission to disclose for health oversight activities does not include investigations or activities (a) in which the individual is the subject, and (b) that do not arise out of and are not directly related to:

- the receipt of health care;

- a claim for public benefits related to health; or
- qualification for or receipt of public benefits or services, when a patient's health is integral to the claim for such benefits or services.

D-3: (If Applicable) Joint Activities or Investigations

If a health oversight activity is conducted in conjunction with an oversight activity or investigation relating to a claim for public benefits not relating to health, the joint activity or investigation is considered a health oversight activity.

D-4: (If Applicable) Our Practice as a Health Oversight Agency

If the Practice is also a health oversight agency, it may use PHI for health oversight activities consistent with this section.

Public Purpose E—Judicial and Administrative Activities

Introduction

The Privacy Rule permits uses and disclosures of PHI in judicial or administrative activities as described below.

Definition

Qualified protective order means an order of a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

- prohibits the parties from using or disclosing the PHI for any purpose other than the litigation or proceeding for which the PHI was requested; and
- requires either the destruction of or return to the Practice of the PHI, including all copies made, at the end of the litigation or proceeding.

E-1: Disclosing PHI Under Court Order

Our Practice may disclose PHI in a judicial or administrative proceeding in response to an order of a court or administrative tribunal.

E-2: Disclosing PHI Pursuant to Subpoena or Discovery Request

If a subpoena, discovery request, or other lawful process is not accompanied by such an order, the Practice may disclose PHI if the Practice receives satisfactory assurance in writing from the party seeking the information that it has made reasonable efforts:

(a) to ensure that the subject individual has been given notice of the request, or

(b) to secure a qualified protective order.

Our Practice may also disclose the PHI without receiving satisfactory assurances from the party seeking the information (as described in the preceding sentence) if our Practice has made reasonable efforts to comply with either (a) or (b) above.

E-3: Assurances of Reasonable Efforts to Notify Patient

Satisfactory assurances that the requestor has made reasonable efforts to notify the patient (see E-2(a) above) can be made by a written statement and accompanying documentation stating:

- the party requesting PHI has made a good faith attempt to provide written notice to the individual;
- the notice included sufficient information about the litigation or proceeding in which the PHI is requested; and
- the time for the individual to raise objections to the court or administrative tribunal has elapsed and either:
  - (a) no objections were filed, or
  - (b) all objections filed have been resolved by the court or tribunal, and the requested disclosures are consistent with that resolution.

E-4: Assurances of Reasonable Efforts to Secure Qualified Protective Order

Satisfactory assurances that the requestor has made reasonable efforts to secure a qualified protective order (see E-2(b) above) can be made by a written statement and accompanying documentation stating:

- the parties to the dispute giving rise to the request for information have agreed to a qualified protective order and have presented it to the court or tribunal with jurisdiction over the dispute; or
- the party seeking the PHI has requested a qualified protective order from such court or tribunal.

Public Purpose F—Law Enforcement Purposes

Introduction

The Privacy Rule permits uses and disclosures of PHI for law enforcement purposes.

F-1: Disclosing PHI for Law Enforcement Purposes

Our Practice may disclose PHI to a law enforcement official for law enforcement purposes, provided that the conditions in F-2, F-3, F-4, or F-5 are also met, as follows:

If disclosing…	**Then use…**
■ In compliance with law or regulations	F-2
■ To locate a suspect or fugitive	F-3
■ About crime victims	F-4
■ As evidence of a crime	F-5
■ In emergencies	F-6

F-2: Disclosing PHI In Compliance With Law and Legal Orders

Our Practice may disclose PHI as required by law, including laws that require reporting of certain types of wounds or other physical injuries (except that laws applying to Victims of Abuse, Neglect, or Domestic Violence are governed by Subsection C above).

Our Practice may disclose PHI in compliance with, and as limited by:

- a court order or court-ordered warrant, a subpoena, or summons issued by a judicial officer;
- a grand jury subpoena; or
- an administrative request, provided that (a) the information sought is relevant and material to a legitimate law enforcement inquiry, (b) the request is specific and limited in scope to the extent reasonably practicable in light of the purpose for which the information is sought, and (c) de-identified information could not reasonably be used.

F-3: Disclosing PHI to Locate a Suspect or Fugitive

In addition to disclosures required by law under F-2 above, the Practice may also disclose PHI in response to a law enforcement officer's request for the purposes of identifying or locating a suspect, fugitive, material witness, or missing person, with the following restrictions:

- our Practice may only disclose the individual's:
  - ☐ name and address
  - ☐ date and place of birth
  - ☐ social security number
  - ☐ ABO blood type and rh factor
  - ☐ type of injury
  - ☐ date and time of treatment
  - ☐ date and time of death, if applicable

- ☐ description of distinguishing physical characteristics
- ☐ under this section, except for the eight types of information listed above, the Practice may not disclose any PHI related to the individual's DNA or DNA analysis, dental records, or typing, samples, or analysis of bodily fluids or tissue.

F-4: Disclosing PHI About Crime Victims

In addition to disclosures required by law under F-2 above, and to the extent not already covered by Public Purpose C, Victims of Abuse, Neglect, or Domestic Violence above, the Practice may disclose PHI about victims of crime subject to the following restrictions:

- the individual's agreement; or
- our Practice cannot obtain the individual's agreement due to incapacity or other emergency circumstance, provided that:
  - ☐ the law enforcement official represents that the information is needed to determine whether a violation of law by a person other than the victim has occurred, and the information is not intended to be used against the victim;
  - ☐ the law enforcement official represents that immediate law enforcement activity that depends on the information would be materially and adversely affected by waiting until the individual can agree; and
  - ☐ the Practice determines in its professional judgment that the disclosure is in the best interests of the individual.

F-5: Disclosing PHI As Evidence of a Crime on the Premises

Our Practice may disclose PHI to a law enforcement officer that the Practice believes in good faith constitutes evidence of criminal conduct that occurred on the premises of the Practice.

F-6: Reporting Crime in Emergencies

When providing emergency health care in response to a medical emergency, other than on our premises, our Practice may disclose PHI to a law enforcement official if the disclosure appears necessary to alert law enforcement to:

- the commission and nature of a crime;
- the location of the crime or of the victim(s) of the crime; and
- the identity, description, and location of the perpetrator of the crime.

Note

If we believe that the medical emergency is the result of abuse, neglect, or domestic violence of the individual in need of emergency health care, F-6 does not apply and any disclosure we make to a law enforcement official for law enforcement purposes must be made under Subsection C above, Victims of Abuse, Neglect, or Domestic Violence.

Public Purpose G—Decedents

Introduction

The Privacy Rule permits PHI of a decedent to be disclosed for the purpose of alerting law enforcement of possible criminal conduct.

G-1: Disclosing Decedent's PHI

If our Practice suspects that the death may have resulted from criminal conduct, our Practice may disclose PHI about an individual who has died to a law enforcement official for the purposes of alerting law enforcement of such death.

G-2: Disclosing PHI to a Coroner

Our Practice may use or disclose PHI to a coroner or medical examiner for the purpose of identifying a deceased person, determining the cause of death, or other duties as authorized by law. If the Practice performs the duties of a coroner or medical examiner, it may use PHI for the purposes stated in this Subsection G-2.

G-3: Disclosing PHI to a Funeral Director

Our Practice may disclose PHI to funeral directors consistent with applicable law, and as needed for the funeral directors to carry out their duties regarding the decedent. If necessary for funeral directors to carry out their duties, the Practice may disclose PHI prior to and in reasonable anticipation of the individual's death.

Public Purpose H—Cadaveric Organ, Eye, or Tissue Donation

Introduction

The Privacy Rule permits the use or disclosure of PHI for organ procurement.

Disclosing PHI for Organ Procurement

Our Practice may use or disclose PHI to organ procurement and related organizations for the purpose of facilitating organ, eye, or tissue donation and transplantation.

Public Purpose I—Research

Introduction

Our Practice may use or disclose PHI for research purposes in compliance with PP1.9, Authorization. In addition, we may use or disclose PHI without an Authorization as described in this Section I, Research.

The Privacy Rule permits use or disclosure of PHI for research purposes without an individual Authorization as described below.

If research disclosure is…	**Then use…**
■ Pursuant to an Authorization	PP1.9
■ Pursuant to waiver of authorization requirement	Step A
■ Preparatory to research	Step B
■ Solely for research on decedents	Step C

Definition

A **qualified privacy board** has members with varying backgrounds and appropriate professional competency as necessary to review the effect of the research protocol on the individual's privacy rights and interests; includes at least one member who is not affiliated with the Practice, not affiliated with the entity conducting or sponsoring the research, and not related to any person affiliated with any of such entities; and does not have any member participating in a review of any project in which the member has a conflict of interest.

I-1: Disclosing PHI for Research Purposes

Our Practice may use or disclose PHI for research purposes, regardless of the source of funding, if any one of the following three conditions is met:

(1) *IRB Waiver.* Our Practice obtains proper documentation pursuant to Subsection I-2 below that an alteration or waiver of the individual authorization required for use or disclosure of PHI has been approved by either an Institutional Review Board (IRB) or a qualified privacy board;

(2) *Preparatory to Research.* Our Practice obtains representations from the researchers that:

- use or disclosure is sought solely to review PHI as necessary to prepare for research protocols or other similar purposes preparatory to research;
- no PHI is to be removed from the Practice by the researcher during the review; and
- the PHI is necessary for the research purposes; or

(3) *Decedents.* Our Practice obtains the following from the researchers:

- representation that the use or disclosure is sought solely for research on PHI of decedents;
- at the Practice's request, documentation of the death of such individuals; and
- representation that the PHI is necessary for the research purposes.

I-2: Documentation of Waiver Approval

Our Practice must obtain the following documentation when relying on an IRB or a qualified privacy board approval of alteration or waiver of individual authorization:

- The documentation must include a statement identifying and confirming the authority of the IRB or privacy board and the date on which the alteration or waiver of authorization was approved.
- The documentation must include a statement that the IRB or privacy board has determined that the alteration or waiver satisfies the following criteria:
  - ☐ the use or disclosure of PHI involves no more than minimal risk to the individual's privacy;
  - ☐ the research could not practicably be conducted without the alteration or waiver; and
  - ☐ the research could not practicably be conducted without access to and use of the PHI.
- At least the following elements must be present to ensure that there is a minimal risk to the individual's privacy:
  - ☐ an adequate plan to protect the identifiers from improper use or disclosure;
  - ☐ an adequate plan to destroy the identifiers at the earliest possible opportunity consistent with the conduct of the research, unless there is a health or research justification for retaining the identifiers or their retention is required by law; and
  - ☐ adequate written assurances that the PHI will not be reused or disclosed to any other person, except as required by law, for authorized oversight of the research study, or for other research for which use or disclosure of the PHI would be permitted under the Privacy Rule.
- The documentation must include a brief description of the PHI for which use or access is necessary, as determined by the IRB or privacy board.
- The documentation must include a statement that the alteration or waiver of authorization has been reviewed and approved under either normal or expedited review procedures.
- The chair of the IRB or the privacy board, or another member designated by the chair, must sign the documentation of the alteration or waiver of authorization.

Public Purpose J—To Avoid Serious Threat to Health or Safety

Introduction

The Privacy Rule permits certain uses and disclosures without patient authorization to prevent or lessen a serious and imminent threat to health or safety.

J-1: Disclosing PHI to Lessen Imminent Threat

Consistent with ethical conduct and applicable law, the Practice may use or disclose PHI if it believes in good faith that the use or disclosure is necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, and is made to a person reasonably able to prevent or lessen the threat, including the target of the threat.

J-2: Disclosing PHI to Apprehend a Criminal

Consistent with ethical conduct and applicable law, the Practice may use or disclose PHI (other than PHI acquired in the course of counseling or therapy) if it believes in good faith that the use or disclosure is necessary for law enforcement authorities to identify or apprehend an individual:

(a) because of a statement by the individual admitting participation in a violent crime that the Practice reasonably believes may have caused serious physical harm to the victim; or

(b) where it appears from all circumstances that the individual has escaped from a correctional institution or from lawful custody. See Public Purpose N below for definition of correctional institution.

J-3: Do Not Disclose PHI Learned in Treatment

Our Practice may *not* disclose PHI to apprehend a criminal if the Practice learns of the threat

(a) in the course of treatment to affect the propensity to commit criminal conduct, or counseling, or therapy; or

(b) through a request by the individual to initiate or to be referred for the treatment, counseling, or therapy referenced above.

J-4: Disclose Only Limited PHI

Disclosures of PHI made in accordance with Subsection J-2 above should be limited to the individual's statement referenced above and the following information about the individual:

- name and address
- date and place of birth
- social security number
- ABO blood type and rh factor
- type of injury
- date and time of treatment
- date and time of death, if applicable
- description of distinguishing physical characteristics

J-5: Belief Must Be Based on Knowledge

For purposes of this section, the Practice is presumed to have acted in good faith regarding a belief described in Subsections J-1 or J-2 above if the belief is based on the Practice's actual knowledge or in reliance on a credible representation by a person with apparent knowledge or authority.

Public Purpose K—Military and Veterans' Activities

Introduction

The Privacy Rule permits uses and disclosures without patient authorization for certain military purposes.

K-1: Disclosing PHI of Armed Forces Personnel

Our Practice may use and disclose PHI of armed forces personnel for activities deemed necessary by appropriate military command authorities to assure the proper execution of the military mission, if the military authority has published a notice in the *Federal Register* with the following information:

- appropriate military command authorities; and
- the purposes for which the PHI may be used or disclosed.

K-2: Disclosing PHI of Foreign Military Personnel

Our Practice may disclose the PHI of foreign military personnel to their appropriate foreign military authority for the same purposes for which uses and disclosures regarding armed forces personnel are permitted under the notice published in the *Federal Register*.

Public Purpose L—National Security and Intelligence Activities

Introduction

The Privacy Rule permits the use and disclosure of PHI without patient authorization for national security and intelligence activities.

Disclosing PHI for Intelligence Purposes

Our Practice may disclose PHI to authorized federal officials for the conduct of lawful intelligence, counter-intelligence, and other national security activities authorized by the National Security Act and implementing authority (eg, an executive order).

Public Purpose M—Protective Services for the President and Others

Introduction

The Privacy Rule permits the use or disclosure of PHI without patient authorization to protect the president of the United States.

Disclosing PHI to Protect the President

Our Practice may disclose PHI to authorized federal officials to:

- provide protective services to the president of the United States, foreign heads of state, and other authorized persons, or
- conduct certain related investigations.

Public Purpose N—Correctional Institutions and Other Law Enforcement Custodial Situations

Introduction

The Privacy Rule permits the use and disclosure of PHI without patient authorization about inmates.

Definition

Correctional institution: Any penal or correctional facility, jail, reformatory, detention center, work farm, halfway house, or residential community program center operated by or under contract to the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, for the confinement or rehabilitation of persons charged with or convicted of a criminal offense or other persons held in lawful custody. Others in lawful custody include juvenile offenders adjudicated delinquent, aliens detained awaiting deportation, persons committed to mental institutions through the criminal justice system, witnesses, or others awaiting charges or trial.

N-1: Disclosing PHI About Inmates in Correctional Institutions

Our Practice may disclose PHI about an inmate to a correctional institution or law enforcement official maintaining lawful custody of the inmate if the correctional institution or law enforcement official maintains that the information is necessary for the following:

- the provision of health care to the individual;
- the health and safety of the individual or other inmates;
- the health and safety of the officers or employees or others of the correctional institution;
- the health and safety of those responsible for transporting of inmates or their transfer from one institution to another;
- law enforcement on the premises of the correctional institution; or
- the administration and maintenance of safety, security, and good order of the correctional institution.

Note

If the Practice is a correctional institution, it may use the PHI of inmates for any purpose that the PHI may be disclosed for in this section.

N-2: No Inmates Are on Parole

For the purposes of this section, an individual is no longer an inmate when released on parole, probation, supervised release, or is otherwise no longer in lawful custody.

Public Purpose O—Workers' Compensation

Introduction

The Privacy Rule permits uses and disclosures of PHI to comply with laws governing compensation for work-related injuries.

Disclosing PHI for Workers' Compensation

Our Practice may disclose PHI as authorized by and to the extent necessary to comply with laws relating to workers' compensation or other similar programs that are established by law and provide benefits for work-related injuries or illness regardless of fault.

Note

Form F1.8O is attached to provide the Privacy Official with a place to note state laws regarding workers' compensation and other similar programs applicable in the state in which our Practice is located.

F1.8A

State Law Required Disclosures

Described below are the circumstances in which the laws in the State of _____ require disclosure of confidential medical information (and the limits placed on such disclosure under such laws).

F1.8B-4

State Law
Notification Requirements
Spread of Disease

Described below are the circumstances in which the laws of the State of _____ require our Practice to report confidential medical information regarding the spread of disease.

F1.8C

State Law
Notification Requirements
Victims of Abuse

Described below are the circumstances in which the laws of the State of _____ require our Practice to report confidential medical information regarding victims of abuse.

F1.8D

State Law
Notification Requirements
Health Oversight Activities

Described below are the circumstances in which the laws of the State of _____ require our Practice to report confidential medical information regarding health oversight activities.

F1.8O

State Law
Workers' Compensation Laws

Described below are workers' compensation and other similar programs described in PP1.8, Public Purpose O, applicable in the State of _____ in which our Practice is located.

PERMISSIONS: AUTHORIZATION PP1.9

Overview

Introduction

The Privacy Rule provides that the Practice may not use or disclose PHI without a valid Authorization from the patient, unless such use or disclosure is otherwise permitted or required by the Privacy Rule.

Most of our Practice's operations will not require that we receive or request an Authorization, because most of what we do involves treatment, payment, or health care operations.

Though somewhat limited, the situations in which we are required to have an Authorization from the patient are important. This policy and other policies will help us identify those situations.

Policies and Procedures

PP1.9 describes our Practice's policies and procedures relating to Authorizations.

Contact Person

Our Privacy Official is designated to be the contact person for questions, suggestions, or complaints related to Authorizations and our compliance with the Privacy Rule related to Authorizations.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PERMISSIONS: AUTHORIZATION PP1.9

General Policy

Policy

Our Practice's policy is to comply with the Privacy Rule requirement that we not use or disclose PHI without a valid Authorization, unless the use or disclosure is otherwise permitted or required by the Privacy Rule. It is also our Practice's policy to document and retain any Authorization we rely on to use, disclose, or request PHI.

What Is a Valid Authorization?

A valid Authorization is a document signed by (or on behalf of) the patient that contains a number of specific elements. Step 2 of PP1.9 describes the elements of a valid Authorization.

Scope of Policy

This policy covers Authorization requirements for all of the Practice's uses and disclosures of PHI, unless the Privacy Rule permits a use or disclosure without an Authorization.

Uses and Disclosures Not Requiring Authorization

Uses and disclosures of PHI that are not covered by this policy, because the Privacy Rule permits them to be made without an Authorization, include those made under the following policies and procedures:

- Required Disclosures, PP1.1
- Disclosures to the Patient, PP1.2
  - (also see Personal Representatives, PP1.15)
- Our Treatment, Payment, Operations, PP1.3
- Others' Treatment, Payment, Operations, PP1.4
- Operations of Organized Health Care Arrangement, PP1.5
- Family, Friends, and Disaster Relief Organizations, PP1.6
- Incidental Disclosures, PP1.7
- Public Purpose, PP1.8
- De-Identification, PP1.10
- Limited Data Set, PP1.11

Note

The Special Requirements policies and procedures may require an Authorization in some cases, even when an Authorization would not be required under the above policies and procedures. For example, a disclosure of Psychotherapy Notes might still require Authorization. (See Special Requirements PP1.17.)

Authorization Procedures

Unless a Practice policy or procedure specifically permits or requires a use or disclosure of PHI without an Authorization, follow the steps described in PP1.9, Authorization—Index of Procedures, when using or disclosing PHI.

PERMISSIONS: AUTHORIZATION PP1.9

Index of Procedures

Introduction

Every Practice employee should be able to perform Step 1 of these Authorization Procedures. Everyone needs to know when an Authorization is required for an intended use or disclosure of PHI or if the Privacy Official or another properly trained Practice employee has determined that the Practice must obtain Authorizations from patients for certain of the Practice's uses or disclosures of PHI. If a Practice employee has questions, he or she should refer the matter to the Privacy Official.

Where an Authorization is required, only the Privacy Official or a properly trained person designated by the Privacy Official may determine that the Authorization form is valid.

Ensuring that an Authorization is a valid document prior to making a use or disclosure of PHI is a multi-step process. The Privacy Official (or a designated person) is responsible for completing Steps 2–5.

The Privacy Official is responsible for reviewing Authorization procedures as necessary, and for handling difficult Authorization procedures. Generally, the Privacy Official should use Step 2 and the Authorization attached as F1.9 to ensure the validity of any Authorization the Practice creates. As with other procedures, the Privacy Official may designate properly trained persons to assist with these functions.

Inquiry/Action Steps

Follow these steps prior to making a use or disclosure of PHI that may require an Authorization:

Step	Inquiry/Action
1	Does the use or disclosure require an Authorization?
2	Confirm that the Authorization is valid.
3	Confirm compliance with applicable Special Requirements.
4	Document the Authorization.
5	Refrain from making the use or disclosure (if applicable).
6	Process revocation of the Authorization (if applicable).

Step 1: Does the Use or Disclosure Require an Authorization?

Introduction

A Practice employee should use this procedure to determine whether a use or disclosure may be made without an Authorization, because it is otherwise permitted by the Privacy Rule and by the Practice's polices and procedures.

Step 1.1

Review the Quick Reference Guide

If the use or disclosure is listed under another Permission in the Quick Reference Guide, comply with the conditions of the other Permission. This Authorization policy and procedure does not apply (unless triggered by a Special Requirement like Marketing, PP1.16, or Psychotherapy Notes, PP 1.17).

Step 1.2

Determine if the Use or Disclosure of PHI is Permitted or Required Without an Authorization

If the Quick Reference Guide does not list the intended use or disclosure, or if you have questions, consider whether the use or disclosure of PHI is permitted or required by the Privacy Rule and the Practice's policies and procedures without an Authorization.

A use or disclosure of PHI is permitted or required by the Privacy Rule and the Practice's policies and procedures without an Authorization if it is made under one of the following policies and procedures:

- Our Treatment, Payment, Operations, PP1.3
- Others' Treatment, Payment, Operations, PP1.4
- Operations of Organized Health Care Arrangement, PP1.5
- Family, Friends, and Disaster Relief Organizations, PP1.6
- Incidental Disclosures, PP1.7
- Public Purpose, PP1.8
- De-Identification, PP1.10
- Limited Data Set, PP1.11

If the use or disclosure of PHI may be made under one of these policies, an Authorization is not required. Follow the applicable policy.

If the use or disclosure of PHI may not be made under one of the above-listed policies, **proceed to Step 2.**

Step 2: Confirm That the Authorization Is Valid

Introduction

The Privacy Official or other properly trained person will use this procedure and the Authorization attached as form F1.9 to ensure the validity of any Authorizations the Practice creates or obtains for its uses and disclosures of PHI.

Generally, our Practice will require Authorization Form PP1.9 when an Authorization is required before releasing PHI. In the rare instance when the Privacy Official accepts another authorization form, he or she (or a trained designated employee) will use this procedure to determine whether an Authorization requesting that the Practice disclose PHI to a third party is valid.

Policy on Assisting Patient With Authorization Forms

Use the rules described in Step 2 to revise or complete the Authorization as necessary to ensure that you have an Authorization that is valid with respect to the Practice's intended use or disclosure of PHI.

Privacy Official Training

Step A The Privacy Official will train the Practice employees who will seek Authorizations from patients to understand what information must be obtained from the patient for the Authorization to be valid.

Step B The Privacy Official will train the Practice employees who will be using or disclosing PHI pursuant to the Authorization to understand what uses and disclosures the Authorization permits.

Note

The Privacy Official will designate and certify those employees who are sufficiently trained to prepare Authorizations or to make determinations with respect to the sufficiency of any Authorization on behalf of our Practice. If you are not trained and certified, refer any Authorization you receive to the Privacy Official.

Follow Steps to Confirm Valid Authorization

Follow Steps 2.1 through 2.7 to confirm that an Authorization is valid and complete.

Step 2.1

Confirm That the Authorization Contains Required Core Elements

Confirm whether the Authorization contains all of the following core elements:

- a description of the PHI to be used or disclosed that identifies the information in a meaningful fashion;
- the name or specific identification of the person(s) or class of persons authorized to make the use or disclosure;
- the name or specific identification of the person(s) or class of persons to whom the requested use or disclosure may be made;
- a description of the purpose for the use or disclosure ("at the request of the individual" is a sufficient description if the individual initiates the Authorization);
- an expiration date or expiration event ("end of the research study" or "none" is sufficient if the Authorization is for a research-related use or disclosure); and
- the signature and date of signature of the individual whose information will be used or disclosed (if the Authorization is signed by a personal representative of the individual, a description of the representative's authority to act for the individual must also be provided).

If the Authorization contains all of the core elements in Step A, **proceed to Step 2.2.**

If the Authorization does not contain all of the core elements listed in Step A, the Authorization is not valid. **Skip to Step 5.**

Step 2.2

Confirm That the Authorization Provides Required Notice

Confirm that the Authorization contains statements adequate to place the individual on notice of all of the following:

- the individual's right to revoke the Authorization in writing and either (a) exceptions to the right to revoke and a description of how the individual may revoke the Authorization; or (b) a reference to the Notice of Privacy Policies section that discusses exceptions to the right to revoke and a description of how an individual may revoke an Authorization;
- either (a) a statement that the Practice (or other party seeking the Authorization) may not condition treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the Authorization or (b) if the Privacy Rule permits conditioning the provision of treatment, payment, enrollment, or eligibility for benefits on whether the individual signs the Authorization, the consequences to the individual of refusing to sign the Authorization (see Step 2.5(F)); and
- the potential for information disclosed pursuant to the Authorization to be redisclosed by the recipient and to no longer be protected by the Privacy Rule.

If the Authorization contains all of the statements described above, **proceed to Step 2.3.**

If the Authorization does not contain all of the statements described above, it is not valid. **Skip to Step 5.**

Step 2.3

Confirm That the Authorization Includes Notice if it is for Marketing Purposes and Involves Compensation

Confirm that the Authorization includes proper notice if it is for marketing purposes and involves compensation.

Step A Refer to Marketing, PP1.16, to determine whether a use or disclosure of PHI involves Marketing and, if so, whether it requires an Authorization.

Step B If, under Marketing, PP1.16, a use or disclosure of PHI involves Marketing and requires an Authorization, **proceed to Step C.** Otherwise, **skip to Step 2.4.**

Step C If the Marketing involves direct or indirect compensation to the Practice, the Authorization must state that such compensation is involved.

Step 2.4

Confirm That the Authorization is Written in Plain Language

Step A Confirm that the Authorization is written in plain language. Among other relevant considerations, the "plain language" review of the Authorization should include consideration of whether the Authorization:

- is organized to serve the needs of the reader;
- is written in short sentences and in the active voice;
- uses common, everyday words in sentences; and
- divides material into short sections.

Step B If the Authorization is written in plain language, **proceed to Step 2.5.**

Step C If the Authorization is not written in plain language, it is not valid. **Skip to Step 5.**

Step 2.5

Determine Whether the Authorization is Defective

Step A Determine whether any of the following is true:

- the expiration date has passed or a Practice employee knows that the expiration event has occurred;
- the Authorization has not been filled out completely with respect to the core elements described in Step 2.1;
- a Practice employee knows that the Authorization has been revoked. (See the procedure for revoking an authorization at the end of this module.); or
- a Practice employee knows that any material information in the Authorization is false.

Step B If none of the conditions described in Step A is true, **proceed to Step D.**

Step C If any of the conditions described in Step A are true, the Authorization is not valid. **Skip to Step 5.**

Step D Determine whether the Authorization is combined with another document. This is called a Compound Authorization. If the Authorization is not combined with another document, **skip to Step F**. Otherwise, **proceed to Step E.**

Step E Determine whether the Compound Authorization is permitted.

1. Determine whether the Compound Authorization fits within one of the following three categories:

- An Authorization for the use or disclosure of PHI for a research study combined with any other type of written permission for the same research study (including another Authorization for the use or disclosure of PHI for such research or a consent to participate in such research);
- An Authorization for a use or disclosure of Psychotherapy Notes combined with another Authorization for a use or disclosure of Psychotherapy Notes (see Psychotherapy Notes, PP1.17); or
- An Authorization for a use or disclosure of PHI (other than Psychotherapy Notes) combined with any other Authorization for a use or disclosure of PHI, (except if the Authorization conditions the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an Authorization).

2. If the Compound Authorization is one of the three types described in Step E(1), **proceed to Step F.**
3. If the Compound Authorization is not one of the three types described in Step E(1), it is not valid. **Skip to Step 5.**

Step F Determine whether the Authorization conditions treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an Authorization. If the Authorization includes such a condition, **proceed to Step G.** Otherwise, **skip to Step 2.6.**

Step G Determine whether the Authorization may condition treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an Authorization.

1. Determine whether the Authorization is one of the following three types:
   - An Authorization conditioning the provision of research-related treatment on provision of the Authorization for the use or disclosure of PHI for such research;
   - An Authorization for disclosure of PHI (other than Psychotherapy Notes) to a health plan, conditioning enrollment in the health plan, or eligibility for benefits on provision of the Authorization; or
   - An Authorization conditioning the provision of health care that is solely for the purposes of creating PHI for disclosure to a third party on provision of the Authorization permitting disclosure of such PHI to such third party.
2. If the Authorization is one of the three types described in Step G(1), **proceed to Step 2.6.**
3. If the Authorization conditions treatment, payment, enrollment in a health plan, or eligibility for benefits on the provision of an Authorization, but is not one of the three types described in Step G(1), it is not valid. **Skip to Step 5.**

Step 2.6

Provide Patient a Copy (if applicable)

Step A Determine whether the Practice is seeking the Authorization or whether a third party is seeking the Authorization for the Practice to make a disclosure of PHI to such third party.

Step B If the Practice is seeking the Authorization, provide the individual with a signed copy of the Authorization.

Step C If the Practice is not seeking the Authorization, **proceed to Step 2.7.**

Step 2.7

Do Special Requirements Apply?

Proceed to Step 3 to determine compliance with any applicable Special Requirements.

Step 3: Confirm Compliance With Applicable Special Requirements

Introduction

This procedure should be followed by a Practice employee who has received a valid Authorization pursuant to Step 2. Subject to compliance with applicable Special Requirements, the Practice may make the PHI use or disclosure pursuant to the Authorization.

Note

The Privacy Rule does not require the Practice to act on Authorizations we receive, even if those Authorizations are valid; however, state laws may require the Practice to act on an Authorization for disclosures of PHI when the Authorization is signed by the individual.

Step 3.1

Confirm Compliance With Applicable Special Requirements (if any)

Even if you confirm that you have received a valid Authorization, you still need to confirm compliance with any applicable Special Requirements, which are the policies and procedures at PP1.12 through PP1.20.

Note that more than one Special Requirement may apply to an intended use or disclosure. For example, disclosure of HIV information about a patient as requested by and to a person whose identity is not known to the Practice triggers PP1.12, Verification, and may trigger PP1.20, Consent (special patient consent requirements may be triggered under applicable state law that are different from HIPAA requirements and that survive HIPAA preemption).

Uses and disclosures made with a valid Authorization are not subject to either Minimum Necessary, PP1.13, or Accounting, PP2.3.

Step 3.2

Make Use or Disclosure

After obtaining a valid Authorization pursuant to Step 2 and confirming compliance with any applicable Special Requirements, a Practice employee may make uses and/or disclosures of PHI as permitted in the Authorization.

Proceed to Step 4.

Step 4: Document the Authorization

Introduction

The Practice must document and retain any signed Authorization it obtains or receives.

Document Authorization

Document and retain any signed Authorization. See Documentation, PP3.4. Unless otherwise directed by the Privacy Official, place the signed patient Authorization in the Patient HIPAA File described in PP3.4.

Step 5: (If Applicable) Refrain from Making the Use or Disclosure

Introduction

This procedure should be followed by a Practice employee who has determined that he or she has received an invalid Authorization.

Step 5.1

Do Not Use or Disclose PHI

If you have determined that an Authorization is not valid, do not use or disclose PHI pursuant to that Authorization.

Step 5.2

Address Deficiency (optional)

If the Privacy Official or other properly trained person has directed you to request Authorization for a particular use or disclosure of PHI and you have determined such an Authorization is not valid, notify the Privacy Official or other appropriate party immediately.

If you receive an Authorization from a third party and you have determined that such Authorization is not valid, use your best judgment to determine whether it is appropriate to notify the individual or entity from whom you received the Authorization that the Authorization is invalid so that such individual or entity has the opportunity to correct any deficiencies. Consult with the Privacy Official if you have questions.

Note

The Privacy Rule does not require the Practice to take action to correct an invalid Authorization it receives from a third party.

Step 6: (If Applicable) Process Revocation of the Authorization

Introduction

An individual generally may revoke an Authorization at any time, provided the revocation is in writing.

Have You Received a Written Request for Revocation?

Determine whether the individual's revocation of an Authorization is in writing.

Not in Writing. If an individual asks to revoke an Authorization he or she has previously provided, but the request is not made in writing, inform the individual that to revoke an Authorization, he or she must make the revocation in writing. Do not proceed to the next step.

In Writing. If an individual revokes an Authorization in writing, proceed to process the revocation as described below.

Consider Authorization Invalid Going Forward

An individual may revoke an Authorization, provided the revocation is in writing, except to the extent the Practice has already taken action relying on the Authorization. This makes it essential to have good documentation practices when our Practice receives a revocation of an Authorization.

After a Practice employee has received a written revocation, he or she must take necessary steps to ensure that the Practice does not use or disclose PHI pursuant to the revoked Authorization. Contact the Privacy Official or the person designated by the Privacy Official to report the revocation immediately. Consult with the Privacy Official if you have questions about what other steps may be necessary.

Document Revocation

Document and retain any written revocation. Place the written revocation in the Patient HIPAA File (see Documentation, PP3.4).

Mark the original Authorization in the Patient HIPAA File to show that it is revoked and the date of revocation.

Notify Others as Appropriate

Notify Practice employees, business associates, researchers, marketing companies, and others who may have received PHI per the Authorization that the Authorization has been revoked.

F1.9

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Authorization for Use or Disclosure of Health Information

Patient Name: _____
[print or type]

Patient's Date of Birth: _____Patient's Identification/Chart No.: _____

I hereby authorize the use and disclosure of individually identifiable health information relating to me as described below:

Specific Description of the Information to be Used or Disclosed Including (if practicable) the Dates of Service(s) Related to Such Information:

_____

_____

_____

The above information will be called "Authorized Information" throughout the rest of this form.

Persons or Class of Persons Authorized to Make the Use or Disclosure of Authorized Information:

_____

_____

_____

Persons or Class of Persons to Whom the Use or Disclosure of Authorized Information May be Made:

_____

_____

Authorized Information will be used and/or disclosed for the following purposes:

☐ At the request of the individual (check box if applicable)

☐ Other (Please list each purpose of the use(s) or disclosure(s) in the space provided.):

_____

_____

■ I understand that if the person or entity receiving Authorized Information is not a health plan or health care provider covered by federal privacy regulations, the authorized information may be re-disclosed by the recipient and may no longer be protected by federal or state law.

- I understand that I may revoke this authorization at any time by notifying _____ [NAME OF PRACTICE] in writing. However, if I choose to do so, I understand that my revocation will not affect any actions taken by _____ [NAME OF PRACTICE] before receiving my revocation.
- I understand that I may refuse to sign this authorization and that my refusal to sign in no way affects my treatment, payment, enrollment in a health plan, or eligibility for benefits.
  [ALTERNATIVE, IF APPLICABLE: I understand that _____ [NAME OF PRACTICE] may require me to sign an authorization prior to receiving research-related treatment or treatment solely for the purpose of creating health information for another party and that _____ [NAME OF PRACTICE] will not provide such research-related treatment unless I provide this authorization. NOTE: If this provision is applicable, the third party for whom the information is being created must be listed under "Persons or Class of Persons to Whom the Use or Disclosure of Authorized Information May be Made." Also, the purpose for which the information is to be created and disclosed must be listed under "Authorized Information will be Used or Disclosed for the Following Purposes."
- [FOR MARKETING AUTHORIZATIONS ONLY, IF APPLICABLE] I understand that the person or entity I am authorizing to use and/or disclose Authorized Information for marketing purposes may receive either direct or indirect compensation for doing so.

This authorization expires at the earlier of _____OR the date the following

event occurs: _____
[describe event or write "not applicable"]

Signature of Patient or Patient's
Personal Representative: _____

Date: _____

For Personal Representative of the Patient (if applicable):

Print Name of Personal Representative: _____

Describe Personal Representative Relationship/Authority to Act for the Individual
(parent, guardian, etc.): _____

PERMISSIONS: DE-IDENTIFICATION PP1.10

Introduction

The Privacy Rule applies to PHI. Properly de-identified information is not PHI. This policy describes how our Practice may determine that information has been de-identified under the HIPAA Privacy Rule so that it is no longer PHI.

Policy

It is our Practice's policy to create, use, and disclose de-identified information in compliance with the HIPAA Privacy Rule. Our policy is that PHI may be de-identified only in compliance with either the safe harbor method or the expert statistician method described below.

Safe Harbor De-Identification Method

Our Practice may determine that information is de-identified information by using the "safe harbor" method. Information is de-identified according to this method only if our Practice has no actual knowledge that the de-identified information could be used to re-identify the patient, and the information does not contain any of the identifiers listed on **Form F1.10,** De-Identification Safe Harbor Checklist.

Expert Opinion De-Identification Method

Our Practice may also de-identify information by utilizing the expert opinion method. To utilize this method, each of the following facts must be confirmed and documented. This can be done through a certification from the expert as to each of these facts.

1. A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable
2. applies such principles, and
3. makes a determination that "the risk is very small" that the information can be used (i) alone or in combination with other reasonably available information, (ii) by an anticipated recipient, (iii) to identify the individual, and
4. the person documents the methods and results of the analysis that justify the determination.

Use of Business Associate to De-Identify

It is permissible to disclose PHI to a business associate of the Practice for the purpose of the business associate's de-identification of the PHI, whether or not our Practice will use the de-identified information.

Re-Identification Codes

Our Practice may assign a code or other means of record identification to allow de-identified information to be re-identified by our Practice, provided that:

1. The code or other means of record identification is not derived from or related to information about the patient and is not otherwise capable of being translated so as to identify the patient; and
2. We do not use or disclose the code or other means of record identification for any purpose, and we do not disclose the mechanism for re-identification.

Special Requirements for De-Identification by Business Associates

If we disclose PHI to someone outside our Practice for the information to be de-identified or used to create de-identified information, then follow the requirements for Business Associates, PP1.14. Do this regardless of whether the de-identified information will be used by our Practice.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

F1.10

Practice Name: _____

De-Identification "Safe Harbor" Checklist

For the de-identification "safe harbor" to apply, we must be able to answer "true" to both statements:

True _____ False _____ The Practice does not have actual knowledge that the information could be used alone or in combination with other reasonably available information to re-identify the individual.

True _____ False _____ All of the following identifiers of the *individual* or of *relatives, employers,* or *household members* of the individual have been removed or are not present:

_____ 1. Names;

_____ 2. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code, and their equivalent geocodes:

- ■ except for the initial three digits of a zip code if, according to the currently available data from the Bureau of the Census:
  - ☐ The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
  - ☐ The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000;

_____ 3. All elements of dates (except year) or dates directly relating to an individual, including:

- ■ birth date, admission date, discharge date, date of death;
- ■ and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;

_____ 4. Telephone numbers;

_____ 5. Fax numbers;

_____ 6. Electronic mail addresses;

_____ 7. Social security numbers;

_____ 8. Medical record numbers;

_____ 9. Health plan beneficiary numbers;

_____ 10. Account numbers;

_____ 11. Certificate/license numbers;

_____ 12. Vehicle identifiers and serial numbers, including license plate numbers;

_____ 13. Device identifiers and serial numbers;

_____ 14. Web Universal Resource Locators (URLs);

_____ 15. Internet Protocol (IP) address numbers;

_____ 16. Biometric identifiers, including finger and voice prints;

_____ 17. Full-face photographic images and any comparable images; ***and***

_____ 18. Any other unique identifying number, characteristic, or code (except as permitted for re-identification codes under Privacy Rule §164.514(c)).

PERMISSIONS: LIMITED DATA SET PP1.11

Introduction

Our Practice is permitted to use or disclose a Limited Data Set to recipients who will use the information only for the purposes of research, public health, or health care operations. This policy describes our Practice's policy with respect to Limited Data Set disclosures.

Policy

Our Practice may use or disclose a Limited Data Set that meets the requirements of this policy if our Practice enters into a data use agreement with a Limited Data Set recipient in compliance with this policy.

What Is a Limited Data Set?

A Limited Data Set is PHI that excludes the following direct identifiers of the patient or of relatives, employees, or household members of the patient:

1. Names;
2. Postal address information, other than town or city, state, and zip code;
3. Telephone numbers;
4. Fax numbers;
5. Electronic mail addresses;
6. Social security numbers;
7. Medical record numbers;
8. Health plan beneficiary numbers;
9. Account numbers;
10. Certificate/license numbers;
11. Vehicle identifiers and serial numbers, including license plate numbers;
12. Device identifiers and serial numbers;
13. Web Universal Resources Locators (URLs);
14. Internet Protocol (IP) address numbers;
15. Biometric identifiers, including finger and voice prints; and
16. Full-face photographic images and any comparable images.

Limited Purpose of Limited Data Set

Our Practice may use or disclose a Limited Data Set only for the purposes of research, public health, or health care operations. We may use PHI to create a Limited Data Set or disclose PHI to a business associate for such purpose, whether or not the Limited Data Set is to be used by our Practice.

Data Use Agreement

We may use or disclose a Limited Data Set only if we obtain a data use agreement signed by the Limited Data Set recipient agreeing that it will only use or disclose the PHI for limited purposes.

A data use agreement between our Practice and the Limited Data Set recipient must:

A. Establish the permitted uses and disclosures of such information by the Limited Data Set recipient. The date use agreement may not authorize the Limited Data Set recipient to use or further disclose the information in a manner that would violate HIPAA, if done by the Practice;

B. Establish who is permitted to use or receive the Limited Data Set; and

C. Provide that the Limited Data Set recipient will:

(1) Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

(2) Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

(3) Report to the Practice any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

(4) Ensure that any agents, including a subcontractor, to whom it provides the Limited Data Set agrees to the same restrictions and conditions that apply to the Limited Data Set recipient with respect to such information; and

(5) Not identify the information or contact the individuals.

Documentation

The Privacy Official shall ensure that we maintain documentation of Limited Data Set agreements in compliance with Documentation Procedures, PP3.4.

Required Action Upon Material Breach

If our Practice knows of a pattern or activity of practice of the Limited Data Set recipient that constitutes a material breach or violation of the data use agreement, we are required to take steps to cure the breach or end the violation. If such steps are unsuccessful, we are required to discontinue disclosure of PHI to the recipient and report the problem to the Secretary of HHS.

Determine Whether Special Requirements Apply

Even if the use or disclosure of PHI is proper under the standard for Limited Data Sets, the procedure below should be followed to determine whether any Special Requirements apply to the intended use or disclosure of PHI. Note: Limited Data Sets disclosures are not subject to the Disclosure Accounting Policy and Procedure, PP2.3.

Step

1 Based on the terms of the following policies and procedures, determine whether one or more of these Special Requirements apply to an intended use or disclosure of PHI:

- Verification, PP1.12
- Minimum Necessary, PP1.13
- Business Associates, PP1.14
- Personal Representatives, PP1.15
- Consistent with Notice of Privacy Practices, PP1.18
- Consistent with Other Documents, PP1.19
- Consent (State and Other Law), PP1.20

2 If one or more of the Special Requirements applies, proceed to review the policies and procedures that apply and make the use or disclosure only in compliance with applicable policies.

3 If none of the Special Requirements applies, proceed to disclose PHI in the Limited Data Set as intended.

SPECIAL REQUIREMENTS: VERIFICATION PP1.12

Note: PP1.1 through PP1.11 describe our "Permission" policies and procedures that address the various ways PHI uses and disclosures are permitted under the HIPAA Privacy Rule. PP1.12 through PP1.20 describe our "Special Requirements" policies and procedures, which are additional restrictions on PHI uses and disclosures that can apply, depending on the facts.

Overview

Introduction

Our Practice may disclose PHI to a person whose identity and whose authority to access the PHI are known to us without following any special verification procedures.

This section contains our Practice's policies and procedures to verify the identity and authority of persons requesting PHI whose identity and authority to access the PHI are not known to us. Verification is important as a barrier against the improper sharing of PHI with people other than the patient or authorized persons.

Verification is the process of confirming the identity and authority—whether by pre-existing relationship or current inquiry—of any person who requests PHI, and of obtaining any required documentation regarding that request.

Policies and Procedures

PP1.12 describes our Practices' policies and procedures relating to Verification.

Contact Person

Our Privacy Official is designated to be the contact person for questions relating to Verification and our compliance with the Privacy Rule related to Verification.

SPECIAL REQUIREMENTS: VERIFICATION PP1.12

General Policy

Policy

Our Practice's policy is to comply with the Privacy Rule requirement that, before releasing PHI, the Practice must verify the identity of any person unknown to the Practice who requests PHI and the authority of any person known or unknown to our Practice to have access to PHI. The Practice also must obtain any documentation required for release of PHI from the person requesting the PHI.

Remember: PHI cannot be used or disclosed unless the use or disclosure comes within a permission, PP1.1 through PP1.11. Verification is a Special Requirement to verify the identity and authority of the person receiving PHI. It is not itself a Permission to use or disclose PHI.

Definition

Verification: The process of confirming the identity and authority—whether by pre-existing relationship or current inquiry—of any person who requests PHI and of obtaining any required documentation regarding that request.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

Exceptions to Verification Requirements

Our policy is to verify the identity and authority of all persons requesting PHI, whether in person or by other means of communication, except for the following persons:

- a person known to the Practice as someone authorized to access the requested PHI;
- a person reasonably able to prevent or lessen the threat to health or safety of an individual or of the public in an emergency situation; or
- under circumstances where the patient is informed about a proposed disclosure of PHI to the person and has the opportunity to agree to or object to that disclosure. See Family, Friends, and Disaster Relief Organizations, PP1.6, for more details. The uses and disclosures permitted under PP1.6 are not subject to the Verification requirements.

Verification Procedures

When a person requests disclosure of PHI, follow the steps described in PP1.12, Verification—Index of Procedures.

SPECIAL REQUIREMENTS: VERIFICATION PP1.12

Index of Procedures

Introduction

Verifying the identity and authority of a person requesting PHI or otherwise receiving PHI is a multi-step process. Every employee should be able to perform Verification procedures, if the request for PHI is made to the employee. If the employee has questions, he or she should refer the matter to the Privacy Official.

The Privacy Official is responsible for reviewing Verification procedures as necessary and for handling difficult Verification procedures. As with other procedures, the Privacy Official may designate properly trained persons to assist with these functions.

Inquiry/Action Steps

Follow these steps to verify the identity and authority of a person requesting PHI:

Step	Inquiry/Action
1	Determine whether Verification is required
2	Review the Verification Procedure Guide (review more detailed information in Step 3 as needed)
3	Follow applicable Verification procedure (A–G)
4	Decline to establish identity and authority (if applicable)
5	Recognize identity and authority (if applicable)

Step 1: Determine Whether Verification Is Required

Introduction

Under the Privacy Rule, Verification is not a Permission to use or disclose PHI. It is a Special Requirement that applies to determine that the person who requests PHI is the correct person and is permitted to receive the PHI. Verification is triggered where a person requests PHI from our Practice and an exception does not apply. Verification is not required for those whose identity and authority to access the PHI are known to our Practice or in other limited circumstances described below.

Step 1.1

Identify Permission(s) for Proposed Use or Disclosure

Before any use or disclosure of PHI can be made by our Practice, it must be permitted under at least one of the Permissions in PP1.1 through PP1.11. Determine the Permission that applies. If you cannot identify a Permission for a use or disclosure, our Practice cannot release the PHI and you must decline any request that we do so.

When you have determined why the use or disclosure is permitted under the Privacy Rule (ie, identified the Permission), **proceed to Step 1.2.**

Step 1.2

Determine Whether an Exception to Verification Applies

If any exception to Verification under exception A, B, or C below applies, no Verification procedure need be conducted.

Exception A: Verification is not required when the person requesting the PHI is *known to you or the Practice* as someone authorized to access the PHI requested. The person could be "known" based on a known place of business, address, phone or fax number, or the fact that the person is known to you as the patient, or a relative or other individual involved in the patient's care.

- For example, the fact that a patient brings a person into the doctor's office when treatment information will be discussed establishes the person's identity.

Exception B: Verification is not required when a person involved in the patient's care is picking up a prescription medication for the patient, or is similarly permitted to receive PHI under Family, Friends, and Disaster Relief Organizations, PP1.6. Verification is not required for any disclosures of PHI permitted under PP1.6.

Exception C: Verification is not required for a use or disclosure of PHI in good faith to prevent or lessen a *serious threat to health or safety,* or to *apprehend a criminal* as permitted under Public Purpose, PP1.8, Public Purposes J-1 and J-2.

If any of the above exceptions to Verification applies, proceed to use or disclose the requested PHI to the person under the conditions of the Permission you identified in Step 1.1.

If none of the exceptions to Verification apply, **proceed to Step 2.**

Step 2: Review the Verification Procedure Guide

Introduction

If the person requesting PHI is not known to our Practice, and none of the exceptions to Verification set forth in Step 1 applies, the Practice must make a reasonable effort to determine that the PHI is being disclosed to a person or entity authorized to receive it. The Verification process will be different depending upon the circumstances of the request and the person making the request.

Determine Which Verification Procedure Applies

Review the Verification Procedure Guide on the following page to determine which Verification procedure to use. Consider all of the situations applicable to the request for PHI and pick the one most specific to the situation.

For example, a public official may make a request for PHI in person, but the applicable Verification procedure will be the procedure specific to a public official. Likewise, a public official may be acting as a patient's personal representative when making the request for PHI, in which case his or her status as a public official is irrelevant and the procedure for the patient's personal representative will apply.

The Verification Procedure Guide may contain the information you need to comply with our Verification procedures. If you want more detailed discussion, proceed to Step 3 and the section listed next to the applicable type of PHI request.

Verification Procedure Guide (PP1.12)

(Identity and Authority of the Person Requesting PHI Are Not Already Known)

Step 3...	If the person requesting PHI is...	Then...
A	Claiming to be the patient and in person	■ Require a driver's license, a passport, a state identification, or similar evidence of identity. ■ Request his/her social security number or other personal information that can be verified from his/her medical record. ■ The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith.
B	Claiming to be the patient, but not in person	■ Request his/her social security number or other personal information that can be verified from his/her medical record. ■ Send the PHI to a recognizable organizational mailing address. ■ Call the requestor back through the main organization switchboard rather than through a direct dial number to verify the instructions if the PHI is to be transmitted by fax or telephone or e-mail. ■ Use some other appropriate common-sense means of verifying that the person making the request is in fact the patient. ■ The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith.
C	Not the patient, but in person with the patient	■ Generally, if the patient is known to us or his or her identity is verified, and if the patient is with the person and identifies the person as someone entitled to receive the patient's PHI, that is sufficient Verification of the person's identity and authority. ■ If the patient is known to our Practice, that is sufficient Verification of the patient. If the patient is not known or recognized, verify the patient's identity under B above.
D	Not the patient, but in person without the patient	Use reasonable means to verify the person's *identity:* ■ Require a driver's license, a passport, a state identification, or similar evidence of identity. ■ The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith. Use reasonable means to verify the person's *authority.* ■ Require a copy of a power of attorney, a letter on official letterhead, a subpoena, or similar official document to evidence authority. ■ If the Permission (PP1.1 through PP1.11) you have identified for the use or disclosure of PHI requires particular documentation, statements, or representations by the person requesting PHI, request the required items and determine whether the evidence offered is sufficient. ■ In making this determination, our Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements—if our reliance is reasonable under the circumstances and is in good faith.

Step 3...	If the person requesting PHI is...	Then...
		■ For certain disclosures required by law, the condition of the Permission can be met by administrative subpoena or similar process or by a separate written statement that, on its face, shows the requirements have been met. **Note** No Verification of identity or authority is required if the person requesting PHI is permitted to receive the PHI because he or she is a family member or someone involved in the patient's care or is picking up prescription medications or otherwise permitted to receive the PHI under Family, Friends, and Disaster Relief Organizations, PP1.6.
E	Not the patient and not in person	Use reasonable means to verify the person's *identity* by: ■ Sending the PHI to a recognizable organizational mailing address, or ■ Calling the requestor back through the main organization switchboard rather than through a direct dial number to verify the instructions, if the PHI is to be transmitted by fax or telephone or e-mail, or ■ Using some other appropriate common-sense means of verifying that the person making the request is in fact the person authorized to receive the patient's PHI. Use reasonable means to verify the person's *authority*. ■ Require a copy of a power of attorney, a letter on official letterhead, a subpoena, or similar official document to evidence authority. ■ If the Permission (PP1.1 through PP1.11) you have identified for the use or disclosure of PHI requires particular documentation, statements, or representations by the person requesting PHI, request the required items and determine whether the evidence offered is sufficient. ■ In making this determination, our Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements—if our reliance is reasonable under the circumstances and is in good faith. ■ For certain disclosures required by law, the condition of the Permission can be met by administrative subpoena or similar process or by a separate written statement that, on its face, shows the requirements have been met.
F	Claiming to be patient's personal representative	Use reasonable means to verify the person's identity and authority to act for the patient as follows: ■ Examine a copy of the personal representative's court appointment as executor of a deceased patient's estate, or other reasonable evidence of the personal representative's authority. ■ Examine a copy of the power of attorney for a personal representative of an adult patient or a copy of the court appointment if the personal representative has been appointed by the court, or other reasonable evidence of the personal representative's authority to act for the patient.

Step 3...	If the person requesting PHI is...	Then...
		■ Ask questions to determine that an adult acting for a young child has the requisite relationship to the child to support his or her status as personal representative to the child. (Note: Where disclosure depends on personal representative status, this step applies in addition to any of the other steps described in this chart.)
G	Claiming to be a public official or acting on behalf of a public official	If it is reasonable under the circumstances to do so, our Practice may rely on the following to verify the *identity* of a public official or a person acting on behalf of a public official: ■ If the request is in person, presentation of an agency identification badge, other official credentials, or other proof of government status; ■ If the request is in writing, the request is on appropriate government letterhead; or ■ If the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official. If it is reasonable under the circumstances to do so, our Practice may rely on the following to verify the *authority* of a public official or a person acting on behalf of a public official: ■ A written statement of the legal authority under which the information is requested or, if a written statement of legal authority under which the information is requested would be impracticable, an oral statement of such legal authority; or ■ If the request is made pursuant to a legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

Step 3: Follow Applicable Verification Procedure

Introduction

Remember, Verification is a process of taking reasonable steps to establish the identity and the authority of an individual to have access to PHI. This amounts to taking reasonable steps to verify that the request is lawful under the Privacy Rule.

Review Verification procedures A through G below to determine which is most applicable to the specific use or disclosure of PHI.

A: If the Person Requesting PHI Is Claiming to Be the Patient and In Person

Introduction

It is our Practice's policy to provide a patient, when requested, access to his or her own PHI. Under typical circumstances, the patient's identity in person will be known to our Practice (ie, we recognize the patient in person) and the Verification procedures won't apply. If not, proceed to verify as instructed below.

A-1: Verify Identity if Patient Is In Person

If the patient is in person and is not initially known to the Practice employee interacting with the patient, establish his or her identity as follows:

- Require a driver's license, a passport, a state identification, or similar evidence of identity.
- Request his/her social security number or other personal information that can be verified from his/her medical record.
- The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith.

A-2: Patient Has Authority

The patient has authority to access his or her PHI under our Practice's policies and procedures as described in PP1.2, To the Patient, and PP2.1, Access.

B: If the Person Requesting PHI Is Claiming to Be the Patient But Not In Person

Introduction

It is our Practice's policy to provide a patient, when requested, access to his or her own PHI. Even if the patient is not in person, the patient's identity through regular communication channels often will be known to our Practice (eg, we recognize the patient's voice on the telephone) and the Verification procedures won't apply. If not, proceed to verify as instructed below.

B-1: Verify Identity if Patient Is Not In Person

If the patient is not present and is not known to us to be the person making the request for PHI, establish his or her identity as follows:

- Request his/her social security number or other personal information that can be verified from his/her medical record.
- Send the PHI to a recognizable organizational mailing address.
- Call the requestor back through the main organization switchboard rather than through a direct dial number to verify the instructions if the PHI is to be transmitted by fax or telephone or e-mail.
- Use some other appropriate common-sense means of verifying that the person making the request is in fact the patient.
- The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith.

B-2: Patient Has Authority

The patient has authority to access his or her PHI under our Practice's policies and procedures as described in PP1.2, To the Patient.

C: If the Person Requesting PHI Is Not the Patient, But In Person With the Patient

Introduction

Generally, if the patient is with the person and identifies the person as someone entitled to receive the patient's PHI, that is sufficient Verification of the person—but only if we recognize the patient (ie, the patient is known to us) or we verify the patient's identity.

C-1: Identify or Verify the Patient

If the patient is known to our Practice, that is sufficient Verification of the patient. If the patient is not known or recognized, verify the patient's identity as follows:

- Require a driver's license, a passport, a state identification, or similar evidence of identity.
- Request his/her social security number or other personal information that can be verified from his/her medical record.
- The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith.

C-2: Verify the Identity of the Person With the Patient

Generally, the fact that a person accompanies the patient and is identified by the patient is sufficient Verification of that person's identity as well.

C-3: Verify the Authority of the Person With the Patient

The most common requests for PHI by a person accompanying the patient will not require Verification because of the exception for Family, Friends, and Disaster Relief Organizations, PP1.6. Re-check the exceptions to be sure that Verification is required. Even if Verification is not required by HIPAA, our Practice employees may want to take reasonable care that persons receiving PHI are who they claim to be.

If the exception for Family, Friends, and Disaster Relief Organizations, PP 1.6, does not apply, request the permission of the patient or identify another Permission under PP1.1 through PP1.11 before releasing any PHI to the person accompanying the patient.

D: If the Person Requesting PHI Is Not the Patient But In Person Without the Patient

Introduction

If the person requesting PHI is not the patient, but is in person without the patient, usually it will be necessary to establish both the *identity* and the *authority* of the person requesting PHI before responding to his or her request for PHI.

D-1: To Establish Identity

Establish the *identity* of the person requesting PHI (if the person is not known to our Practice) according to reasonable Verification procedures, which may include one or more of the following:

- Require a driver's license, a passport, a state identification, or similar evidence of identity.
- The Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements for establishing identity—if our reliance is reasonable under the circumstances and is in good faith.

D-2: To Establish Authority

Establish the *authority* of the person requesting PHI according to reasonable Verification procedures, which may include one or more of the following:

- Require a copy of a power of attorney, a letter on official letterhead, a subpoena, or similar official document to evidence authority.
- If the Permission (PP1.1 through PP1.11) you have identified for the use or disclosure of PHI requires particular documentation, statements, or representations by the person requesting PHI, request the required items and determine whether the evidence offered is sufficient.
- In making this determination, our Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements—if our reliance is reasonable under the circumstances and is in good faith.
- For certain disclosures required by law (specifically, see Public Purpose, PP1.8, Public Purpose A), the condition of the Permission can be met by the administrative subpoena or similar process or by a separate written statement that, on its face, shows the requirements are met.

D-3: Re-check the Exceptions

If the person requesting PHI is permitted to receive the PHI because he or she is a family member or someone involved in the patient's care or is picking up prescription medications or otherwise permitted to receive the PHI under PP1.6, Family, Friends, or Disaster Relief Organizations, no Verification of identity or authority is required.

E: If the Person Requesting PHI Is Not the Patient and Not In Person

Introduction

This procedure deals with Verification when the person requesting PHI is not physically present but has made the request over the telephone, in a letter, by facsimile transmission, or by some other means of communication.

E-1: Verify the Person's Identity

Use reasonable means to verify the person's *identity* by:

- sending the PHI to a recognizable organizational mailing address, or
- calling the requestor back through the main organization switchboard rather than through a direct dial number to verify the instructions, if the PHI is to be transmitted by fax or telephone or e-mail, or
- using some other appropriate common-sense means of verifying that the person making the request is in fact the person authorized to receive the patient's PHI.

E-2: Verify the Person's Authority

Verify the *authority* of the person requesting the PHI by taking reasonable steps to verify that the requested use or disclosure of PHI is permitted under the Privacy Rule.

- Require a copy of a power of attorney, a letter on official letterhead, a subpoena, or similar official document to evidence authority.
- If the Permission (PP1.1 through PP1.11) you have identified for the use or disclosure of PHI requires particular documentation, statements, or representations by the person requesting PHI, request the required items and determine whether the evidence offered is sufficient.
- In making this determination, our Practice may rely on documentation, statements, or representations that, on their face, meet the applicable requirements—if our reliance is reasonable under the circumstances and is in good faith.
- For certain disclosures required by law (specifically, see Public Purpose, PP1.8, Public Purpose A), the condition of the Permission can be met by the administrative subpoena or similar process or by a separate written statement that, on its face, shows the requirements are met.

F: If the Person Requesting PHI Is Claiming to Be the Patient's Personal Representative

Introduction

Our Practice treats the patient's personal representative as the patient, as required by the Privacy Rule, for purposes of using and disclosing PHI of the patient.

F-1: Treat the Person as the Patient

The Privacy Rule generally requires that our Practice treat the patient's personal representative as though he or she were the patient for purposes of uses and disclosures of the patient's PHI. See Personal Representatives, PP1.15, for the Special Requirements applicable to personal representatives.

This means, generally, that if the personal representative can verify that he or she is the patient's personal representative, his or her authority to access the patient's PHI would be the same as the authority of the patient to access his or her PHI.

F-2: Verify the Personal Representative's Status

The status of a personal representative will depend upon state law. To verify the status of a personal representative of the patient, we can rely on documentation, statements, or representations that, on their face, meet the applicable requirements—if our reliance is reasonable under the circumstances and is in good faith. Rely on the following to verify authority of the personal representative:

- Examine a copy of the personal representative's court appointment as executor of a deceased patient's estate, or other reasonable evidence of the personal representative's authority.
- Examine a copy of the power of attorney for a personal representative of an adult patient or a copy of the court appointment if the personal representative has been appointed by the court, or other reasonable evidence of the personal representative's authority to act for the patient.
- Ask questions to determine that an adult acting for a young child has the requisite relationship to the child to support his or her status as personal representative to the child. Where disclosure depends on personal representative status, this step applies in addition to any of the other steps described in Subsection F-2.

G: If the Person Requesting PHI Is Claiming to Be a Public Official or Acting on Behalf of a Public Official

Introduction

Our Practice observes the Privacy Rule's special procedures for verification of the identity and authority of a public official or a person acting on behalf of a public official to permit access to PHI.

G-1: Is Requestor a Public Official?

Ask whether the requestor of PHI is a public official or acting on behalf of a public official.

A "public official" is a person who holds an office with a government entity, including, for example, public health or police.

G-2: Examine Evidence of Identity

Examine evidence of *identity* of the public official. This procedure applies only if he or she has authority to access the requested PHI by reason of his or her public official status. If it is reasonable under the circumstances to do so, our Practice may rely on the following to verify the identity of a public official or a person acting on behalf of a public official:

- if the request is in person, presentation of an agency identification badge, other official credentials, or other proof of government status;
- if the request is in writing, the request is on appropriate government letterhead; or

- if the disclosure is to a person acting on behalf of a public official, a written statement on appropriate government letterhead that the person is acting under the government's authority or other evidence or documentation of agency, such as a contract for services, memorandum of understanding, or purchase order, that establishes that the person is acting on behalf of the public official.

G-3: Examine Evidence of Authority

Examine evidence of *authority* of the public official to access PHI. If it is reasonable to do so under the circumstances, our Practice may rely on the following to verify the authority of a public official or a person acting on behalf of a public official:

- a written statement of the legal authority under which the information is requested or, if a written statement of legal authority under which the information is requested would be impracticable, an oral statement of such legal authority; or
- if the request is made pursuant to a legal process, warrant, subpoena, order, or other legal process issued by a grand jury or a judicial or administrative tribunal, it is presumed to constitute legal authority.

Step 4: Decline to Recognize Identity and Authority (if applicable)

Introduction

Our Practice, its employees and members, and its Privacy Official will observe these procedures when declining to recognize the identity or authority of an individual requesting PHI.

Step 4.1

Response Where Identity or Authority Is Not Established

If you have undertaken the steps of these Verification procedures and your reasonable inferences do not indicate that the requestor has the authority to obtain the requested PHI, decline to release the PHI.

If the request was made in person, politely tell the requestor that you are unable to release the PHI to him or her without further evidence of his or her identity and authority or some other permission to disclose under our Practice's policies and procedures and the Privacy Rule.

Step 4.2

Privacy Official's Authority to Respond

If you have questions about a request for PHI that you intend to decline for lack of Verification, the request may be referred to the Privacy Official. As with any other procedure, the Privacy Official may designate other trained employees to assist.

Step 4.3

Report the Lack of Verification

When Verification is not completed, report the incident to the Privacy Official.

Step 5: Recognize Identity and Authority (if applicable)

Introduction

When completing a Verification process by establishing the identity and authority of a person requesting or receiving PHI, our Practice will observe these procedures.

Step 5.1

Privacy Official's Authority to Respond

If you have a question about Verification of the identity or authority of an individual requesting PHI, the matter may be referred to the Privacy Official. As with any other procedure, the Privacy Official may designate other trained employees to assist.

Step 5.3

Release the PHI

If the Verification has been successfully completed, release the PHI requested, but only in accordance with the applicable Permission you identified in Step 1.

SPECIAL REQUIREMENTS: MINIMUM NECESSARY PP1.13

Overview

Introduction

The HIPAA Privacy Rule requires Covered Entities to make reasonable efforts to limit uses, disclosures, and requests for disclosure of PHI to the Minimum Necessary to accomplish the intended purpose of the use, disclosure, or request. Implementing Minimum Necessary policies and procedures will help the Practice avoid unnecessary sharing of PHI.

The Minimum Necessary requirement does not apply to disclosures to and requests by a Health Care Provider for PHI for treatment purposes. This is because such a restriction on treatment could be contrary to sound medical practice, increase medical errors, and lead to increased liability. For example, caregivers might be unable to anticipate the exact parameters of the information that other caregivers would need to diagnose or treat the patient.

The Privacy Rule also provides other exceptions to the Minimum Necessary requirement. These exceptions are described in Step 2.1.

Under the Privacy Rule, if your Practice takes reasonable steps to meet the Minimum Necessary requirement and implements reasonable and adequate Safeguards, PP3.10, then uses and disclosures that are an incidental by-product to a permitted or required use or disclosure do not violate the Privacy Rule. See PP1.7, Incidental Disclosures.

Policies and Procedures

PP1.13 describes our Practice's policies and procedures for using, disclosing, and requesting the Minimum Necessary PHI. Steps 1 and 2 apply to everyone. Steps 3–6 apply to the Privacy Official.

Contact Person

Our Privacy Official is designated to be the contact person for questions, suggestions, or complaints relating to the Minimum Necessary standard and our compliance with the Privacy Rule relating to Minimum Necessary, PP1.13.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

SPECIAL REQUIREMENTS: MINIMUM NECESSARY PP1.13

Policies and Procedures

General Policy

The Practice's policy is to make reasonable efforts to limit uses, disclosures, and requests for disclosure of protected health information (PHI) to the Minimum Necessary to achieve the purpose of the use, disclosure, or request. This includes reasonable efforts to limit each staff member's access to the Minimum Necessary PHI to carry out his or her duties. This policy applies except as described in Step 2 of the procedures for this policy.

The Practice also will take reasonable steps to avoid Incidental Disclosures that result from otherwise required or permitted uses or disclosures of PHI (see PP1.7).

Definition

Minimum Necessary is not defined in the Privacy Rule, but we use this term to describe the amount of PHI that is needed to perform a particular task or function. The Privacy Rule does not specify what the minimum amount of information is; instead, the Privacy Rule requires that our Practice specify what is the Minimum Necessary for routine types of PHI uses, disclosures, and requests, and develop criteria for determining Minimum Necessary for non-routine uses, disclosures, and requests.

Procedure

This policy applies to all PHI uses, disclosures of, and requests by the Practice, subject to the exceptions listed in Step 2.1.

When you need to make a PHI request, use, or disclosure, follow the steps described in PP1.13, Minimum Necessary.

SPECIAL REQUIREMENTS: MINIMUM NECESSARY PP1.13

Index of Procedures

Introduction

The requirement to use, disclose, or request the Minimum Necessary information arises in a number of circumstances, including in our Practice's internal operations, our disclosures of information to external entities, and our requests for disclosures from external entities.

Steps 1 and 2 below apply to all employees. Minimum Necessary compliance means that each employee must ensure that his or her own conduct complies with the Minimum Necessary policies and procedures.

Steps 3–6 apply to the Privacy Official. Implementing the Minimum Necessary requirement means the Privacy Official must oversee development of specific Minimum Necessary policies and procedures.

Inquiry/Action Steps

Use the following procedures to apply the Minimum Necessary standard:

Step	Inquiry/Action
All Employees:	
1	Review the Quick Reference Guide
2	Determine compliance with the Minimum Necessary standard
Privacy Official:	
3	Establish Minimum Necessary staff access to PHI
4	Develop policies and procedure for routine disclosures
5	Develop policies and procedures for routine requests
6	Develop reasonable criteria for non-routine uses, disclosures, and requests

Step 1: Review the Quick Reference Guide

Introduction

The Quick Reference Guide (Chapter 1, Section 1.2) contains a column dedicated to Minimum Necessary. This means that for every PHI use, disclosure, or request listed in the Quick Reference Guide, the Privacy Official will indicate whether the Minimum Necessary requirement applies, and if so, how it applies.

Step 1.1

Follow Quick Reference Guide

If the use, disclosure, or request is listed in the Quick Reference Guide:

- If the Minimum Necessary requirement applies, as shown in the Minimum Necessary column, follow the Privacy Official's instructions and use, disclose, or request only the PHI listed in the Minimum Necessary column of the Quick Reference Guide.

Note

Each employee or member of the workforce must take care to access only the Minimum Necessary PHI for his or her use.

- If the Minimum Necessary requirement does not apply, as shown in the Minimum Necessary column of the Quick Reference Guide, Minimum Necessary, PP1.3, proceed to use, disclose, or request PHI pursuant to Permissions (PP1.1–1.11) and comply with any other applicable Special Requirements (PP1.12–1.20).

Step 1.2

If the use, disclosure, or request is not set forth in the Quick Reference Guide, **proceed to Step 2.**

If Necessary, Proceed to Step 2

Step 2: Determine Compliance With the Minimum Necessary Standard

Introduction

Certain uses, disclosures, and requests for disclosure of PHI must reasonably be limited to the Minimum Necessary for the intended purposes.

Remember: Each use or disclosure must come within a permission, PP1.1 through PP1.11. Then, use the following procedure to make reasonable efforts to limit uses and disclosures of PHI to the Minimum Necessary where required.

Use Step 2.1 to determine whether the Minimum Necessary requirement applies.

Use Steps 2.2 and 2.3 to determine the Minimum Necessary amount of information for the intended PHI use, disclosure, or request.

Step 2.1

Does Any Exception to Minimum Necessary Requirement Apply?

Determine whether the use, disclosure, or request meets any of the following specific exceptions to the Minimum Necessary requirement:

- the disclosure is to or requested by a health care provider and is for treatment purposes,
- the disclosure is to or for use by the individual and is either permitted or required by HIPAA,
- the use or disclosure is pursuant to a valid Authorization,
- the disclosure is to the Secretary of HHS in order to determine compliance with HIPAA,
- the use or disclosure is required by law, or
- the use or disclosure is required for compliance with the HIPAA "administrative simplification" rules, including the Privacy rule.

If the PHI use, disclosure or request does not meet any of the above exceptions, the Minimum Necessary requirement applies. **Proceed to Step 2.2.**

If it does meet an exception, then the Minimum Necessary, PP1.13, requirement does not apply. Proceed to use, disclose or request PHI pursuant to Permissions (PP1.1-1.11) and comply with any other Special Requirements (PP1.12-1.20).

Step 2.2

Is the Use, Disclosure, Request Routine?

Step A Determine whether the use or disclosure or request is a routine use, disclosure, or request for our Practice that has not been included in the Quick Reference Guide.

Step B If the use, disclosure, or request is routine but not listed in the Quick Reference Guide, propose to the Privacy Official that the use, disclosure, or request be added to the Quick Reference Guide and determine with the Privacy Official how the Minimum Necessary requirement applies in the Quick Reference Guide.

Step C If the use, disclosure, or request is not routine, **proceed to Step 2.3.**

Step 2.3

If Not Routine, Review on Individual Basis

If the use, disclosure, or request is not routine, the Privacy Official or other trained employees or members of the workforce must separately review each proposed use, disclosure, or request according to the criteria developed for that purpose by the Practice, using their professional judgment.

Criteria for non-routine uses will be developed by the Privacy Official or other trained employees or members of the workforce, with the participation of physicians and other employees in our Practice; will be in writing; and should be based upon a professional determination of the Minimum Necessary amount of PHI, in our Practice's setting, to accomplish the purpose of the use, disclosure, or request.

Remember: The use, disclosure, or request must come within a Permission (PP1.1–1.11) and must be in compliance with any other applicable Special Requirements (PP1.12–1.20).

Step 2.4

(If Applicable) Entire Medical Record

Consider whether the entire medical record is being used, disclosed, or requested. The Practice must provide specific justification for any use or disclosure of, or request for, a patient's entire medical record. This specific justification can be stated as a standard protocol in the Quick Reference Guide or in another manner that is applicable to routine uses, disclosures, and requests. Absent such a statement, if the Minimum Necessary standard applies, there must be a specific justification in connection with the use, disclosure, or request of the entire medical record.

Note

Use, disclosure, or request regarding an entire medical record without an exception or other specific justification can be a presumptive violation of these policies and procedures and the Privacy Rule.

Note

Regardless of whether the Minimum Necessary standard applies, in making a permitted or required disclosure, take care to avoid incidental disclosures of PHI. See Incidental Disclosures, PP1.7.

Step 3: Establish Minimum Necessary Staff Access to "Uses" of PHI

Introduction

The Practice must limit each staff member's access to PHI to the Minimum Necessary amount to carry out his or her duties and responsibilities on behalf of the Practice ("access to" PHI basically means "use of" PHI). Think of this as "need to know" clearance for access to PHI.

The purpose of this restriction is to avoid unnecessary access to PHI by staff members who do not need such information in order to treat the individual or to carry out other duties on behalf of the Practice.

The Privacy Official shall use this procedure to make reasonable efforts to limit staff access to PHI to the Minimum Necessary.

Step 3.1

List Those With Access to PHI

With modifications to Workforce Form, F1.13A, as appropriate, the Privacy Official makes a list of all Practice employees, Practice volunteers, and other workforce members who might have access to PHI collected by or on behalf of the Practice.

Step 3.2

Identify Access Needs

The Privacy Official, in consultation with staff, identifies in Form F1.13A the persons or classes of persons who need access to PHI to carry out their duties.

Form F1.13A, like Forms F1.13B, C, and D, is a tool to assist the Privacy Official in setting standards for routine uses, disclosures, and requests, and in completing the Minimum Necessary column of the Quick Reference Guide for routine uses, disclosures, and requests.

Step 3.3

Identify PHI Needed

The Privacy Official identifies in form F1.13A the categories of PHI to which such persons or classes of persons identified in Step 3.2 need access.

Step 3.4

Limit Access to PHI

The Privacy Official and Practice management establish reasonable precautions to limit each person's access to only the PHI that is necessary for such person to carry out his or her duties. Such steps should take into account the potential for incidental disclosures of PHI in the course of each person's everyday access to PHI.

Step 3.5

Implement Safeguards

Coordinate these efforts with measures to implement Safeguards, PP3.10, under Procedures AP5 (Access Control/Personnel Security/Termination Procedure), PS2 (Media Controls), and TSS1 (Computer Access, Audit, and Authorization Controls).

Step 3.6

Document Procedures

Retain documentation reflecting that the Practice has taken Steps 3.1 through 3.5.

Step 3.7

Continue to Monitor

Monitor access and system use. Address any incidents that arise under Safeguards, PP3.10, Procedure AP6 (Internal Audit/Security Incident).

Step 4: Develop Policies and Procedures for Routine PHI Disclosures

Introduction

The Practice must put in place policies and procedures (including standard protocols) for disclosures of PHI that the Practice makes on a routine or recurring basis. Policies and procedures must be tailored to our Practice's regular operations. The following steps will assist the Practice in developing policies and procedures for routine disclosures.

Remember: The use, disclosure, or request must come within a Permission (PP1.1–1.11) and must be in compliance with any other applicable Special Requirements (PP1.12–1.20).

Step 4.1

Identify Routine Uses and Disclosures

The Privacy Official will use the chart for disclosures attached hereto as the Minimum Necessary Worksheet—Routine PHI Disclosures, Form F1.13C, as an assessment tool to identify disclosures routinely made by the Practice by the following characteristics:

- the type of PHI to be used or disclosed,
- the types of persons who will use or who will receive the disclosure,
- the conditions that will apply to the use or disclosure, and
- the purpose for which the PHI will be used or disclosed.

Step 4.2

Analyze Routine Disclosures

For each type of disclosure routinely made by the Practice, the Privacy Official will determine whether the Minimum Necessary requirement applies by following Step 2.1 of this procedure. He or she will identify key characteristics for each type of disclosure that meets an exception to the Minimum Necessary requirement.

Step 4.3

Do Routine Disclosures of PHI Meet Reliance Criteria?

For each type of disclosure routinely made by the Practice, determine whether the disclosure is in response to a request made by:

- a public official and related to a permissible use or disclosure of PHI;
- another entity that is a Covered Entity under HIPAA;
- a professional who is a member of the Practice's workforce and who is requesting the use or disclosure for the purpose of providing professional services;
- a professional who is a Business Associate of the Practice who is requesting the use or disclosure for the purpose of providing business assistance to the Practice; or
- a researcher for the purpose of research and supported by documentation proving that an alteration to or waiver of the individual Authorization generally required for use or disclosure of PHI has been approved by a proper Institutional Review Board or privacy board.

For each type of disclosure identified under the above criteria, the Practice may reasonably rely upon the requestor's assertion that only the Minimum Necessary PHI is being disclosed. Such an assertion should be documented if the Practice chooses to rely on the assertion.

Step 4.4

Develop Protocols

For any remaining disclosures originally identified under Step 4.1 above, the Privacy Official will classify those requests based on the information described in Step 4.1, identify the physicians and other employees within the Practice who are most familiar with the records involved for each category of use or disclosure, and work with them to develop protocols for identifying the information that should be included in any response to the request.

Form F1.13C, like Forms F1.13A, B and D, is a tool to assist the Privacy Official in setting standards for routine uses, disclosures, and requests and in completing the Minimum Necessary column of the Quick Reference Guide for routine uses, disclosures, and requests.

Note

For practices with electronic medical records, the Practice may elect to develop predefined search parameters to automatically identify Minimum Necessary information for routine uses and disclosures. Alternatively, the Practice may elect to acquire a tool from a vendor that is capable of performing such functions.

Step 5: Develop Policies and Procedures for Routine PHI Requests

Introduction

The Practice must put in place policies and procedures (including standard protocols) for requests for PHI that the Practice makes on a routine or recurring basis. Policies and procedures must be tailored to our Practice's regular operations. The following steps will assist the Practice in developing policies and procedures for routine requests.

Remember: The use, disclosure, or request must come within a Permission (PP1.1–1.11) and must be in compliance with any other applicable Special Requirements (PP1.12–1.20).

Step 5.1

Identify Routine Requests

The Privacy Official, modifying the chart for requests attached hereto as Minimum Necessary Worksheet—Routine PHI Requests, Form F1.13D, will identify requests routinely made by the Practice by the following characteristics:

- type of PHI to be requested,
- types of persons who will receive the requests,
- conditions that will apply to the requests, and
- purpose for which the PHI will be requested.

Step 5.2

Analyze Routine Requests

For each type of request routinely made by the Practice, the Privacy Official will determine whether the Minimum Necessary standard applies by following Step 2.1 of this Procedure. He or she will identify key characteristics for each type of request that meets an exception to the Minimum Necessary requirement.

Step 5.3

Do Routine Requests of PHI Meet Reliance Criteria?

For each type of request routinely made by the Practice, determine whether the request is made:

- to another entity that is a Covered Entity under HIPAA;
- by a professional who is a member of the Practice's workforce and who is requesting the PHI for the purpose of providing professional services;

- by a Business Associate of another Covered Entity who is providing business assistance to the Covered Entity; or
- by a researcher in our Practice for the purpose of research and supported by documentation proving that an alteration to or waiver of the individual Authorization generally required for use or disclosure of PHI has been approved by a proper Institutional Review Board or privacy board.

For each type of disclosure identified under the above criteria, the Practice should request the Minimum Necessary PHI and assert that only the Minimum Necessary PHI is being disclosed. The recipient of the request may choose to rely on our Practice's assertion that only the Minimum Necessary PHI is requested.

Step 5.4

Develop Protocols

For any remaining requests originally identified under Step 5.1 above, the Privacy Official will classify those requests based on the information described in Step 5.1, identify the physicians and other employees within the Practice who are most familiar with the records involved for each category of request, and work with them to develop protocols for identifying the information that should be included in any request.

Form F1.13D, like Forms F1.13A, B, and C, is a tool to assist the Privacy Official in setting standards for routine uses, disclosures, and requests and in completing the Minimum Necessary column of the Quick Reference Guide for routine uses, disclosures, and requests.

Step 6: Develop Reasonable Criteria for Non-routine Uses, Disclosures, and Requests

Introduction

The Practice must use criteria to guide individual determinations that PHI in non-routine uses, disclosures, and requests is the Minimum Necessary reasonable to achieve the purpose for which the use, disclosure, or request was made. Policies and procedures must be tailored to our Practice's PHI. The following steps will assist the Privacy Official in developing criteria for non-routine uses, disclosures, and requests.

Step 6.1

Privacy Official to Identify Non-Routine Types of Uses, Disclosures, and Requests for PHI

Using data accumulated in Steps 3, 4, and 5, the Privacy Official will identify types of non-routine uses, disclosures, and requests for PHI our Practice experiences or is likely to experience from time to time.

Step 6.2

Criteria for Evaluating Non-Routine Uses, Disclosures, and Requests for PHI

Criteria for non-routine uses, disclosures, and requests will be developed by the Privacy Official with the participation of physicians and other employees in our Practice, will be in writing, and should be based upon a professional determination of the minimum amount of PHI necessary, in our Practice's setting, to accomplish the purpose of the non-routine use, disclosure, or request.

Appropriate criteria should include the following:

- The use, disclosure, or request is permissible under HIPAA (see Permissions, PP1.1 through PP1.11, and Special Requirements, PP1.12 through PP1.20).
- An Authorization for the use, disclosure, or request has been obtained, if required. See Authorization, PP1.9.
- The Practice has not agreed to additional privacy restrictions. See Further Restrictions, PP2.5.
- The patient has not objected to the disclosure and has had an opportunity to do so. See Family, Friends, and Disaster Relief Organizations, PP1.6.
- When established, the Privacy Official will add the written criteria for non-routine uses, disclosures, or requests to the Quick Reference Guide.

Step 6.3
Reasonably Rely on the Requestor of PHI

The criteria should include exceptions and situations permitting the Practice to reasonably rely on the requestor of the information as criteria for evaluating non-routine requests as described in Step 4.3.

F1.13A

Minimum Necessary Workforce Form

Name of Practice:

Address:

Privacy Official:

Telephone:

Practice workforce (also see F3.5A)	Person/class of persons who need access to PHI	Permitted PHI access	Need for access	Precautions/safeguards to limit access (see PP3.10)
Employees	Billing staff	Coding/encounter sheets	Billing and payment activities	
	Physicians	Entire chart	Payment Treatment	Adopt policy not to look at PHI not subject to permission
	Receptionist			
Volunteers				
Business associates				

F1.13B

Minimum Necessary Worksheet—Routine PHI Uses

Name of Practice:

Address:

Privacy Official:

Telephone:

Last Udated: _____

Type of Use	Purpose for Use	Information Used	User/Workforce Members(s) with Access	User Category	Rule Permission for Use	Where PHI Stored	Minimum Necessary	Comments

Minimum Necessary Worksheet—Routine PHI Disclosures

Name of Practice:

Address:

Privacy Official:

Telephone:

Last Udated: _____

Type of Disclosure	Purpose for Disclosure	Information Disclosed	Recipient	PHI Requested?	Recipient Category	Rule Permission for Disclosure	Minimum Necessary	Comments

F1.13D

Minimum Necessary Worksheet—Routine PHI Requests

Name of Practice:

Address:

Privacy Official:

Telephone:

Last Udated: _____

Type of Request	Purpose for Request	Information Requested	Person Making Request/ Receiving Access	Requestor Category	Basis for Request	Where PHI Stored	Minimum Necessary	Comments

SPECIAL REQUIREMENTS: BUSINESS ASSOCIATES PP1.14

General Policy

It is our Practice's policy to enter into a Business Associate Amendment with all Business Associates of the Practice before disclosing PHI to a Business Associate or allowing a Business Associate to create or receive PHI on behalf of the Practice.

Business Associate List in Quick Reference Guide

The Quick Reference Guide contains a list of Business Associates of our Practice with whom we have a Business Associate Amendment. Check with the Privacy Official if you have any questions.

What Is a "Business Associate"?

A person or entity can be a Business Associate under either of the following definitions:

- A person or entity that performs or assists in the performance of a service or function on behalf of the Practice when the function or activity involves the use or disclosure of individually identifiable health information. This includes:
  - ☐ claims processing or administration;
  - ☐ data analysis, processing, or administration;
  - ☐ utilization review;
  - ☐ quality assurance;
  - ☐ billing;
  - ☐ benefit management;
  - ☐ practice management;
  - ☐ repricing; or
  - ☐ any other function or activity regulated by the Privacy Rule.
- A person to whom PHI is disclosed by the Practice (or another Business Associate of the covered entity) and who provides any of the following types of professional services to or for the Practice: legal, actuarial, accounting, consulting, data aggregation, management, administration, accreditation, or financial.

Business Associate Amendments

The Standard Business Associate Amendment (F1.14A) will be used for all Business Associates of the Practice. Any change to this Standard Amendment must be approved by the Privacy Official. The Privacy Official will seek advice from legal counsel regarding any changes to the Standard Amendment as appropriate.

Exhibit A of the Standard Business Associate Amendment must be completed for each Business Associate. This exhibit describes the types of uses and disclosure of PHI that are permitted by the particular Business Associate.

"Contract Consideration": Obligations of the Practice to the Business Associate

> **Note**
>
> The Privacy Official will discuss with legal counsel the issue of "contract consideration" when the Business Associate Amendment is used to modify an already existing agreement for services.

If the Business Associate Amendment is included with the "main" contract between the parties at the time of signing, the "consideration" that otherwise exists for the main contract may meet this requirement (discuss with legal counsel).

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

If the Business Associate Amendment is signed after the main agreement was signed, address whether the obligations of the Practice in the Business Associate Amendment meet applicable requirements for "contract consideration."

The Privacy Official should discuss with legal counsel other possible approaches to consideration, including paying some modest monetary amount to the Business Associate (eg, $50 to $100) or including other obligations of the Practice.

Paragraph 1 of the Standard Business Associate Amendment (F1.14A) is drafted to allow the Practice to select the appropriate form of contract consideration by initialing next to the chosen option.

Documentation of Business Associate Amendments

Step A Use the Business Associate Amendment Log (F1.14B) to document the following for all Business Associate Amendments:

- Name of Business Associate
- Date Business Associate Amendment signed
- Date Business Associate Amendment terminates

Step B File the signed Business Associate Amendment and a copy of the Agreement it amends (if applicable) in a central file of Business Associate Amendments.

Periodic Review of Status of Business Associate Amendments

The Privacy Official will periodically review the Business Associate Amendment Log (F1.14B) to assure that Business Associate Amendments are in effect with respect to all Business Associates to whom the Practice discloses PHI. The Privacy Official will also cross-reference to Form F1.13A, Minimum Necessary Workforce Form, which includes information on "Minimum Necessary" restrictions on PHI uses, disclosures, and requests by Business Associates.

Policy: Business Associate Violations

The Privacy Official will make appropriate inquiry or investigation into any complaints about Business Associates or any information indicating that a Business Associate may have breached the Business Associate Agreement.

If the Practice becomes aware of a pattern of activity or practice of a Business Associate that constitutes a material breach or violation of the Business Associate's obligations under the Business Associate Amendment, the Practice, through the Privacy Official, will:

- take reasonable steps to cure the breach or end the violation;
- terminate the contract; *or*
- report the problem to the Secretary of HHS.

Complaints regarding the practices of Business Associates will be received and documented according to the policy and procedure for Complaints (PP2.6).

Policy: Mitigation of Harm Done By Business Associate

Our policy is to mitigate, to the extent practicable and required by the Privacy Rule, any harm that results from a privacy breach or violation by a Business Associate.

Termination of Business Associate Amendment

When a Business Associate Amendment terminates, whether by natural expiration of its term or when terminated by either party for any reason, the Privacy Official will assure that all PHI disclosed to the Business Associate pursuant to the Amendment is either returned, destroyed, or retained by the Business Associate under extended protection of the Business Associate Amendment. The Privacy Official will complete the Business Associate Amendment Termination Form (F1.14C) for each termination.

Business Associate Documentation

Business Associate documentation shall be maintained in accordance with the policy and procedure for Documentation (PP3.4).

F1.14A

Medical Practice HIPAA Business Associate Amendment Terms and Conditions

Business Associate: _____

Medical Practice: _____

Describe Agreement Between Business Associate and Medical Practice: _____

_____

Effective Date of these Terms and Conditions:_____
(April 14, 2003, unless otherwise indicated)

In consideration of the Parties' continuing obligations under the above-referenced agreement and other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, Business Associate, as defined above, and Medical Practice, as defined above, hereby agree to amend the above-referenced agreement between Business Associate and Medical Practice by inclusion of these Terms and Conditions (these Terms and Conditions and the agreement are hereby collectively referred to as "the Agreement" or "this Agreement"). These Terms and Conditions are effective as of the Effective Date specified above.

Capitalized terms used, but not otherwise defined in this Agreement, shall have the same meaning as those terms in the HIPAA "Privacy Rule," (the "Standards for the Privacy of Individually Identifiable Health Information"), which is codified at 45 C.F.R. Parts 160 and 164.

Medical Practice is a "Covered Entity" within the meaning of the Privacy Rule. Medical Practice has or will disclose "protected health information" to Business Associate in connection with the services provided to Medical Practice, and Business Associate is or may become a "Business Associate" of Medical Practice under the Privacy Rule.

"Protected Health Information" or "PHI," as used in this Agreement, means (subject to the definition provided at 45 C.F.R. § 164.501) individually identifiable health information that Business Associate receives from Medical Practice or that it creates or receives on behalf of Medical Practice in connection with the performance of the services under this Agreement by Business Associate.

These Terms and Conditions are intended to comply with the requirements for Business Associate agreements under the HIPAA Privacy Rule and are to be construed to achieve compliance with those requirements.

1. Contract Consideration. The following provision that is initialed and dated by both parties is hereby incorporated into these Terms and Conditions (initial and date only one provision, and only the initialed and dated provision is made part of these Terms and Conditions):

Bus. Assoc. Initials/Date	Practice Initials/Date	
_____	_____	A. The parties agree that these Terms and Conditions are hereby incorporated into and executed simultaneously with the above-referenced agreement.
_____	_____	B. In consideration of _____ dollars ($___.00) paid to Business Associate at the time of execution of these Terms and Conditions, Business Associate agrees to the Terms and Conditions as provided herein.
_____	_____	C. Medical Practice obligations with respect to these terms and conditions are contained in Exhibit B attached hereto and incorporated herein by reference.

2. Uses and Disclosures Permitted by HIPAA. Business Associate may use or disclose PHI only as permitted in Exhibit A attached hereto and incorporated herein by reference. Notwithstanding Exhibit A, Business Associate may not use or further disclose the information in a manner that would violate the requirements of the HIPAA Privacy Rule, if done by the Medical Practice, except that Business Associate may use and disclose PHI for the proper management and administration of Business Associate or to carry out the legal responsibilities of Business Associate consistent with the provisions of 45 C.F.R. § § 164.504(e)(4)(i) and (ii). Business Associate may only disclose PHI for such purposes if:

    a) the disclosure is required by law; or

    b) Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and will be used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

    c) Business Associate will not use or further disclose PHI other than as permitted or required by this Agreement or as required by law.

3. Uses and Disclosures Permitted By Agreement or By Law. Business Associate will not use or further disclose PHI other than as permitted or required by this Agreement or as required by law.

4. Safeguards. Business Associate will use appropriate safeguards to prevent the use or disclosure of PHI other than as provided for by this Agreement.

5. Mitigation. Business Associate agrees to mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of PHI by Business Associate in violation of the requirements of this Agreement.

6. Reporting of Certain Disclosures. Business Associate will report to Medical Practice any use or disclosure of PHI not provided for by this Agreement of which it becomes aware.

7. Agents/Subcontractors. Business Associate will ensure that any agent of Business Associate, including a subcontractor of Business Associate, to whom it provides PHI received from or created or received by Business Associate on behalf of Medical Practice, agrees to the same restrictions and conditions that apply to Business Associate with respect to such information.

8. Access. Business Associate agrees to provide access to PHI at the request of Medical Practice, and in the time, manner, and place designated by Medical Practice, to Medical Practice or, as directed by Medical Practice, to an individual in order to meet the requirements under 45 CFR § 164.524. The obligations of Business Associate in this Paragraph apply only to PHI in "designated record sets" in Business Associate's possession or control as such term is defined at 45 C.F.R. § 164.501.

9. Amendment. Business Associate will make PHI available to Medical Practice in the time, manner, and place designated by the Medical Practice, to the extent required for amendment and incorporate any amendments to PHI in accordance with 45 C.F.R. § 164.526, which describes the requirements applicable to an individual's request for an amendment to the PHI relating to the individual. The obligations of Business Associate in this Paragraph apply only to "designated record sets" in Business Associate's possession or control as such term is defined at 45 C.F.R. § 164.501.

10. Accounting. Business Associate will make PHI and information related to disclosures of PHI by Business Associate available to the Medical Practice in the time, manner, and place designated by the Medical Practice, to the extent required to provide an accounting of disclosures in accordance with 45 C.F.R. § 164.528, which describes the requirements applicable to an individual's request for an accounting of disclosures of PHI relating to the individual. Business Associate agrees to document such disclosures of PHI and information related to such disclosures as would be required for Medical Practice to respond to a request by an individual for an accounting of disclosures of PHI in accordance with 45 C.F.R. § 164.528.

11. HHS Access. If Business Associate receives a request, made on behalf of the Secretary of the Department of Health and Human Services, that Business Associate make its internal practices, books, and records relating to the use and disclosure of PHI available to the Secretary of the Department of Health and Human Services for purposes of determining Medical Practice's compliance with the HIPAA Privacy Rule, then Business Associate will promptly comply with the request; provided, however, that this provision shall not apply in the event a court of competent jurisdiction determines, in response to a challenge raised by Medical Practice, that the Privacy Rule provision requiring the inclusion of this provision in the Terms and Conditions is void or otherwise unenforceable.

12. Breach. Upon Medical Practice's knowledge of a material breach of these Terms and Conditions by Business Associate, Medical Practice shall provide an opportunity for Business Associate to cure the breach or end the violation. If Business Associate does not cure the breach or end the violation within the time specified by Medical Practice, Medical Practice may terminate this Agreement. If Business Associate has breached a material term of this Agreement and cure is not possible, Medical Practice may immediately terminate this Agreement.

13. Return or Destruction of PHI. Upon termination of this Agreement for any reason, if feasible, Business Associate will return or destroy all PHI received from Medical Practice or created or received by Business Associate on behalf of Medical Practice that Business Associate still maintains in any form and retain no copies of such information. If such return or destruction is not feasible, Business Associate will extend the protections of this Agreement to the information retained and limit further uses and disclosures to those purposes that make the return or destruction of the information infeasible.

14. Termination. The Term of these Terms and Conditions shall terminate when all of the Protected Health Information provided by Medical Practice to Business Associate, or created or received by Business Associate on behalf of Medical Practice, is destroyed or returned to Medical Practice.

15. No Third Party Beneficiary. These Terms and Conditions are intended for the sole benefit of the Business Associate and Medical Practice and do not create any third party beneficiary rights, except to the extent that the Privacy Rule validly requires the Secretary of the Department of Health and Human Services or any other person to be a third party beneficiary to this Agreement.

16. Amendment of Terms and Conditions. These Terms and Conditions cannot be amended except by the mutual written agreement of Business Associate and Medical Practice.

17. Amendment for Compliance. In the event that any provision of these Terms and Conditions is held by a court of competent jurisdiction to be invalid or unenforceable, the remainder of the provisions of this Agreement will remain in full force and effect. In addition, in the event Medical Practice believes in good faith that any provision of the Terms and Conditions fails to comply with the then-current requirements of the HIPAA Privacy Rule, Medical Practice shall notify the Business Associate in writing. For a period of up to thirty days, the parties shall address in good faith such concern and shall amend the terms of this Agreement, if necessary to bring it into compliance. If after such thirty-day period these Terms and Conditions fail to comply with the HIPAA Privacy Rule with respect to the concern(s) raised pursuant to this Paragraph, then Medical Practice has the right to terminate this Agreement upon written notice to Business Associate.

BUSINESS ASSOCIATE

By: _____

Name (Print): _____

Title: _____

Date: _____

MEDICAL PRACTICE

By: _____

Name (Print): _____

Title: _____

Date: _____

Exhibit A to Medical Practice
Business Associate Amendment

Permitted Uses and Disclosure of Protected Health Information by Business Associate

Business Associate may use and disclose Protected Health Information only for purposes of providing services to Medical Practice. Business Associate shall use, further disclose, and request PHI only in compliance with Medical Practice's "Minimum Necessary" policies and procedures as maintained and revised by the Medical Practice. Subject to the terms of this Agreement, permitted PHI uses and disclosures include the following:[1]

> [Business Associate to provide descriptive list for review by Medical Practice and for the completion of this Exhibit.]

---

1. Note: Describe the permitted uses and disclosures of PHI that may be made by the Business Associate in connection with the engagement. In its December 2000 commentary, HHS commented on the degree of specificity that the Privacy Rule requires in describing permitted uses and disclosures:

   > the Business Associate contract [is not required to] specify each and every use and disclosure of protected health information permitted to the Business Associate. Rather, the contract must state the purposes for which the Business Associate may use and disclose protected health information, and must indicate generally the reasons and types of persons to whom the Business Associate may make further disclosures.

   65 Fed. Reg. 82505. While the above language indicates that at least some level of specificity is required, HHS stated in the August 2002 commentary to the final modifications to the Privacy Rule that "The Department clarifies that the business associate provisions may be satisfied by standard or model contract forms which could require little or no modification for each covered entity." 67 Fed. Reg. 53252. If such an unmodified form contract may be used, then the specificity of permitted uses and disclosures may be less than previously indicated by HHS. But keep in mind that the Practice has obligations with respect to "minimum necessary" and business associates.

Exhibit B to Medical Practice
Business Associate Amendment
(Use Only if Applicable)

Medical Practice Obligations

[Use this Exhibit only if the Medical Practice intends to describe promises that the Medical Practice can reasonably make to support contract consideration of the Business Associate Amendment (see Section 1 of the Amendment). Any promises that the Practice makes should be incorporated into the Practice's Polices and Procedures.]

F1.14B

Name of Practice:

Address:

Privacy Official:

Telephone:

Business Associate Amendment Log

Name of Business Associate (BA)	Description (and Date) of Main Agreement With the BA	Date BA Amendment Effective	Date Main Agreement Terminates

F1.14C

Name of Practice:

Address:

Privacy Official:

Telephone:

Business Associate Amendment Termination Form

Name of Business Associate: _____

Date Amendment Terminated: _____

Reason for Termination:

Disposition of Protected Health Information:

Name of Person Completing Form: _____ Date Completed: _____

SPECIAL REQUIREMENTS: PERSONAL REPRESENTATIVES PP1.15

General Policy

It is the Practice's policy to treat the "Personal Representative" of a patient just as we would the patient with respect to disclosures of PHI, access to PHI, and exercise of patient HIPAA rights. Our Practice will follow both HIPAA requirements and applicable state law in this area.

Note

The application of this Personal Representative Policy and Procedure in a particular state will be highly dependent on relevant state laws. The Privacy Official, consulting with legal counsel as appropriate, will use Form F1.15A, sections A through D to describe applicable state laws.

What is a Personal Representative?

The Privacy Rule specifies who may act as a Personal Representative for the following three categories of persons:

If the patient is . . .	**Then the personal representative is . . .**
a deceased individual (or the deceased individual's estate)	the executor, administrator, or other person who has the authority under state law to act on behalf of the deceased individual or the individual's estate.
an adult or emancipated minor	the person who has the authority under state law to act on behalf of the adult or emancipated minor **in making decisions related to health care**
an unemancipated minor	the parent, guardian, or a person acting in the place of a parent who has the authority under applicable state law to act on behalf of an unemancipated minor **in making decisions related to health care.**

Note

The key question for the purposes of determining whether a person is a Personal Representative under HIPAA for adults and minors is whether state law authorizes that person to make decisions related to health care.

The Scope of Personal Representation

When a person qualifies as a Personal Representative of a patient, the person must be treated as the patient with respect to uses and disclosures as well as the patient's rights under the HIPAA Privacy Rule.

However, an individual who qualifies as the Personal Representative of a patient may only be treated as the Personal Representative with respect to PHI that relates to the scope of that particular representation.

For example: A person with a limited health care power of attorney for a patient with respect to a specific treatment, such as artificial life support, may only be treated as that patient's Personal Representative with respect to PHI that relates to that particular health care decision.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

Adults and Emancipated Minors

Part A of PP1.15 describes our Practice's policies and procedures for determining when the Practice may treat a person as the Personal Representative of an adult or emancipated minor.

Deceased Individuals

Part B of PP1.15 describes our policies and procedures for determining when the Practice may treat a person as the Personal Representative of a deceased individual.

Unemancipated Minors

Part C of PP1.15 describes our policies and procedures for determining when the Practice may treat a person as the Personal Representative of an unemancipated minor.

Parental Access Under State Law

Part D of PP1.15 describes our policies and procedures for determining when the Practice may disclose to or provide access to a parent, guardian, or person acting in the place of a parent **even when** the person does not qualify as a Personal Representative under the HIPAA Privacy Rule as covered in Part C.

The Difference Between Emancipated and Unemancipated Minors

Generally, an **emancipated minor** is a person of minority age (as defined by the laws of a particular state) who has the legal authority to act on his or her own behalf in all matters.

An **unemancipated minor** is a minor who is subject to the authority of a parent or guardian. The specific definitions of "emancipated" and "unemancipated" minor in our state are described in Form F1.15A, section E (State Laws Governing Personal Representatives).

Part A: Adults and Emancipated Minors

Personal Representatives of Adults and Emancipated Minors

Use the following procedure to determine whether the Practice may treat a person as the Personal Representative of an adult or emancipated minor. You may also refer to Flow Chart F1.15B for further explanation of this procedure.

Step 1

Verify the identity of the person seeking to be treated as the Personal Representative of the patient. Follow the procedures in Verification (PP1.12) as necessary for determining the identity and authority of a person requesting to be treated as a Personal Representative.

2

Confirm that the person has the authority to act on behalf of the unemancipated minor **in making decisions related to health care** by referencing Form F1.15A, section B (State Laws Governing Personal Representatives).

3

Determine if the abuse, neglect and endangerment exception applies. The Practice **may elect not** to treat a person as a Personal Representative if the Practice has a reasonable belief that:

- The individual has been or may be subjected to domestic violence, abuse, or neglect by such person or treating such person as the Personal Representative could endanger the individual; and
- The Practice, in the exercise of professional judgment, decides that it is not in the best interests of the individual to treat the person as the individual's Personal Representative.

4

Use the following table to determine the next step:

If . . .	then . . .
the person **does not qualify** as a Personal resentative under state law or if the Practice has decided that it will not treat the person as the Personal Representative under the exception for abuse, neglect and endangerment	**do not** treat the person as the Personal Representative of the patient.
the person qualifies as the Personal Representative under state law and the exception for abuse, neglect and endangerment does not apply	treat the individual as the Personal Representative but only with respect to PHI that relates to the scope of that particular representation.

Note

In some cases, it may be appropriate to disclose to the individual under the permission for individuals involved in a patient's care covered in Family, Friends and Disaster Relief Organizations (PP1.6).

Part B: Deceased Individuals

Personal Representatives of Deceased Individuals

Use the following procedure to determine whether the Practice may treat a person as the Personal Representative of a deceased individual. You may also refer to Flow Chart F1.15C for further explanation of this procedure.

Step

1

Verify the identity of the person seeking to be treated as the Personal Representative of the patient. Follow the procedures in Verification (PP1.12) as necessary for determining the identity and authority of a person requesting to be treated as a Personal Representative.

2

Confirm that the person has the authority to act on behalf of the deceased individual or the deceased individual's estate by referencing Form F1.15A, section B (State Laws Governing Personal Representatives).

3

Use the following table to determine the next step:

If . . .	then . . .
the person does not qualify as a Personal Representative under state law	do not treat the person as the Personal Representative of the patient.
the person qualifies as the Personal Representative under state law	treat the individual as the Personal Representative but only with respect to PHI that relates to the scope of that particular representation.

Note

In some cases, it may be appropriate to disclose to the individual under the permission for individuals involved in a patient's care covered in Family, Friends and Disaster Relief Organizations (PP1.6).

Part C: Unemancipated Minors

Overview—Personal Representatives of Unemancipated Minors

The process for determining the Personal Representative status for unemancipated minors is more involved than for adults, emancipated minors, and deceased individuals. Described below is an overview of the steps involved in determining whether the Practice may treat a person as the Personal Representative of an unemancipated minor under the HIPAA Privacy Rule.

Step 1

Determine the Personal Representative status of the person seeking to be treated as a Personal Representative.

2

Determine whether certain HIPAA exceptions apply for personal representation of unemancipated minors.

3

Determine whether state law prohibits disclosure to or provision of access to a parent, guardian, or person acting in the place of a parent.

4

Determine if state law governing parental access and disclosures is applicable under Part D.

Each of these steps is covered in more detail below. Also, refer to Flow Chart F1.15D for further explanation of this procedure.

Step 1: Determine HIPAA Personal Representative Status

Use the following procedure to determine whether the Practice must treat a person as the Personal Representative of an unemancipated minor.

Step 1A

Verify the identity of the person seeking to be treated as the Personal Representative of the patient. Follow the procedures in Verification (PP1.12) as necessary for determining the identity and authority of a person requesting to be treated as a Personal Representative.

1B

Confirm that the person has the authority to act on behalf of the unemancipated minor in making decisions related to health care by referencing Form F1.15A, section C (State Laws Governing Personal Representatives).

1C

Determine if the abuse, neglect and endangerment exception applies. The Practice **may elect not** to treat a person as a Personal Representative if the Practice has a reasonable belief that:

- The individual has been or may be subjected to domestic violence, abuse, or neglect by such person or treating such person as the Personal Representative could endanger the individual; and
- The Practice, in the exercise of professional judgment, decides that it is not in the best interests of the individual to treat the person as the individual's Personal Representative.

Step 2: Determine Whether HIPAA Exceptions Apply for Unemancipated Minors

There are circumstances under the Privacy Rule and state law where a person may not be a Personal Representative of an unemancipated minor, and the minor has the authority to act as the individual with respect to PHI pertaining to a health care service. Use the procedure below to determine if these circumstances apply.

Determine if *any* of the following three circumstances exist:

- The minor consents to such health care service; no other consent to such service is required by law, regardless of whether the consent of another person has also been obtained; and the minor has not requested that such person be treated as a Personal Representative.
- The minor may lawfully obtain such health care service without the consent of a parent, guardian, or other person acting in the place of a parent; and the minor, a court, or another person authorized by law consents to such health care service.
- A parent, guardian, or other person acting in the place of a parent assents to an agreement of confidentiality between a health care provider that is a Covered Entity and the minor with respect to such health care service.

If any of the above circumstances exist, then the individual representative may not be a Personal Representative of an unemancipated minor.

Step 3: Does State Law Prohibit Disclosure or Access?

Even where a parent, guardian, or person acting in the place of a parent qualifies as a Personal Representative under the above rules, the Practice may not disclose to or provide access to a parent, guardian, or person acting in the place of a parent where it is expressly **prohibited** by state law.

Determine whether state law prohibits access or disclosure by referencing Form F1.15A, section D (State Laws Governing Personal Representatives).

Step 4: Determine If Parental Access May or Must Be Given Under State Law

If a parent, guardian, or person acting in the place of a parent does not qualify as a Personal Representative under Steps 1 through 3 above, proceed to Part D to determine if the Practice might still be permitted or required to disclose or provide access to such persons under state law.

Part D: Parental Access and Disclosure Under State Law

Parental Access Under State Law

Even where a parent, guardian, or person acting in the place of a parent does not qualify as a Personal Representative under Part C, the Practice may still be permitted or required to disclose or provide access to PHI under state law to such person. Follow the steps below to determine if state law would permit or require disclosure or the provision of access. You may also refer to Flow Charts F1.15E and F1.15F for further explanation of this procedure.

Step 1: Parental Access Under *Express* State Law

Use the following procedure to determine whether state law expressly permits or requires the Practice to disclose or provide access to a parent, guardian, or person acting in the place of a parent.

Step 1A

Verify the identity of the parent, guardian, or person acting in place of the parent. Follow the procedures in Verification (PP1.12) as necessary for determining the identity and authority of the person.

1B

Determine if the abuse, neglect, and endangerment exception applies. The Practice **may elect not** to disclose to or provide access to a parent, guardian, or person acting in the place of a parent if the Practice has a reasonable belief that:

- The individual has been or may be subjected to domestic violence, abuse, or neglect by such person or treating such person as the Personal Representative could endanger the individual; and

- The Practice, in the exercise of professional judgment, decides that it is not in the best interests of the individual to treat the person as the individual's Personal Representative.

1C

Consult Form F1.15A, section D (State Laws Governing Personal Representatives) to determine whether state law expressly permits or requires disclosure or access.

If state law expressly **permits** the Practice to disclose to or provide access to a parent, guardian, or person acting in the place of a parent, the Practice **may** do so.

If state law expressly **requires** the Practice to disclose to or provide access to a parent, guardian, or person acting in the place of a parent, the Practice **must** do so.

Note

Even if state law controls the right of access to the PHI related to an unemancipated minor, the requirements regarding how access is provided under the Privacy Rule still must be followed. Refer to the policy and procedure for Access (PP2.1).

Step 2: Parental Access Where State Law is Silent

Even when state law **does not expressly** provide for access, the Practice may still provide access to a parent, guardian, or person acting in the place of a parent if the following criteria are met:

- there are no specifically applicable access provisions under state law;
- giving access would be **consistent** with state law; **and**
- the decision to provide access is made by a licensed health care professional in the exercise of professional judgment.

Note

The Practice may need to consult legal counsel to determine if the above three conditions are met in a particular case.

F1.15A

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

State Laws Governing Personal Representatives

A. Adults/Emancipated Minors: Described below are the laws in the State of _____ that govern when a person has the authority to act on behalf of an adult or emancipated minor in making decisions related to health care:

B. Deceased Individuals: Described below are the laws in the State of _____ that govern when an executor, administrator, or other person has the authority to act on behalf of a deceased individual or the individual's estate:

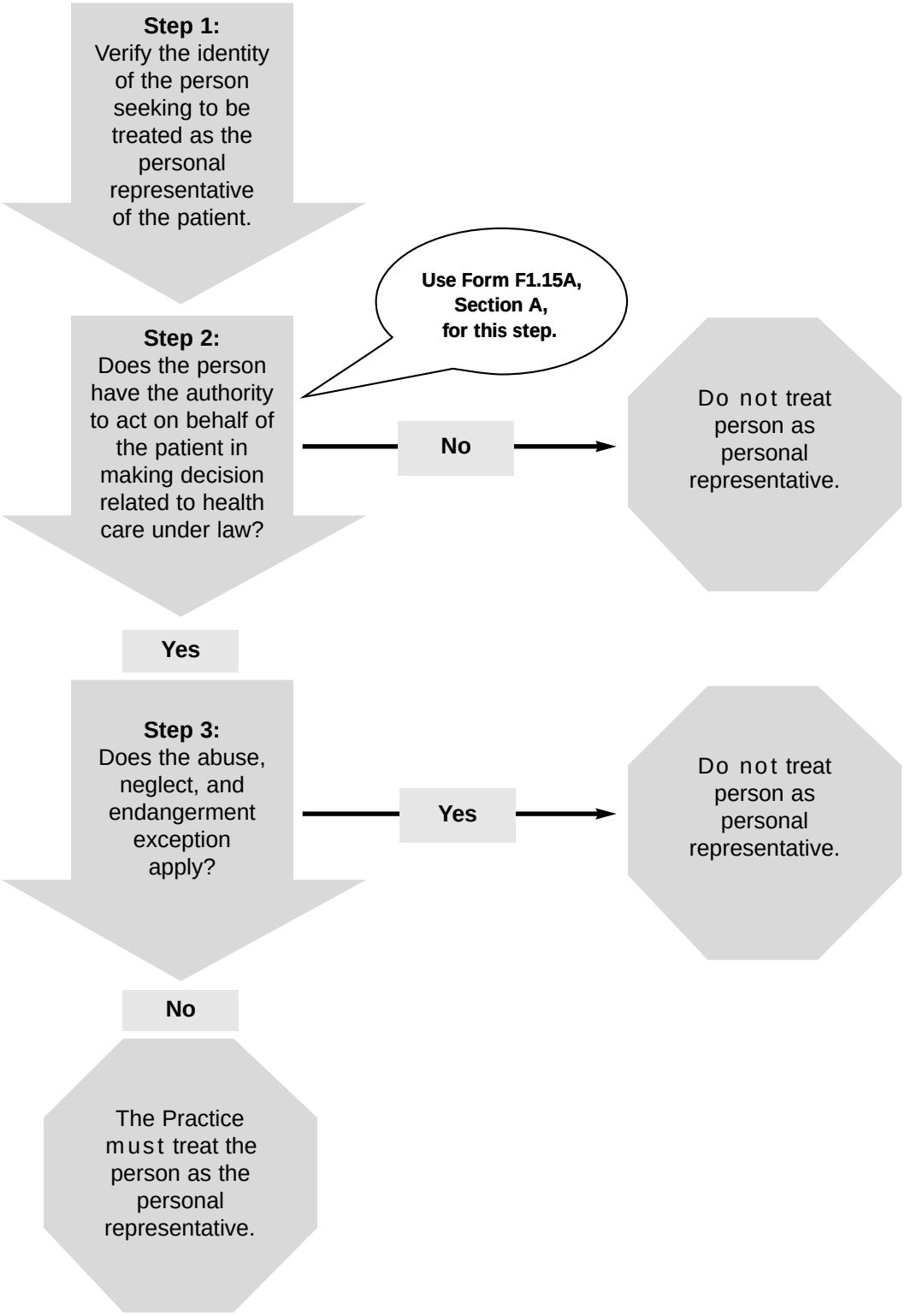
C. Unemancipated Minors: Described below are the laws in the State of _____ that govern when a parent, guardian, or a person acting in the place of a parent has the authority to act on behalf of an unemancipated minor in making decisions related to health care:

D. Parental Access Under State Law: Described below are the laws in the State of _____ that govern when the Practice may or may not disclose or provide access to PHI about an unemancipated minor to a parent, guardian, or person acting in the place of a parent:

E. "Emancipated" and "Unemancipated": Described below are the definitions of "Emancipated" and "Unemancipated" Minor under the laws in the State of _____ :

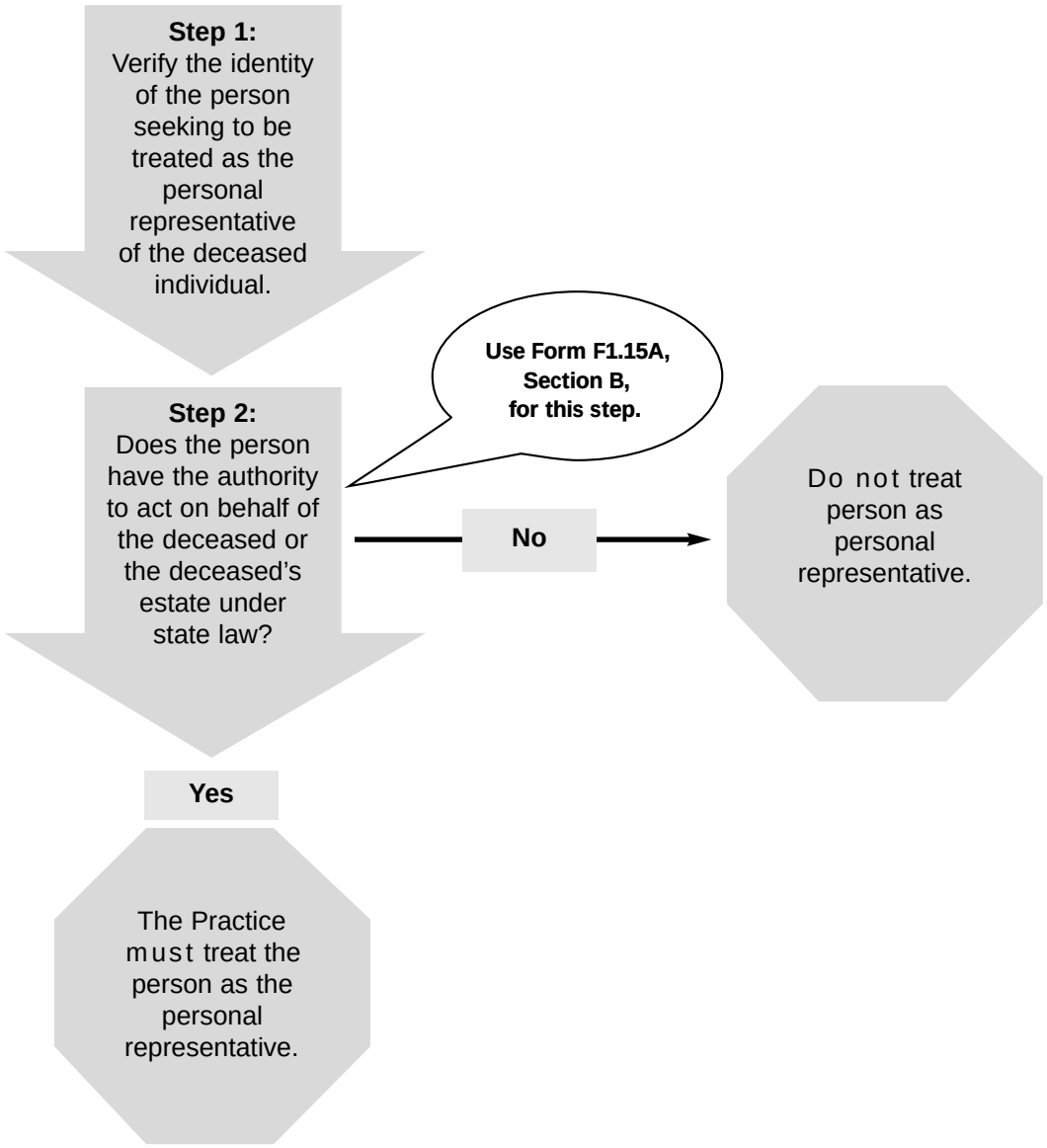
F1.15B

Process for Determining Personal Representative Status with Respect to Adults and Emancipated Minors



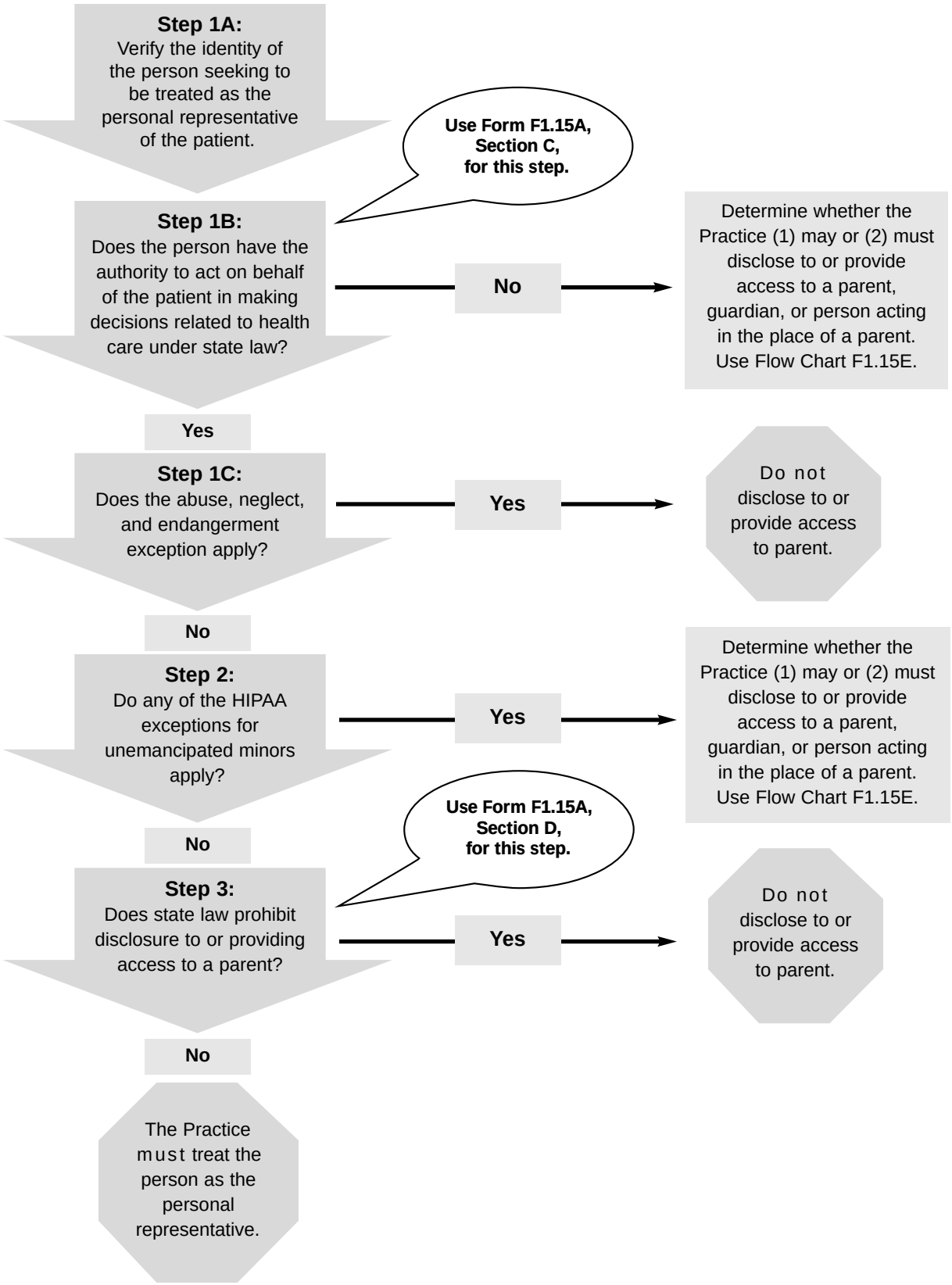
F1.15C

Process for Determining Personal Representative Status with Respect to Deceased Individuals



F1.15D

Process for Determining Personal Representative Status with Respect to Unemancipated Minors

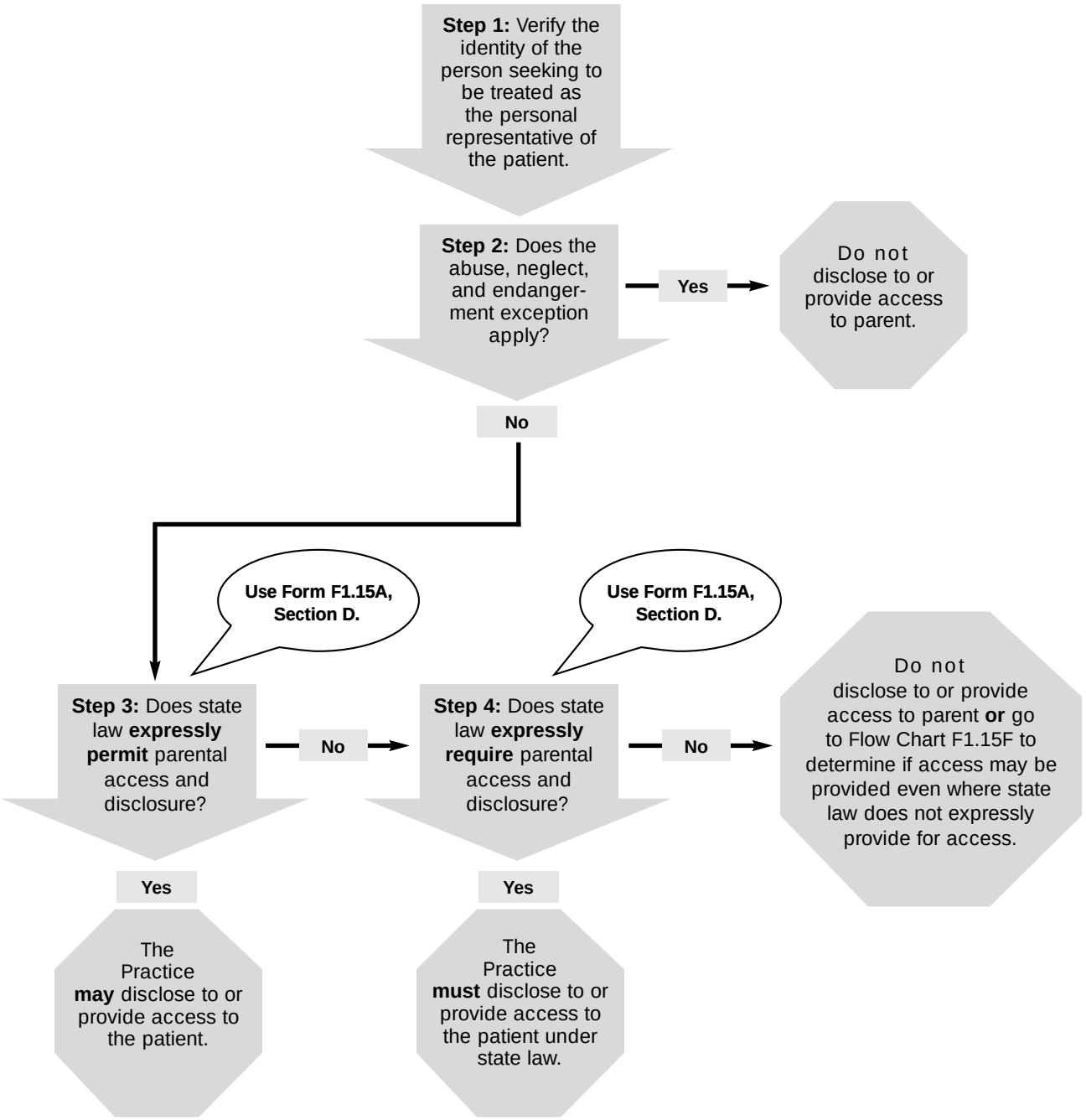


F1.15E

Process for Determining Whether Practice May or Must Disclose to a Parent* or Provide Access to a Parent Under Express State Law

Note

It is only necessary to use this Flow Chart where the parent, guardian, or person acting in the place of a parent **does not** otherwise qualify as a personal representative of the unemancipated minor under HIPAA (see Flow Chart F1.15D).



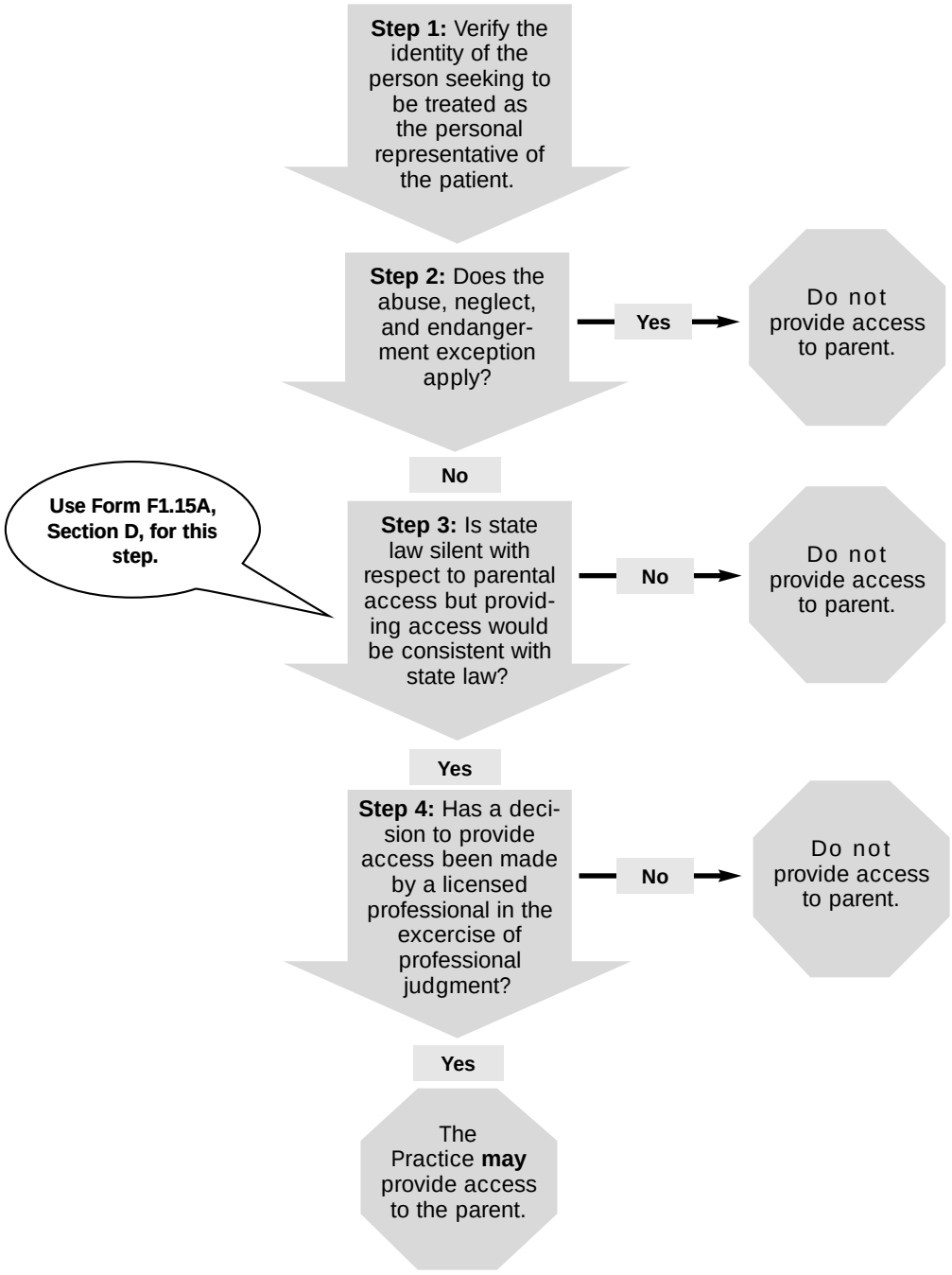
*Note: The term "parent" has been used collectively in this flow chart to refer to a parent, guardian, or a person acting in the place of a parent.

F1.15F

Process for Determining Whether Practice May Disclose to a Parent* or Provide Access to a Parent Where State Law is Silent

Note

It is only necessary to use this Flow Chart where the parent, guardian, or person acting in the place of a parent **does not** otherwise qualify as a personal representative of the unemancipated minor under HIPAA (see Flow Chart F1.15D) and where disclosure is not permitted or required by **express** state law (see Flow Chart F1.15E).



*Note: The term "parent" has been used collectively in this flow chart to refer to a parent, guardian, or a person acting in the place of a parent.

SPECIAL REQUIREMENTS: MARKETING PP1.16

Overview

Introduction

The HIPAA Privacy Rule requires that our Practice obtain an individual's Authorization prior to any use or disclosure of PHI for Marketing purposes, with certain exceptions.

Furthermore, if the Practice expects to receive any type of direct or indirect remuneration (ie, something of value) from a third party as a result of the Marketing, the Authorization must state that such remuneration is expected.

Policies and Procedures

PP1.16 describes our policies and procedures relating to use or disclosure of PHI for Marketing purposes.

Contact Person

Our Privacy Official is designated to be the contact person for questions, suggestions, or complaints relating to use or disclosure of PHI for Marketing purposes and our compliance with the Privacy Rule related to use or disclosure of PHI for Marketing purposes.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

SPECIAL REQUIREMENTS: MARKETING PP1.16

General Policy

Policy

It is the policy of this Practice to obtain a specific Authorization for any disclosure of an individual's PHI for Marketing purposes, except as otherwise permitted by the Privacy Rule. It is also our policy not to disclose PHI to third parties, except as permitted by the Privacy Rule and other federal and state laws and regulations.

Definition

Marketing: The Privacy Rule defines "marketing" as making a communication about a product or service that encourages recipients of the communication to purchase or use the product or service.

The Privacy Rule also defines "marketing" as an arrangement between a Covered Entity and any other entity whereby the Covered Entity discloses PHI to the other entity, in exchange for direct or indirect remuneration, for the other entity or its affiliate to make a communication about its own product or service that encourages recipients of the communication to purchase or use that product or service.

See Glossary for the complete definition.

Procedures

Use PP1.16, Marketing, policies and procedures to govern use or disclosure of PHI for Marketing purposes.

POLICIES AND PROCEDURES FOR MARKETING PP1.16

Index of Procedures

Introduction

With only limited exceptions, our Practice will secure an Authorization before using PHI for Marketing purposes.

Inquiry/Action Steps

Follow these steps for determining whether a Marketing Authorization is required before PHI can be used or disclosed:

Step	Inquiry/Action
1	Determine whether the disclosure is Marketing
2	Determine whether an exception applies

Step 1: Determine Whether the Disclosure Is Marketing

Introduction

This procedure should be followed to determine whether the use or disclosure of PHI is for Marketing purposes. Even if a communication is not Marketing, a Permission in PP1.1 through PP1.11 must be available before PHI can be used or disclosed without an Authorization.

Is There a Marketing Communication?

Determine whether there is a Marketing communication. Steps A through C described below walk you through the definition of Marketing to help you determine whether a communication is Marketing.

Step A Is there a communication about a product or service that encourages recipients of the communication to purchase or use the product or service? *For example*, a communication from a health insurer promoting a home and casualty insurance product offered by the company.

If yes, **proceed to Step B**.

If no, **proceed to Step C**.

Step B Is the communication in Step A made to an individual for one or more of the following purposes?

- To describe (a) health-related products or services, or (b) payments for health-related products or services, that are provided by or included in a benefits plan of the Practice. Descriptions that would fall into this category include those designed to:
  - ☐ describe the entities participating in a health care provider or health plan network;
  - ☐ describe a product or service that is provided by the Practice or included in a plan of benefits;
  - ☐ describe replacement of, or enhancements to, a health plan; and
  - ☐ describe health-related products or services available only to a health plan enrollee that add value to, but are not part of, a plan of benefits.
- For treatment of that individual;
- For case management or care coordination for that individual; or
- To direct or recommend alternative treatments, therapies, health care providers, or settings of care to that individual.

If yes, the communication is not Marketing and no Marketing Authorization is required unless the arrangement described in Step C is present.

If no, the communication is Marketing. Proceed to Step 2 with respect to the Marketing communication.

Whether the answer is yes or no under the first definition of Marketing after Steps A and B, you will want to review the second definition of Marketing to determine whether it applies. **Proceed to Step C**.

Step C Is there an arrangement between our Practice and any other entity that:

- includes disclosure of PHI from the Practice to the other entity, in exchange for direct or indirect remuneration; and
- enables the other entity to make a communication about its own product or service that encourages recipients of the communication to purchase or use the product or service?

  For example, a drug manufacturer receives a list of patients from a Covered Entity and provides remuneration, then uses that list to send discount coupons for a new anti-depressant medication directly to the patients. This is a Marketing disclosure by the Covered Entity under the second definition of Marketing.

If yes, **proceed to Step 2.**

If no, there is no Marketing under the second definition and no Marketing Authorization is required, unless you determined in Steps A and B that the first definition of Marketing applies.

Remember: Even if a communication is not Marketing, there still must be an applicable permission under the Privacy Rule before the use or disclosure may be made without an Authorization.

Proceed to review other Permission Procedures, PP1.1 through PP1.11, to determine whether the PHI can be used or disclosed as intended.

Step 2: Determine Whether an Exception Applies

Introduction

Even if a communication is Marketing under the Privacy Rule definition, there are certain types of Marketing that do not require a Marketing Authorization. This procedure explains when these exceptions apply.

Step 2.1

Does an Exception Apply?

Is the use or disclosure for Marketing:

- a face-to-face communication made by the Practice to an individual, or
- a promotional gift of nominal value provided by the Practice?

Note

Our Practice may discuss any services and products without restriction during a face-to-face communication.

Examples of promotional gifts of nominal value are calendars, pens, and other merchandise that generally promotes the Practice.

Step 2.2

If an Exception Applies

If either exception in Step 2.1 applies, no Authorization is needed with respect to the Marketing communication.

Step 2.3

If No Exception Applies

If no exception applies, an Authorization must be obtained from the patient for the intended Marketing use or disclosure of the PHI.

Proceed to Authorization, PP1.9, for policies and procedures with respect to obtaining an Authorization.

Remember: If the Marketing communication will involve direct or indirect remuneration to our Practice from a third party, the Authorization must state that such remuneration is involved.

SPECIAL REQUIREMENTS: PSYCHOTHERAPY NOTES PP1.17

Overview

Introduction

HIPAA generally prohibits Covered Entities from using or disclosing Psychotherapy Notes without an Authorization. However, there are a number of exceptions. The Psychotherapy Notes Authorization requirement does not apply to:

- uses by the originator of the Psychotherapy Notes for treatment purposes;
- uses or disclosures by our Practice for our own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;
- uses or disclosures by our Practice to defend ourselves in legal actions or other proceedings brought by the individual;
- disclosures to the individual as required by HIPAA;
- disclosures to the Secretary of HHS as required by HIPAA;
- uses or disclosures that are required by law;
- disclosures to health oversight agencies with respect to oversight of the originator of the Psychotherapy Notes;
- uses and disclosures that are by or to a coroner or medical examiner for certain purposes; and
- uses and disclosures that are necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public *and* to a person reasonably able to prevent or lessen the threat.

All other uses and disclosures of Psychotherapy Notes require proper Authorization.

Policies and Procedures

PP1.17 describes our policies and procedures relating to use or disclosure of Psychotherapy Notes.

Contact Person

Our Privacy Official is designated to be the contact person for issues relating to use or disclosure of Psychotherapy Notes.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

SPECIAL REQUIREMENTS: PSYCHOTHERAPY NOTES PP1.17

General Policy

General Policy

Our Practice's policy is that we will not use or disclose Psychotherapy Notes without an Authorization signed by the individual or a personal representative of the individual, except as specifically permitted by law.

Definition

Psychotherapy Notes. Psychotherapy Notes means notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and *that are separated from the rest of the individual's medical record.*

Psychotherapy Notes *do not* include the following:

- medication prescription and monitoring,
- counseling session start and stop times,
- the modalities and frequencies of treatment furnished,
- results of clinical tests, and
- any summary of the following items:
  - diagnosis,
  - functional status,
  - the treatment plan,
  - symptoms,
  - prognosis, and
  - progress to date.

Procedure

Use Psychotherapy Notes, PP1.17, to evaluate whether a use or disclosure of Psychotherapy Notes is permitted.

USE OR DISCLOSURE OF PSYCHOTHERAPY NOTES PP1.17

Index of Procedures

Introduction — Determining whether, and under what conditions, Psychotherapy Notes may be used or disclosed is a multi-step process.

Inquiry/Action Steps — Follow these steps with respect to a possible use or disclosure of Psychotherapy Notes:

Step	Inquiry/Action
1	Determine whether PHI includes Psychotherapy Notes
2	Determine whether the Psychotherapy Notes can be used or disclosed without an Authorization

Step 1: Determine Whether PHI Includes Psychotherapy Notes

Introduction — This procedure should be followed by any Practice employee to determine if the PHI in question includes Psychotherapy Notes.

Step 1.1

Determine Whether Materials Include Psychotherapy Notes

PHI is subject to more stringent protections for Psychotherapy Notes only if it meets all of the following four parts of the definition of Psychotherapy Notes:

- recorded notes (any medium),
- by a health care provider who is a mental health professional,
- analyzing a conversation during a counseling session, and
- the notes are separated from the rest of the patient's medical record.

Even if PHI otherwise meets the above elements, the following PHI is not considered to be Psychotherapy Notes:

- medication prescription and monitoring,
- counseling session start and stop times,
- the modalities and frequencies of treatment furnished,
- results of clinical tests, and
- any summary of the following items:
  - diagnosis,
  - functional status,
  - the treatment plan,
  - symptoms,
  - prognosis, and
  - progress to date.

Step 1.2

If Yes

If Psychotherapy Notes are involved, **proceed to Step 2.**

Step 1.3

If No

If no Psychotherapy Notes are involved, this procedure does not apply. Review Permission Procedures, PP1.1 through PP1.11, to determine whether a use or disclosure of PHI is permitted or required and complies with any other Special Requirements, PP1.12 through PP1.20.

Step 2: Determine Whether Psychotherapy Notes Can Be Used or Disclosed Without an Authorization

Introduction

HIPAA generally prohibits the use or disclosure by Covered Entities of Psychotherapy Notes without an Authorization. However, there are nine exceptions to this general rule. This procedure should be used to determine if the proposed use or disclosure falls under one of the exceptions.

Step 2.1

Does the Use or Disclosure Fit Into an Exception to the Authorization Requirement?

Determine whether the use or disclosure fit into one of the following categories:

- uses by the originator of the Psychotherapy Notes for treatment purposes;
- uses or disclosures by our Practice for its own training programs in which students, trainees, or practitioners in mental health learn under supervision to practice or improve their skills in group, joint, family, or individual counseling;
- uses or disclosures by our Practice to defend ourselves in legal actions or other proceedings brought by the individual;
- disclosures to the individual as required by HIPAA (see Required Disclosures, PP1.1);
- disclosures to the Secretary of HHS as required by HIPAA (see Required Disclosures, PP1.1);
- uses or disclosures that are required by law (see Public Purpose, PP1.8, Public Purpose A);
- disclosures to health oversight agencies with respect to oversight of the originator of the Psychotherapy Notes (see Public Purpose, PP1.8, Public Purpose D);
- uses or disclosures that are by or to a coroner or medical examiner for the purpose of identifying a deceased person, determining a cause of death, or other duties as authorized by law (see Public Purpose, PP1.8, Public Purpose G); and
- uses or disclosures that are necessary to prevent or lessen a serious and imminent threat to the health or safety of a person or the public, *and* to a person reasonably able to prevent or lessen the threat (see Public Purpose, PP1.8, Public Purpose J).

Step 2.2

If an Exception Applies

If an exception applies, our Practice may use or disclose the PHI with Psychotherapy Notes without an Authorization if the use or disclosure is otherwise permitted.

Step 2.3

If No Exception Applies, Acquire an Authorization

When using or disclosing Psychotherapy Notes not subject to an exception under Step 2.2, require an Authorization to use or disclose the Psychotherapy Notes. **Proceed to Authorization, PP1.9.**

SPECIAL REQUIREMENTS: CONSISTENT WITH NOTICE OF PRIVACY PRACTICES PP 1.18

Policy

It is our Practice's policy that we will not use or disclose PHI in a manner inconsistent with our Practice's Notice of Privacy Practices (NPP).

Our NPP policies are described in more detail in PP3.3. If you have any question about the NPP or whether a use or disclosure is consistent with the NPP, contact the Privacy Official.

Our Practice will not engage in any of the following activities unless the Practice's NPP includes a separate statement notifying the patient that:

- the Practice may contact the patient to provide appointment reminders or information about treatment alternatives or other health-related benefits and services that may be of interest to the patient; *or*
- the Practice may contact the patient to raise funds for the Practice.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

SPECIAL REQUIREMENTS: CONSISTENT WITH OTHER DOCUMENTS PP 1.19

Policy	It is our Practice's policy that we will use and disclose PHI consistent with any limitations placed on the use or disclosure of such PHI by other documents or agreements entered into by the Practice.
Scope of Policy	This policy applies to any documents or agreements limiting our Practice's use or disclosure of PHI about a patient. Five examples of such documents or agreements are described briefly below in this Policy.
Authorization Limitations	Our Practice will limit its use and disclosure of PHI consistent with the limitations on uses or disclosures of such PHI that may be contained in a patient Authorization. Refer to the Authorization Policies and Procedures (PP 1.9).
Agreement to Further Restrict Use or Disclosure of PHI	Our Practice generally does not agree to requests to further restrict the use or disclosure beyond what the Privacy Rule requires (PP 2.5), If, however, our Practice does agree to such a Further Restriction Request, our Practice will comply with the Agreed Restriction except in the circumstances listed in the Further Restrictions Policies and Procedures (PP 2.5).
Agreement to Provide Alternative Communications	If our Practice agrees to a patient's request to receive communications of PHI by alternative means or at an alternative location, our Practice will comply with this agreement. Refer to the Alternative Communications Policies and Procedures (PP 2.4).
Future Disclosures of PHI Following the Grant or Denial of an Amendment Request	If our Practice denies a Request to Amend Records, our Practice may be required to include documents related to the request and its denial in any future disclosure of the PHI that is the subject of the Request to Amend. The documents our Practice may be required to include in such future disclosures of PHI are specified in the Amendment Policies and Procedures (PP 2.2). If our Practice agrees to a Request to Amend Records, our Practice must include the amendment in future disclosures of records containing PHI affected by the amendment.
Other Contracts	Our policy is to comply with any limitations on the use or disclosure of PHI contained in any other contracts entered into by the Practice, except as otherwise required by law or directed by the board or other governing body of our Practice.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

SPECIAL REQUIREMENTS: CONSENT (STATE OR OTHER LAW) PP1.20

Introduction

There are circumstances in which state or other federal laws will require some form of consent or notice for certain uses or disclosures of PHI even where HIPAA does not require an authorization. Also, other laws may provide a greater right of access to PHI. This policy and procedure describes circumstances applicable to our operations where such consent, notice, or access is required.

Consent Required by State Law

In our state, a consent or notice is required in the circumstances described in Form F1.20A, State Law Consent Requirements. The circumstances in which our state laws provide a greater right of access to PHI are also described in Form F1.20A. The Privacy Official will oversee the completion and updating of this form.

Consent Required by Federal Law

Federal law requires a consent or notice in the circumstances described in Form F1.20B, Federal Law Consent Requirements. The Privacy Official will oversee the completion and updating of this form.

Consent Form(s)

Our Privacy Official will consult with legal counsel and develop consent language as required or advisable to address applicable state law and other legal requirements. This language will be included in Practice form(s) as the Privacy Official directs.

Our Privacy Official will consult with legal counsel regarding the advisability of including consent language with respect to all uses and disclosures of PHI for treatment, payment, and health care operations, with cross-references to our Practice's Notice of Privacy Practices.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

F1.20A

Practice Name: _____

Last Updated: _____

State Law Consent Requirements

Described below are the circumstances in which the laws in the State of _____ require a consent or notice for the use or disclosure of confidential medical information and provide a greater right of access to confidential medical information.

I. Consent/Notice Requirements

A. General Consent/Notice Requirements:

_____

_____

_____

B. Communicable Diseases:

_____

_____

_____

C. Mental Health:

_____

_____

_____

D. Substance Abuse:

_____

_____

_____

G. Genetic:

_____

_____

_____

F. Other:

_____

_____

_____

II. Access Requirements

Described below are the state laws that provide greater rights of access:

_____

_____

_____

F1.20B

Practice Name: _____

Last Updated: _____

Federal Law Consent Requirements

Described below are the circumstances in which federal laws (other than HIPAA) require a consent or notice for the use or disclosure of confidential medical information:

PATIENT RIGHTS PP2.0

Introduction

This policy provides an overview of our Practice's policies and procedures regarding the new federal patient rights granted by the HIPAA Privacy Rule.

General Policy

Our policy is to comply with the HIPAA Privacy Rule's new patient rights requirements. These include the right to:

- request Access to and obtain copies of PHI;
- request Amendments to PHI;
- request Accountings of Disclosures of PHI;
- request Alternative Communications of PHI;
- request Further Restrictions of PHI; and
- make a Complaint to the Practice or to HHS.

If you have questions regarding these patient rights, contact the Privacy Official.

Verification

The patient rights described in this policy involve a request, or a complaint, made by or on behalf of a patient to our Practice. In responding to such requests or complaints, our Practice must follow certain additional procedures to verify the identity and authority of the person communicating with our Practice (PP 1.12).

Patient Rights Policies and Procedures

The following is a list of our policies and procedures for the federal patient rights granted by the HIPAA Privacy Rule:

Patient Rights	**Section**
General Policy	PP2.0
Access	PP2.1
Amendment	PP2.2
Accounting	PP2.3
Alternative Communications	PP2.4
Further Restrictions	PP2.5
Complaints	PP2.6

Privacy Official Discretion

Where consistent with the HIPAA Privacy Rule, other applicable legal requirements, and professional judgment, our Privacy Official may exercise discretion in applying these policies and procedures. Subject to these requirements, flexibility and approach as to particular circumstances may be warranted to serve the needs of our patients.

Documentation

Our Practice's handling of patient rights requests and complaints must be documented consistent with the HIPAA Privacy Rule's special documentation requirements, which are described in PP 3.4.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PATIENT RIGHTS: ACCESS PP2.1

Overview

Introduction

A patient has the right to request access to and obtain copies of PHI about the patient that are maintained by or for the practice in records that are called "Designated Record Sets." These requests are called "Access Requests."

PP2.1 contains our Practice's policies and procedures for (A) documenting Designated Record Sets, and (B) processing patient Access Requests.

Designated Record Sets Policies and Procedures

Part A of PP2.1 describes our Practice's policies and procedures for documenting Designated Record Sets about our patients that are subject to patients' Access Requests.

Access Requests Policies and Procedures

Part B of PP2.1 describes our policies and procedures for processing patient Access Requests.

Contact Person

Our Privacy Official is the contact person for receiving and processing Access Requests. The Privacy Official is also the contact person for handling questions, suggestions, or complaints about our Practice's affairs relating to Access Requests or our compliance with the privacy rule related to Access Requests.

Part A: Designated Record Sets Policies and Procedures

Policy

It is our Practice's policy to comply with the HIPAA Privacy Rule requirements for documenting Designated Record Sets. Our policy is to document all Designated Record Sets that are subject to a patient's HIPAA rights to inspect and copy records.

What Is a Designated Record Set?

Designated Record Sets are records maintained by or for our Practice that may include medical records, billing records, and other records used (in whole or in part) to make decisions regarding the patient.

> **Note**
>
> Designated Record Sets can include records maintained, collected, or used by a Business Associate or other person on behalf of our practice.

Maintain Designated Record Set Log

Use the Designated Record Set Log (F2.1A) to document the Designated Record Sets maintained by or for the Practice. The Designated Record Set Log (F2.1A) describes the general types and locations of Designated Record Sets we (and our Business Associates) maintain. The Designated Record Set Log (F2.1A) also describes specific Designated Record Sets that we maintain for particular patients.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

It is also permissible to designate in a patient chart or billing record that a particular Designated Record Set is maintained in another specific location. This documentation shall be made by the employee(s) involved with or responsible for Designated Record Sets maintained in the other record locations.

The Privacy Official will maintain and regularly update the Designated Record Set Log (F2.1A) as necessary to keep our documentation of Designated Record Sets reasonably current.

Require Business Associates to Document Designated Record Sets

The Privacy Official shall inform Business Associates of the requirement that they must document all Designated Record Sets maintained, collected, or used by such Business Associates on behalf of the Practice that are subject to the patient's right of access. This requirement shall also be stated in the Practice's contracts with Business Associates.

Documentation

The Practice shall maintain the Designated Record Set Log (F2.1A) consistent with the requirements of PP3.4.

Part B: Access—General Policy

Policy

Our Practice's policy is to comply with the Privacy Rule regarding a patient's request to have access to and obtain copies of PHI about the patient maintained by or for the Practice in a Designated Record Set. This request is called an "Access Request" in these policies and procedures.

Our policy is also to comply with other applicable laws relating to patient access to records.

Scope of Policy

This policy applies to all requests by patients for access to and copies of PHI about them maintained in a Designated Record Set.

What Is a Designated Record Set?

Designated Record Sets are billing records, medical records, and other records used to make decisions regarding the patient.

> **Note**
>
> Designated Record Sets can include records maintained, collected, or used by a Business Associate on behalf of our Practice.

Exceptions to Right of Access

Except as may be stated in Form F1.20A, Section II, "Access Requirements," it is our policy that a patient does not have a right of access to:

- Psychotherapy Notes (PP1.17);
- PHI compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding; and
- any laboratory reports or other related information to which a patient does not have a right of access under the Clinical Laboratory Improvement Amendments or applicable state law (eg, if applicable where we are providing laboratory services for other providers).

Other Grounds for Denying Access Requests

The Privacy Rule allows our Practice to deny a patient's Access Request under certain other circumstances. The grounds for such a denial are described in Step 3 of PP2.1. In some circumstances, a patient may be entitled to request a review of our Practice's denial of an Access Request.

Access Request Procedures

When a patient makes an Access Request, follow the steps described in the following Index of Procedures.

Every employee should read Step 1, Respond to the Access Request. This is because every employee needs to be able to recognize when an Access Request is being made to the Practice. In general, an employee should refer Access Requests to the Privacy Official or the person designated by the Privacy Official.

PATIENT RIGHTS: ACCESS PP2.1

Index of Procedures

Introduction

Responding to an Access Request involves a multi-step process. Every employee should be able to perform Step 1, Respond to the Access Request, if the request is made to the employee.

The Privacy Official is responsible for handling Steps 2 through 7. As with other procedures, the Privacy Official may designate properly trained persons to assist with these functions.

Steps for Responding to an Access Request

Follow these steps to respond to an Access Request:

Step	Action
1	Respond to the Access Request.
2	Privacy Official Intake.
3	Review Request.
4	(If Applicable) Grant Request.
5	(If Applicable) Deny Request.
6	(If Applicable) Review Denial.
7	Confirm Documentation.

Step 1: Respond to the Access Request

Introduction

This procedure should be followed by any Practice employee to respond to an Access Request made to the employee. This includes requests made by a patient and requests by a person stating that he or she is acting on behalf of a patient.

Note

Use common sense and professional judgment in determining whether the patient is making a formal access request under the patient's rights granted under the Privacy Rule. In some cases, a request to see information is simply for the purpose of payment or treatment matters. Ask the patient if you are unsure of what the patient intends.

What Is an Access Request?

An Access Request is a request by the patient that our Practice permit the patient to inspect or copy records about the patient. This includes requests made by personal representatives of patients.

Step 1.1

Do Not Disclose PHI Without Verifying Identity and Authority

Caution: Do not disclose any PHI to the person requesting access without first following the Verification Policies and Procedures, PP1.12. This means that you may only disclose PHI if:

1. You know the identity and authority of the person to receive the PHI, or
2. You first follow steps in the Verification procedure.

Note

Keep in mind that in some cases, disclosure of PHI may occur simply by confirming that a person is a patient of our Practice.

What to say (follow these steps):

Step A If the identity and authority of the person requesting the access are known to you, respond to oral and written requests as described in Step 1.2 (oral) or Step 1.3 (written) below.

Step B If the identity or the authority of the person is not known to you, either follow the Verification Procedure, PP1.12, or respond to the request without disclosing any PHI.

For example, you may say: "*You need to present your request to our Practice's Privacy Official. It is our Practice's policy that I cannot discuss whether a person is or is not a patient. I also cannot discuss any request that you make to have access to patient records.*"

Step 1.2

Oral Requests—What To Do

Depending on the circumstances, respond in one of the following two ways to Access Requests that are made orally. Use your best judgment, and follow Privacy Official guidance, as to which response is better under the circumstances.

Option A State that the Practice's policy is that an Access Request must be in writing. Provide the patient with a Request for Access to Records form (F2.1B) and explain that the form should be completed, signed, and provided to the Practice's Privacy Official.

Note

A patient does not have to use the Request for Access to Records form (F2.1B), so long as the patient does make the request in writing.

Option B State that the Privacy Official is the contact person for making Access Requests and explain how to contact the Privacy Official.

Step 1.3

Written Requests—What To Do

If the request is made in writing, forward it promptly to the Privacy Official. Make sure you tell the Privacy Official the date the written request was received.

Step 1.4

Privacy Official Takes Over

The Privacy Official is responsible for the remaining steps in these procedures.

Proceed to Step 2.

Step 2: Privacy Official Intake of Access Request

Introduction

This procedure should be followed by the Privacy Official in order to facilitate the review of and response to an Access Request.

Step 2.1

Follow the Procedures in Step 1

Follow the procedures in Step 1: Respond to the Access Request. **Then proceed to Step 2.2.**

Step 2.2

Document the Request

Step A Record the request in the Access Request Log (F2.1C), including the deadline for our response.

Step B Place the written Access Request in the Patient HIPAA File (Documentation Policies and Procedures (PP3.4) describes the Patient HIPAA File).

Step 2.3

Initiate Review Process

Proceed to Step 3.

Step 3: Review of Access Requests

Introduction

The Privacy Official should use this procedure to review an Access Request and determine the appropriate initial response to an Access Request.

Step 3.1

Review Designated Record Set Logs

Step A Confirm that the request is made about a patient about whom we maintain records.

Step B Review the Practice's Designated Record Set Log (F2.1A). Identify and locate the Designated Record Sets held by the Practice.

Step 3.2

Contact Business Associates

Contact Business Associates of the Practice who may have Designated Record Sets containing PHI that is the subject of the Access Request. Ask them to identify and produce to the Practice any Designated Records Sets that contain PHI subject to the request.

Step 3.3

Determine Whether an Exception Applies

Determine if any of the PHI contained in the Designated Record Sets is subject to an exception to the right of access.

Subject to Form F1.20A, a patient's right of access does not apply to:[1]

1. Psychotherapy Notes; and
2. PHI compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding.

Step 3.4

Determine Whether There are Non-Reviewable Grounds for Denial

Determine whether we may deny an Access Request for other reasons. Even where an exception in Step 3.2 does not apply, there are other grounds for our Practice to deny any Access Request. These grounds are divided into those that trigger a right of review and those that do not trigger a right of review.

The right to request a review needs to be considered as to each type of PHI in Designated Record Sets. An exception may apply to some but not all of the records. We may deny an Access Request, without providing the patient an opportunity to review the denial, in any of the following circumstances:

1. No right. No right exists because there is an exception to the right of access (see Step 3.3).
2. Correctional institution. The PHI is (1) held by a correctional institution or a provider acting under its discretion and (2) disclosure to an inmate would jeopardize safety, health, security, custody, or rehabilitation of the inmate, other inmates, or employees of the correctional institution.
   - This exception only applies to an inmate *obtaining* a copy. The inmate retains the right *to inspect* his or her PHI.
3. Research that includes treatment. The PHI was created or obtained by the Practice in a course of research that includes treatment, in which case, access may be suspended for as long as the research is in progress, if:
   - the patient agreed to a suspension of access by consenting to participate in the research; *and*
   - the Practice has informed the patient that the right of access will be reinstated upon completion of the research.

1. If the Practice provides laboratory services and reports for other health care providers, a patient's right of access also may not apply to certain types of PHI that are subject to or exempt from the Clinical Laboratory Improvement Act of 1988 (CLIA). The CLIA exception generally relates to whether patients have a right under state law to obtain clinical laboratory test records and results directly from the laboratory. CLIA requires clinical laboratories to disclose test results or reports only to "authorized persons," as defined by state law. If a state does not define the term, CLIA defines it to include only the person who orders the test (usually the physician).

4. Federal Privacy Act. The requested PHI (1) is subject to the Federal Privacy Act and (2) is information to which the patient would not be granted access under that Act (applies to government records).
5. Promise of confidentiality. The PHI was (1) obtained by someone other than a health care provider under a promise of confidentiality, and (2) granting access would be reasonably likely to reveal the source of the information.

Note

As with all policies and procedures in this Desk Reference, consider whether stricter state laws may trigger the need to modify these Access Request policies and procedures. State law may require providing access even where a HIPAA exception to access exists. (See Form F1.20A, Section II.) To modify these policies and procedures, use Form F3.3.B, "Policy/Procedure Modification Form."

Step 3.5

Determine Whether There are Reviewable Grounds for Denial

Determine whether we may deny an Access Request for other reasons. We may deny an Access Request in the following circumstances, but we must provide the requesting patient an opportunity to have the denial reviewed:

1. Endangerment. A licensed health care professional determines, in exercising his or her professional judgment, that the Access Requested is reasonably likely to endanger the life or physical safety of the patient or another person.
2. Reference to another person. The PHI (1) makes reference to another person who is not a health care provider, and (2) a licensed health care professional has determined, in exercising his or her professional judgment, that (3) the Access Requested is reasonably likely to cause substantial harm to such other person.

Note

What is "substantial harm"? The Preamble to the Privacy Rule states that a Practice may withhold information when the release of such information is "reasonably likely to cause substantial physical, emotional, or psychological harm."

3. Personal representative. The request is (1) by a patient's Personal Representative, and (2) a licensed health care professional has determined, in exercising his or her professional judgment, that (3) granting access to such Personal Representative is reasonably likely to cause substantial harm to the patient or another person.

Step 3.6

Respond to Request Within Time Limit or Obtain an Extension

Response time. Respond to an Access Request within the required time period.

- On-site Records. If the requested information is maintained on-site or is accessible on-site, the Practice has **30 days** to respond to the request.
- Off-site Records. If the information is maintained off-site, the Practice has **60 days** to respond to the request.

Extension. If the Practice is unable to respond to an Access Request within the allotted time period, it may extend the time to respond to the request by no more than 30 days, provided that:

- the Practice provides the patient with (1) a written statement of the reasons for the delay and (2) the date by which the Practice will provide the accounting.

The Practice is only entitled to one 30-day extension per Access Request.

Step 3.7

Provide What We Can Provide

To the extent possible, provide access to PHI requested by a patient, after excluding information for which there is an exception or other ground to deny access.

Step 3.8

Grant or Deny Request

If *no exceptions or grounds for denial apply* to the requested PHI, **proceed to Step 4.**

If *exceptions or grounds for denial apply to some, but not all,* of the PHI, **proceed to Step 4** and provide the portion of requested PHI that is not subject to an exception or grounds for denial.

If *exceptions or grounds for denial apply to all* requested PHI and the Practice decides to deny the request, **proceed to Step 5.**

Step 4: Grant Access Request (If Applicable)

Introduction

This procedure should be followed by the Privacy Official in granting an Access Request, in whole or in part. This procedure applies after the decision has been made to grant all or part of the request.

Step 4.1

Letters Granting Request (In Whole or In Part)

Step A Complete F2.1D, Response to Request for Access to Records. This form is used to notify the requesting patient that his or her request is granted, in whole or in part.

Step B Record the grant of the Access Request in the Access Request Log (F2.1C).

Step C Place a copy of the completed Response to Request for Access to Records (F2.1D) in the Patient HIPAA File.

Step D Provide the completed Response to Request for Access to Records (F2.1D) to the Patient (usually by mail, but other means may be used).

Step 4.2

Provide PHI in Requested or Alternative Form at Convenient Time and Place

Step A Determine the form of PHI to be provided.

- Provide the patient with access to the PHI in the form or format requested by the patient, if it is readily producible in such form or format.
- If the PHI is not readily producible in the requested form, contact the patient and determine what other forms or formats may be preferable.
- If the parties do not agree on a specific format, the Practice must provide the PHI in a *readable, hard copy* form.
- If the PHI contained in one Designated Record Set merely duplicates the PHI contained in another Designated Record Set held at another location, the Practice is only required to produce the PHI once in response to an Access Request.

Step B Contact the patient to arrange a convenient time and place for the patient to inspect and copy the PHI. The place of inspection shall generally be in an office of the Practice as determined by the Privacy Official. If the patient requests that copies of records be mailed to the patient, **proceed to Step C**.

Step C At the patient's request, mail a copy of the requested PHI to the patient.

Cost of Copies

If a patient requests a copy of the PHI, impose a reasonable cost-based fee.

- This fee should include the cost of copying and postage (if applicable).
- This fee may include a charge for the labor cost of copying the records, but not for retrieving and handling the records.
- The fee should also be consistent with other Practice policies and with applicable state and other laws. (See Form F1.20A, Section II.)

Fees should be collected from the patient prior to or at the time of the Practice's providing the requested copies.

Summary Report

In lieu of providing access to PHI, the Practice may provide the requesting patient with a summary or explanation of the PHI requested, if the patient:

- agrees in advance to such summary or explanation; and
- agrees in advance to the fees imposed, if any, by the Practice for such summary or explanations.

If the patient agrees, the Privacy Official should inform the patient of a reasonable, cost-based fee for preparing an explanation or summary. The Practice will provide the summary report only if the patient agrees to pay that fee or where the Privacy Official in his/her discretion decides to provide the report.

Step 4.3

Proceed to Step 7 to complete the required documentation.

Document Efforts to Provide Access

Step 5: Deny Access Request (If Applicable)

Introduction

This procedure should be followed by the Privacy Official to deny an Access Request. This procedure applies when the decision has been made to deny an Access Request.

Step 5.1

To the extent possible, provide PHI requested by a patient, after excluding information to which there is an exception or other ground to deny access.

Provide What You Can Provide

Step 5.2

If the Practice denies an Access Request, send a timely written denial to the patient.

Notify Patient of Denial

Step A Complete Response to Request for Access to Records (F2.1D). This form is to inform the requesting patient that his or her Request is denied, in whole or in part.

Note

This is the same form used to notify a patient that an Access Request is being granted. You can complete the grant or denial information as applicable to different parts of the Access Request.

Step B Record the denial in the Access Request Log (F2.1C).

Step C Place a completed copy of the Response to Request for Access to Records (F2.1D) in the Patient HIPAA File.

Step D Provide completed Response to Request for Access to Records (F2.1D) to the patient (usually by mail, but other means may be used).

Content of Denial Notice

The written denial must:

(1) be in plain language, and

(2) contain the basis for the denial, and if the basis is a reviewable ground for denial, a statement of the patient's review rights, including how to exercise those rights.

Complete the Response to Request for Access to Records (F2.1D) in its entirety to ensure the Practice meets these requirements.

Be Helpful

If the Practice does not actually maintain the PHI that is requested, but knows where the information is maintained, inform the patient where to direct his or her request for access. You may write this information in the Reason for Denial section of Response to Request for Access to Records (F2.1D).

Step 5.3

Proceed to Step 7.

Document the Denial

Step 5.4

If the patient requests a review of the denial, **proceed to Step 6.**

(If Applicable) Review of Denial

Step 6: Review Access Denial (If Applicable)

Introduction

This procedure should be followed by the Privacy Official to provide a review of the Practice's denial of an Access Request when a review is appropriately requested.

Right of Review

If a denial is based on a reviewable ground for denial, the patient has the right to have the denial reviewed by a licensed health care professional who did not participate in the original decision to deny the requested access.

If the denial is based on an *exception* to the right of access or on another *non-reviewable ground,* the patient should be informed that there is no right of review.

Step 6.1

Designate a Licensed Health Care Professional to Review the Denial

Designate a licensed health care professional who did not take part in the original decision to review the denial. Use the Access Denial Review Log (F2.1E) to document the designated reviewing official for the review.

Such licensed health care professional may be a member or employee of the Practice. He or she may also be someone outside the Practice.

Step 6.2

Refer Review Request

Promptly refer a request for review to the designated reviewing official. Use the Access Denial Review Log (F2.1E) to document when the request for review is referred to the reviewing official.

Step 6.3

Review Determination

The designated reviewing official must determine within a reasonable period of time whether to grant or deny access. Use the Access Denial Review Log (F2.1E) to document the reviewing official's decision.

Step 6.4

Written Notice of Decision

Use the Access Request Review—Decision of Reviewing Official Form (F2.1F) to provide written notification to the patient of the results of the review. Place a copy of this notification letter in the Access Request File.

Use the Access Denial Review Log (F2.1E) to document this patient notification.

Step 6.5

Comply With and Implement Review Decision

Comply with and implement the decision by the designated reviewing official.

- If the review upholds the denial of access, **proceed to Step 7.**
- If the review grants access, **proceed to Step 4.**

Step 7: Confirm Documentation

Introduction

The Privacy Official should ensure that the following documentation is maintained by the Practice. Such documentation should be maintained consistent with the requirements of PP3.4.

Designated Record Sets Subject to Access Requests

The Practice must document all Designated Record Sets that are subject to an Access Request. Use the Designated Record Sets Log (F2.1A).

Document All Communications Required To Be In Writing

Retain copies of all communications required to be in writing. These communications include:

- Request for Access to Records (F2.1B).
- Response to Request for Access to Records (F2.1D).
- Notice to the patient reporting the results of review by the designated reviewing official (Access Request Review—Decision of Reviewing Official, F2.1F).

Maintain Access Request Log

All information requested in the Access Request Log (F2.1C) should be recorded in the log as soon as reasonably practical when the event occurs or the information becomes known.

The Privacy Official shall review this log regularly to monitor compliance with Access Requests policies, procedures, and deadlines.

F2.1A

Name of Practice:

Last Updated:

Designated Record Set Log

General Description of Designated Record Sets Maintained by Practice

Type of Designated Record	Location Where Records Filed/Stored (Including Records Maintained by Business Associate)
Patient Charts	File Room/Physician Offices/Off-Site Storage
Billing and Payment	Practice Management System, Backup Tapes; Billing Company
Physicians' Personal Digital Assistants (PDAs)	
[Etc.]	

Name of Practice:

Last Updated:

Specific Patient Designated Record Sets

Note: Use the log to document designated record sets not otherwise documented in the General Designated Record Set Log or in a patient chart.

Patient Name	Patient Chart/ ID Number	Type of Designated Record Set	Location Where Records Filed/Stored (Including Records Maintained by Business Associates)

F2.1B

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Request for Access to Records

Notice to Patient: You may use this form to request to inspect or copy information maintained about you. This type of request is described in our Practice's Notice of Privacy Practices.

Patient Name: _____
[print or type]

Description of Records Requested:

(Please describe the records or types of records requested. Please also let us know how far back in time you want access to records.)

_____

_____

_____

Scope of Request:

(Please let us know if you want to: 1. inspect records; 2. copy records; or 3. both.)

_____ I would like to *inspect* the requested records.

_____ I would like to obtain a *copy* of the requested records.

_____ I would like to *both inspect and copy* the requested records.

Fee for Copying Requested Records

Our Practice may charge a reasonable fee for the cost of copying your requested records. We may also charge you for postage if you ask us to mail your requested records.

Contact Person

Please contact our Practice's Privacy Official if you have any questions relating to requests to inspect or copy records.

Patient Information and Authorization

Print Name of Patient: _____

Signature of Patient: _____

Date: _____

Date of Birth (for identification purposes):_____

For Personal Representative of the Patient (if applicable)

Print Name of Personal Representative: _____

Describe Personal Representative Relationship: _____ (parent, guardian, power of attorney, etc.)

I hereby certify that I have the legal authority under applicable law to make this request on behalf of the patient identified above.

Signature of Personal Representative: _____Date: _____

F2.1C

Name of Practice:

Last Updated:

Access Request Log

Patient Name	Chart/ID Number	Date of Access Request	Response Deadline	Response to Request G=Grant D=Deny G/D=Both	Date Records Provided	Date Review Requested (if applicable)	Response to Review/Date

F2.1D

Name of Practice:

Address:

Privacy Official:

Telephone:

Response to Request for Access to Records

Patient Name: _____

Address: _____

_____

Chart/ID Number: _____

Access Request Date: _____

Dear Patient:

You have made a request to our Practice to inspect or copy certain records about you. This is our response to your request.

As we explain below, your Access Request is:

☐ Granted

☐ Denied

☐ Granted In Part, Denied In Part

_____ Grant of Your Access Request (In Whole or In Part)

[check if applicable]

Our Practice *grants* your Access Request to the extent specified below.

_____

_____

_____

If your Request is granted, please contact our Privacy Official to arrange a convenient time for you to come to our office to inspect and copy your requested records. You may also request that we mail to you copies of your requested records. Our Practice may charge a reasonable fee for the cost of copying and postage.

_____ Denial of Your Access Request (In Whole or In Part)

[check if applicable]

Our Practice *denies* your Access Request to the *extent* and for the *reason(s)* specified below. We also note below whether you may request a review of this denial.

Records Subject to Denial	Reason for Denial	Denial Subject To Review? (Yes/No)

Review of Denial

If our denial is subject to review, you may request that our Practice have the denial reviewed by a licensed health care professional who did not participate in the original decision to deny your Access Request. To request a review in those cases, please contact our Practice's Privacy Official to request a review of our Practice's denial of your Access Request.

Contact Person

You may contact me if you have any questions relating to your Access Request.

Privacy Official: _____

Signature: _____

Date: _____

Telephone: _____

Address: _____

_____

F2.1E

Name of Practice:

Last Updated:

Access Denial Review Log

Patient Name	Chart/ID Number	Date of Review Request	Name of Reviewing Official	Date Review Request Provided to Reviewing Official	Decision of Reviewing Official/Date G=Grant D=Deny G/D=Both	Date Patient Notified of Review Decision

F2.1F

Practice Name ("Practice"): _____

Access Request Review
Decision of Reviewing Official

[Date]

[Patient Address]

Dear [Patient Name]:

As you know, your Access Request to see health information about you dated _____ was denied, in whole or in part, by [Practice Name] ("Practice"), and you sought a review of this denial. The Practice asked me to review your Request. I am writing to inform you of the outcome of my review. Your Access Request is granted or denied, in whole or in part, as explained below:

_____ Grant of Your Access Request (In Whole or In Part)
[check if applicable]

I disagree with the Practice's denial of your Access Request, and your Request should be granted, to the extent specified below.

_____

_____

_____

You may contact the Practice's Privacy Official to arrange a convenient time for you to come to its office to inspect and copy your requested records. You may also request that the Practice mail to you copies of your requested records. The Practice may charge a reasonable fee for the cost of copying and postage.

_____ Denial of Your Access Request (In Whole of In Part)
[check if applicable]

I agree with the Practice's denial of your Access Request, and your request is not granted.

Request should be denied, to the extent specified below.

_____

_____

_____

Please feel free to contact the Practice's Privacy Official if you have any additional questions regarding your Access Request.

Sincerely,

[Reviewing Official]

cc: [Practice Privacy Official]

PATIENT RIGHTS: AMENDMENT PP2.2

Overview

Introduction

A patient has the right to request that our Practice amend PHI about the patient. This right only applies to PHI contained in a Designated Record Set, and only for as long as the PHI is maintained in the Designated Record Set. Unless certain grounds exist to deny a request, we must make the amendment.

A patient's request that we amend PHI about the patient is called an Amendment Request in these policies and procedures.

Policies and Procedures

PP2.2 describes our policies and procedures relating to Amendment Requests.

Contact Person

Our Privacy Official is the contact person for questions, suggestions, or complaints relating to Amendment Requests or our compliance with the Privacy Rule's requirements for handling Amendment Requests.

Note

In PP3.1, Privacy Official and Contact Person Designation, we designated the person who is our Privacy Official. That policy also contains the description of the Privacy Official's responsibilities.

PATIENT RIGHTS: AMENDMENT PP2.2

General Policy

Policy

Our Practice's policy is to comply with the Privacy Rule (and any applicable state and other laws) regarding a patient's request that our Practice amend PHI about the patient in a Designated Record Set.

Scope of Policy

This policy applies to all requests for amendments of PHI made to our Practice by patients with respect to PHI in Designated Record Sets. This policy applies to Designated Record Sets we maintain and that our Business Associates maintain on our behalf. These requests are called "Amendment Requests" in these policies and procedures.

What Is a Designated Record Set?

Designated Records Sets generally are medical records, billing records, and other records used to make decisions about the patient.

Grounds for Denying an Amendment Request

There are *four* separate grounds that permit our Practice to deny an Amendment Request:

1. We may deny a patient's Amendment Request if we determine that the PHI was not created by our Practice, unless the patient provides to us a reasonable basis to believe that the originator of the PHI is no longer able to act on the requested amendment.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

2. We may deny a patient's Amendment Request if we determine that the PHI is not part of a Designated Record Set.
3. We may deny a patient's Amendment Request if we determine that the PHI is accurate and complete.
4. We may deny a patient's Amendment Request if we determine that the PHI would not be available for inspection under the patient's HIPAA right to inspect and copy PHI (see Step 3 in PP2.1).

Request Procedures

To process Amendment Requests, use the step-by-step process described in the following Index of Procedures.

When a patient makes an Amendment Request, follow the steps described in the following Index of Procedures.

Every employee should read Step 1, Respond to the Amendment Request. Every employee needs to be able to recognize when an Amendment Request is being made to the Practice. In general, an employee should refer Amendment Requests to the Privacy Official or the person designated by the Privacy Official.

PATIENT RIGHTS: AMENDMENT PP2.2

Index of Procedures

Introduction

Responding to an Amendment Request involves a multi-step process.

- If someone makes an Amendment Request to an employee, the employee shall perform Step 1, How to Receive an Amendment Request.
- The Privacy Official shall perform Steps 2 through 6.

Steps For Responding to an Amendment Request

Follow these steps to respond to and process an Amendment Request:

Step	Action
1	Respond to the Amendment Request.
2	Receive the Amendment Request.
3	Review the Amendment Request.
4	Accept the Amendment Request (if applicable).
5	Deny the Amendment Request (if applicable).
6	Confirm Amendment Request Documentation.

Other Procedures

Use these additional procedures as needed:

Action
Process Notice of Amendment made by another Covered Entity.
Provide Amendment Request information in future disclosures.

Step 1: Respond to the Amendment Request

Introduction

This procedure should be followed by any Practice employee to respond to an Amendment Request made to the employee. This applies to requests made by a patient. This also applies to requests made by a person stating that he or she is acting on behalf of a patient.

What is an Amendment Request?

An Amendment Request is a request by the patient that our Practice amend or correct PHI about the patient. This includes requests made by personal representatives of patients.

Step 1.1

Do Not Disclose PHI Without Verifying Identity and Authority

Caution: Do not disclose any PHI to the person requesting the amendment without first following the Verification Policies and Procedures, PP1.12. This means that you may only disclose PHI if:

1. You know the identity and authority of the person to receive the PHI, or
2. You first follow steps in the Verification procedure.

Note

Keep in mind that in some cases, disclosure of PHI may occur simply by confirming that a person is a patient of our Practice.

What to say: Follow these steps:

Step A If the identity and authority of the person making the request are known to you, respond to oral and written requests as described in Step 1.2 (oral) or Step 1.3 (written) below.

Step B If the identity or the authority of the person are not known to you, either follow the Verification Policies and Procedures, or respond to the request without disclosing any PHI.

For example, you may say: "*You need to present your request to our Practice's Privacy Official. It is our Practice's policy that I cannot discuss whether a person is or is not a patient. I also cannot discuss any request that you make to amend patient records.*"

Step 1.2

Oral Requests—What To Do

Depending on the circumstances, respond in one of the following two ways to Amendment Requests that are made orally. Use your best judgment as to what is better under the circumstances:

Option A State that the Practice's policy is that an Amendment Request must be in writing. Provide to the patient a Request to Amend Records (F2.2A) and explain that the form should be completed, signed, and provided to Privacy Official.

Note

A patient does not have to use this form (F2.2A), but the patient must make the request in writing.

Option B State that the Privacy Official is the contact person for making Amendment Requests and explain how to contact the Privacy Official.

Step 1.3

Written Requests—What To Do

If the request is made in writing, forward it promptly to the Privacy Official. Make sure you tell the Privacy Official the date the written request was received.

Step 1.4

Privacy Official Takes Over

The Privacy Official is responsible for the remaining steps in these procedures.
Proceed to Step 2.

Step 2: Privacy Official Intake of Amendment Request

Introduction

This procedure should be followed by the Privacy Official in order to facilitate the review of and response to an Amendment Request.

Step 2.1

Follow the Procedures of Step 1

Follow the procedures of Step 1: Respond to the Amendment Request.

Step 2.2

Document the Request

Step A Record the request in the Amendment Request Log (F2.2B), including the deadline for our response.

Step B Place the written Amendment Request in the Patient HIPAA File (PP3.4, Documentation Policies and Procedures, describes the Patient HIPAA File).

Step 2.3

Initiate Review Process

Proceed to Step 3.

Step 3: Review of Amendment Requests

Introduction

The Privacy Official should use this procedure to review and determine the appropriate response to an Amendment Request.

Step 3.1

Review the Request for Completeness

Review the Amendment Request to make sure that it contains sufficient information in order for the Practice to act on the request.

Step A Determine whether the request contains a reason to support the proposed amendment.

Step B If the request challenges the accuracy or completeness of a record maintained by the Practice, determine whether the request contains sufficient information for the Practice to evaluate whether the Practice's records are accurate and complete.

Step C Contact the patient to request any necessary additional information identified in Steps A and B.

Step D Discuss the Amendment Request with the creator of the record or the physician responsible for the patient's care, as appropriate, to determine if the PHI in the Practice's records is accurate and complete.

Step 3.2

Contact Business Associates

Contact Business Associates of the Practice who may have Designated Record Sets containing PHI that is the subject of the Amendment Request. Ask them to identify and produce to the Practice any Designated Records Sets that contain PHI subject to the request.

Step 3.3

Review Designated Record Sets Subject to Amendment Request

Identify and review the Designated Record Sets held by the Practice and its Business Associates that contain the PHI that is the subject of the patient's Amendment Request. The Designated Record Sets Log described in PP2.1 should assist you with this identification process.

Step 3.4

Determine Whether Grounds for Denial Exist

Determine if there are grounds for denying the Amendment Request. We may deny a patient's Amendment Request in the following four situations:

1. We may deny a patient's Amendment Request if the PHI was not created by our Practice. However, this ground for denial does not apply if the patient provides to

us a reasonable basis to believe that the originator of the PHI is no longer able to act on the requested amendment.

2. We may deny a patient's Amendment Request if the PHI is not part of a Designated Record Set.
3. We may deny a patient's Amendment Request if the PHI would not be available for inspection under the patient's right to access and copy PHI (refer to PP2.1, Step 3 of Access Request Procedures).
4. We may deny a patient's Amendment Request if the PHI is accurate and complete.

Step 3.5

Take Action On Request Within 60 Days or Request An Extension

Step A Take action on an Amendment Request and respond to the patient no later than 60 days after the Practice receives the request.

Step B If the Practice is unable to respond to the request within 60 days, we may extend the time to respond to the Amendment Request by no more than 30 days provided that we properly notify the patient.

- Proper notification means that no later than 60 days after the Practice receives the request, we provide the patient with (1) a written statement of the reasons for the delay and (2) the date by which the Practice will respond to the request; and
- The Practice is entitled to only one 30-day extension per request.

Step C If an extension is obtained, record the new deadline in the Amendment Request Log (F2.2B).

Step 3.6

Record Decision in Amendment Request Log

Once a decision has been made to accept or deny an Amendment Request, the Privacy Official shall record the decision in the Amendment Request Log (F2.2B).

Step 3.7

Implement Decision to Accept or Deny

To implement *acceptance* of an Amendment Request, in whole or in part, **proceed to Step 4.**

To implement *denial* of an Amendment Request, **proceed to Step 5.**

Step 4: (If Applicable) Accept the Amendment Request

Introduction

This procedure should be followed by the Privacy Official to implement acceptance of an Amendment Request. This procedure applies after the decision has been made to agree to or deny a request.

Step 4.1

Make the Amendment

To the extent that the Practice accepts an Amendment Request, make the appropriate amendment to the PHI that is the subject of the request.

Step A Complete an Accepted Amendment Form (F2.2C).

Step B Identify the Designated Record Sets that are affected by the amendment.

Step C Attach the Accepted Amendment Form (F2.2C) to the Designated Records Sets affected by the amendment.

- In general, do not delete the original information that is the subject of the amendment. Instead, make the following entry at the site of the information being amended: "See Attached Amendment [date] [Privacy Official initials]."
- Staple Accepted Amendment Form (F2.2C) to paper records containing the subject PHI.

- As appropriate and feasible, attach or link an electronic version of the amendment to Designated Record Sets in the Practice's computer system that contains the subject PHI.

Step 4.2

Inform the Patient

Step A Using the Response to Request to Amend Records (F2.2D), inform the patient in a timely manner that the requested amendment has been accepted.

Step B Place a copy of forms F2.2C and F2.2D in the Patient HIPAA File.

Step 4.3

Request Permission and Instructions to Disclose Amendment to Others

In Step 4.2, the Practice sent a Response to Request to Amend Records (F2.2D) to the patient. This notification asks the patient to agree in writing that the Practice may inform certain persons about the amendment. It also asks the patient to provide the Practice with a list of other persons the patient identifies as having received the PHI that is the subject of the amendment.

Step A When the Practice receives the patient's agreement to disclose the amendment included in F2.2D, document the agreement in the Amendment Request Log (F2.2B).

Step B Place form F2.2D, completed by the patient, in the Patient HIPAA File.

Step 4.4

Notify Others of Amendment

Step A After receiving the patient's agreement on form F2.2D, make reasonable efforts to inform the following persons of the accepted amendment within a reasonable time:

- Persons the patient identifies as having received PHI that is subject to the amendment; and
- Persons who the Practice knows have PHI that is subject to the amendment and who may have relied, or could foreseeably rely, on it to the detriment of the patient, including Business Associates of the Practice.

Step B Document in the Amendment Notification Confirmation (F2.2E) when notification is provided to authorized persons.

Step C Place the completed Amendment Notification Confirmation (F2.2E) in the Patient HIPAA File.

Confirm Documentation

Proceed to Step 6.

Step 5: (If Applicable) Deny the Amendment Request

Introduction

This procedure should be followed by the Privacy Official to implement a denial of an Amendment Request.

Step 5.1

Complete an Amendment Denial Letter

Complete the Response to Request to Amend Records (F2.2D) to provide to the requesting patient. This letter must explain:

- the basis for the denial.
- that the patient has a right to submit a written statement disagreeing with the denial and describe how to provide such a statement to the Practice's Privacy Official.
- that if the patient does not submit a statement of disagreement, the patient may request that the Practice provide the patient's Amendment Request and the Practice's denial with any future disclosures of the PHI that are the subject of the requested amendment.
- how the patient may complain to the Practice or to the Secretary of HHS. This description should include the name or title and telephone number of the Practice's Privacy Official.

Step 5.2

Send an Amendment Denial Letter to the Patient

Step A Send the Response to Request to Amend Records (F2.2D) to the patient in a timely manner.

Step B Place a copy of F2.2D in the Patient HIPAA File.

Step 5.3

Process Disagreement Statement From Patient

Our Practice will permit a patient to submit a written statement disagreeing with the denial of an Amendment Request and stating the basis for such disagreement (this is called a Disagreement Statement). Our Practice may reasonably limit the length of a patient's Disagreement Statement. Follow these steps to process a Disagreement Statement submitted by the patient.

Step A Record the Disagreement Statement in the Amendment Request Log (F2.2B).

Step B Place a copy of the Disagreement Statement in the Patient HIPAA File.

Step C Attach a copy of the Disagreement Statement to the patient's Designated Record Sets containing PHI subject to the Amendment Request.

Step 5.4

Prepare Practice Rebuttal

If the patient provides a Disagreement Statement, the Privacy Official, in his or her professional judgment, may prepare a written rebuttal letter from the Practice.

Step A Draft a rebuttal letter.

Step B Provide a copy of the rebuttal letter to the patient who submitted the Disagreement Statement.

Step C Record the rebuttal letter in the Amendment Request Log (F2.2B).

Step D Place a copy of the rebuttal letter in the Patient HIPAA File.

Step E Attach a copy of the rebuttal letter to the Designated Record Sets containing PHI subject to the Amendment Request.

Step 5.5

Future Disclosures Following Denial

Refer to the procedure for future disclosures specified later in PP2.2.

Step 5.6

Confirm Documentation

Proceed to Step 6.

Notice of Amendment By Another Covered Entity

Policy

It is our Practice's policy that we must take the following action if the Practice is informed by another covered entity about an amendment to PHI about a patient.

If the PHI that has been amended is contained in the Designated Record Sets that we maintain or that our Business Associates maintain on our behalf, our Practice must amend such PHI in our Designated Record Sets. To do this, follow the requirements of Step 4, Accepting the Amendment Request, as if we made the original decision to amend the PHI.

However, in these cases, the decision to make the requested amendment actually was made by the other Covered Entity. The documents created in Step 4 should reflect that the other Covered Entity made the decision to make the amendment, not our Practice.

Future Disclosures Following a Denial of an Amendment Request

Introduction

This procedure applies to disclosures of PHI made after an Amendment Request has been denied as to that PHI.

The PHI for which the Amendment Request was denied is called the Disputed PHI in these policies and procedures.

If the Patient Provides a Statement of Disagreement

If a patient submits a Disagreement Statement following the denial of an Amendment Request, *include the following documents* (or, at the Practice's election, an accurate summary of the information contained in the documents) *with any subsequent disclosure of the Disputed PHI*:

- Amendment Request Form (F2.2A);
- Response to Request to Amend Records (F2.2D);
- Disagreement Statement;
- Practice's rebuttal (if any).

Make an entry in the patient's physical and computer records where the Disputed PHI is located to highlight the requirement to provide such information with future disclosures.

If the Patient Does Not Provide a Statement of Disagreement

When an Amendment Request is denied, but the patient chooses not to submit a Disagreement Statement, include the patient's request for amendment and the denial (or an accurate summary of such information) with any subsequent disclosure of the PHI *only if the patient makes such a request* to include the request and denial in subsequent disclosures.

If the patient does make such a request to include the Amendment Request and the denial in future disclosures of the Disputed PHI, attach an appropriate "marker" in the patient's physical and computer records where the Disputed PHI is located highlighting the requirement to provide such information with future disclosures of the subject information.

> **Note**
>
> An appropriate "marker" may include a sticker attached to physical records or an electronic note in a computer database.

HIPAA Standard Transactions

If a subsequent disclosure is made using a HIPAA standard transaction that does not permit inclusion of the additional material (request, denial letter, Disagreement Statement, and rebuttal), separately submit the material to the recipient of the standard HIPAA transaction.

Step 6: Confirm Amendment Request Documentation

Introduction

The Privacy Official should ensure the following documentation is maintained by the Practice regarding Amendment Requests. This documentation must be maintained in compliance with the requirements of General Documentation Policy, PP3.4.

Contact for Amendment Requests

The Practice's Privacy Official is the contact person for Amendment Requests and is responsible for receiving and processing Amendment Requests.

Document All Communications Required To Be In Writing

Retain copies of all communications that the Privacy Rule requires to be in writing relating to Amendment Requests.

These communications include:

- Amendment Request Form (F2.2A);
- Response to Request to Amend Records (F2.2D);
- Disagreement Statement;
- Rebuttal letter.

The Privacy Official should also maintain copies of patient authorizations and letters providing others with notice of an accepted amendment, along with the Amendment Notification Log (F2.2E) documenting such notices.

Regularly Review Amendment Request Log

The Privacy Official shall regularly review the Amendment Request Log (F2.2B) for compliance with these policies and procedures.

F2.2A

Name of Practice:

Address:

Privacy Official:

Telephone:

Request to Amend Records

Notice to Patient: Use this form to make a request to our Practice that we amend or make corrections to information maintained about you.

In order for our Practice to respond promptly and accurately to your Amendment Request, please complete this form in its entirety.

Patient Name: _____
[print or type]

Requested Amendment

Please describe in detail how you want records amended.

_____

_____

_____

_____

Reason For Requested Amendment

Please specify the reason(s) for your request.

_____

_____

_____

Contact Person

Please contact our Practice's Privacy Official if you have any questions relating to your request for amendment of records.

Patient Information

Print Name of Patient: _____

Signature of Patient: _____

Date: _____

Date of Birth (for identification purposes): _____

For Personal Representative of the Patient (if applicable)

Print Name of Personal Representative: _____

Describe Personal Representative Relationship: _____ (parent, guardian, power of attorney, etc.)

I hereby certify that I have the legal authority under applicable law to make this request on behalf of the patient identified above.

Signature of Personal Representative: _____Date: _____

F2.2B

Name of Practice:

Date Last Revised:

Amendment Request Log

Patient Name	Chart/ID Number	Date of Request	Response Deadline	Response to Request G=Grant D=Deny G/D=Both	Date Permission Granted to Notify Others of Amendment[1] (if applicable)	Disagreement Statement Date (if applicable)	Rebuttal Statement Date (if applicable)

1. The Practice must notify the patient if it accepts the patient's Amendment Request. The Practice may not notify others about the amendment unless it has received written permission from the patient. The Practice should document in this log when it receives such written permission from the patient. The Practice should use the Amendment Notification Log to document when it notifies others about the amendment.

F2.2C

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Accepted Amendment Form

Patient Information

Patient Name: _____

Patient Chart/ID Number: _____

Date of Amendment Request: _____

Amendment of Patient Records

The records of the Patient named above are amended as follows:

_____

_____

_____

_____

_____

_____

_____

_____

___ Check here if additional pages attached.

Patient Records Affected By Amendment

The following Patient records are affected by this Amendment:

_____

_____

_____

_____

_____

_____

Contact Person

Please contact the Practice Privacy Official if you have any questions relating to this Amendment.

Signature _____ Date _____

(Privacy Official)

F2.2D

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Response to Request to Amend Records

Patient Name: _____

Patient Chart/ID Number: _____

Date of Amendment Request: _____

Amendment Request Date: _____

Dear Patient:

You have made a request that our Practice amend certain records about you. This is our response to your request.

As we explain below, your Amendment Request is:

☐ Granted

☐ Denied

☐ Granted In Part, Denied In Part

_____ Grant of Your Amendment Request (In Whole or In Part)
[check if applicable]

Our Practice *grants* your Amendment Request to the extent specified below.

_____

_____

_____

_____

We will amend the records maintained by our Practice that are affected by this Amendment. In addition to amending our own records, with your permission, we will contact other persons who we know have health information that is subject to this Amendment and who may have relied, or could foreseeably rely, on such information to your detriment. We would also be pleased to provide notification of this Amendment to other persons you identify as having received health information that is affected by the Amendment.

In order to provide us with permission to notify others of your amendment to health information, please fill out the attached Authorization form and return it to me. You may also contact us if you have any questions regarding your Amendment Request and our response to your Request.

_____ Denial of Your Amendment Request (In Whole of In Part)
[check if applicable]

Our Practice *denies* your Amendment Request to the extent and for the reason(s) specified below.

Amendment Request Denied as Follows:

_____

_____

_____

_____

_____

Reason for Denial:

_____ The protected health information (PHI) that is the subject of the Amendment Request was not created by our Practice. PHI is individually identifiable health information that is maintained or transmitted by our Practice.

_____ The PHI that is the subject of the Amendment Request is not part of a Designated Record Set maintained by our Practice.

_____ The PHI that is the subject of the Amendment Request would not be available for inspection under the HIPAA Privacy Rule.

_____ The PHI that is the subject of the Amendment Request is accurate and complete.

You have the right to submit a written statement disagreeing with our denial of your Amendment Request. You may submit this statement of disagreement to me, the Practice's Privacy Official.

If you do not submit a statement of disagreement, you may request that our Practice provide your Amendment Request and our denial of your request with any future disclosures of PHI that is the subject of the Amendment Request.

You also have the right to submit a complaint regarding the denial of your Amendment Request to our Practice and to the Secretary of the United States Department of Health and Human Services. To complain to our Practice, you may submit a complaint to me, the Practice Privacy Official. I may be reached using the contact information listed at the top of this letter. You may also file a written complaint with the Secretary of the United States Department of Health and Human Services within 180 days of any alleged violation. Such a complaint must name the entity that is the subject of the complaint and describe the acts or omissions believed to be in violation of the HIPAA Privacy Rule.

Please feel free to contact me if you have any questions relating to your Amendment Request.

Sincerely,

Privacy Official: _____

Signature: _____

Date: _____

[Note: Include this form only when an Amendment Request is granted in whole or in part.]

Authorization to Provide Notification About Amendment

[DATE]

Privacy Official: _____
Practice: _____
Address: _____
_____

Dear Privacy Official:

I understand that your Practice has made or plans to make an amendment to records about me. I hereby authorize your Practice to notify other persons of the Amendment who you know have health information that is subject to this Amendment and who may have relied, or could foreseeably rely, on such information to my detriment.

I also hereby authorize your Practice to notify the following additional persons about this Amendment:

[Please specify name and address of persons to receive notification of Amendment]

1)

2)

3)

Print Name of Patient: _____
Signature of Patient: _____
Date: _____
Date of Birth (for identification purposes):_____

For Personal Representative of the Patient (if applicable)
Print Name of Personal Representative: _____
Describe Personal Representative Relationship: _____
(parent, guardian, power of attorney, etc.)

I hereby certify that I have the legal authority under applicable law to make this request on behalf of the patient identified above.

Signature of Personal Representative: _____

Date: _____

Name of Practice:

Last Updated:

Amendment Notification Confirmation

Patient Name:_____

Patient Chart/ID Number:_____

Date of Accepted Amendment:_____

Person Notified (and address)	Date of Notice	Why Person Notified?[1] (Request of Patient or Practice Determination)

1. The Practice should specify whether the notification is provided because (1) the recipient was specifically identified by the patient, or (2) the Practice has determined, with the consent of the patient, that it must provide notification because the recipient has PHI that is subject to the amendment and may rely, or could foreseeably rely, on such PHI to the detriment of the patient.

PATIENT RIGHTS: ACCOUNTING PP2.3

Overview

Introduction

This section contains our Practice's policies and procedures specifically relating to a patient's request for an accounting of disclosures of PHI made by our Practice. This type of request is called a Disclosure Accounting Request in these policies and procedures. The Privacy Rule generally provides that a patient may request an accounting of certain types of disclosures of PHI that are made about the patient. This requirement applies both to disclosures made by our Practice and to certain disclosures by our Business Associates on our behalf.

Tracking Policies and Procedures

Every employee should read Part A of PP2.3.

Part A of PP2.3 describes our Practice's policies and procedures for tracking and logging PHI disclosures that are subject to patients' rights to make Disclosure Accounting Requests.

Processing Policies and Procedures

Part B of PP2.3 describes our Practice's procedures for processing Disclosure Accounting Requests.

Every employee should be able to perform Step 1 of Part B, Respond to the Accounting Request.

Contact Person

Our Privacy Official is the contact person for questions, suggestions, or complaints about our Practice's affairs relating to Disclosure Accounting Requests or our compliance with the Privacy Rule related to disclosure accounting.

Part A: Document all Disclosures Subject to an Accounting

Introduction

The Practice must document each disclosure subject to a patient's disclosure accounting rights under the Privacy Rule. We must do this to provide timely and accurate accountings of disclosures of PHI subject to patients' rights to make Disclosure Accounting Requests.

Policy

Our policy is to document all disclosures of PHI made by our Practice (or our Business Associates on our behalf), except for the types of disclosures listed in the next section below. For disclosures that are not subject to an exception or listed in a Research Accounting, the information that must be documented includes the following:

- Date of the disclosure;
- Name of the entity or person receiving the information, and if known, the address of the entity or person;
- A brief description of the PHI disclosed; and

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

- A brief statement of the purpose of the disclosure, or if applicable, a copy of a written request from HHS for disclosure to HHS (defined in PP1.1), or a written request for a "public purpose" disclosure (defined in PP1.8).

Exceptions to Disclosure Accounting Requirement

Our policy is to document all disclosures of PHI, except for the following disclosures:

- Disclosures to carry out treatment, payment, or health care operations;
- Disclosures to the patient;
- Disclosures pursuant to a HIPAA-compliant Authorization;
- Disclosures for a facility directory or to persons involved in the patient's care, or for other notification purposes;
- Disclosures for national security or intelligence purposes;
- Disclosures to correctional institutions or law enforcement officials having lawful custody of a patient;
- Disclosures of Limited Data Set data in compliance with our policies and procedures for Limited Data Set data (PP1.11);
- Incidental Disclosures in compliance with our policies and procedures for Incidental Disclosures (PP1.7);
- Disclosures that occurred prior to April 14, 2003.

Note

If there is a question as to whether a disclosure is subject to an exception to the Disclosure Accounting requirements, you should ask the Privacy Official.

Log/Document Disclosures

Each employee making a disclosure that is subject to an accounting shall use the Practice PHI Disclosure Log (F2.3A) to document the disclosures (or use a copy of a page from the Log and provide the completed copy to the Privacy Official). Promptly consult with the Privacy Official before completing this information, unless you have been authorized by the Privacy Official or Practice Manager to complete it on your own.

Require Business Associates to Log/ Document Disclosures

The Privacy Official shall provide the Business Associate PHI Disclosure Log (F2.3B) to all of the Practice's Business Associates and require such Business Associates to use this form or other acceptable means to log all disclosures of PHI by the Business Associate that are subject to the disclosure accounting requirements under the Privacy Rule.

Log/Document Research Disclosures

Both the Practice and its Business Associates (as applicable) shall document high-volume disclosures of PHI for research purposes that do not require an individual's authorization using the Research Disclosure Log (F2.3C). A high-volume research disclosure is defined as a disclosure of PHI about 50 or more persons.

Periodically Review Practice Disclosure Log

The Privacy Official shall regularly update and maintain the Practice Disclosure Log (F2.3A). The Privacy Official may direct properly trained employees to make entries of the information requested in the Log as appropriate.

Part B: Processing Disclosure Accounting Requests

Policy

Our Practice's policy is to provide, upon a patient's request, an accounting of our Practice's disclosures of PHI about the patient other than for the types of disclosures listed below.

Scope of Policy

This policy applies to all requests made to the Practice for an accounting of disclosures of PHI.

This policy applies to disclosures made by the Practice and by our Business Associates on our behalf.

Exceptions to Disclosure Accounting Requirement

Our policy is that we will not provide an accounting of the following disclosures:

- Disclosures to carry out treatment, payment, or health care operations;
- Disclosures to the patient who is the subject of the disclosed PHI;
- Disclosures pursuant to a HIPAA-compliant Authorization;
- Disclosures for a facility directory or to persons involved in the patient's care, or for other notification purposes;
- Disclosures of Limited Data Set information in compliance with our Limited Data Set Policies and Procedures (PP1.11);
- Disclosures as Incidental Disclosures in compliance with our policies and procedures for Incidental Disclosures (PP1.7);
- Disclosures for national security or intelligence purposes;
- Disclosures to correctional institutions or law enforcement officials having lawful custody of a patient; or
- Disclosures made prior to April 14, 2003.

Content of Accounting

The accounting that we provide to a patient upon the patient's request shall contain the following information for each disclosure:

- Date of the disclosure;
- Name of the entity or person receiving the information, and if known, the address of the entity or person;
- A brief description of the PHI disclosed; and
- A brief statement of the purpose of the disclosure, or if applicable, a copy of a written request from HHS for disclosure to HHS (defined in PP1.1), or a written request for a "public purpose" disclosure (defined in PP1.8).

PATIENT RIGHTS: ACCOUNTING PP2.3

Index of Procedures

Introduction

Providing an Accounting of Disclosures of PHI involves a multi-step process. Every employee shall perform Step 1, How to Respond to Disclosure Accounting Requests, when a Disclosure Accounting Request is presented to the employee.

The Privacy Official is responsible for performing Steps 2 through 5.

Steps For Providing an Accounting

Follow these steps to provide an Accounting of Disclosures:

Step	Action
1	Respond to Disclosure Accounting Request.
2	Privacy Official Intake.
3	Review Request.
4	Provide the Accounting.
5	Confirm Documentation.

Other Procedures

Use these additional procedures in this section as needed:

Action
Suspend right to an Accounting.
Provide summary information for multiple disclosures.
Provide Accounting for certain high-volume research disclosures.

Step 1: Respond to the Disclosure Accounting Request PP2.3

Introduction

This procedure should be followed by any Practice employee to respond to a Disclosure Accounting Request made to the employee. This applies to requests made by a patient or a person stating that he or she is acting on behalf of a patient.

What Is a Disclosure Accounting Request?

A Disclosure Accounting Request is a request by the patient that our Practice provide an accounting of the disclosures that have been made of the patient's PHI over a specified period of time.

Step 1.1

Do Not Disclose PHI Without Verifying Identity and Authority

Caution: Do not disclose any PHI to the person requesting the accounting without first following the Verification Policies and Procedures, PP1.12. This means that you may only disclose PHI if:

1. You know the identity and authority of the person to receive the PHI, or
2. You first follow steps in the Verification procedure.

Note

Keep in mind that, in some cases, disclosure of PHI may occur simply by confirming that a person is a patient of our Practice.

What to say (follow these steps):

Step A If the identity and authority of the person making the request are known to you, respond to oral and written requests as described in Step 1.2 (oral) or Step 1.3 (written) below.

Step B If the identity or the authority of the person is not known to you, either follow the Verification Policies and Procedures, or respond to the request without disclosing any PHI.

For example, you may say: "*You need to present your request to our Practice's Privacy Official. It is our Practice's policy that I cannot discuss whether a person is or is not a patient. I also cannot discuss any request that you make regarding an accounting of disclosures.*"

Step 1.2

Oral Requests—What To Do

Respond in one of the following two ways to Disclosure Accounting Requests that are made orally. Use your best judgment to determine which of the following options is better under the circumstances:

Option A Explain that although a Disclosure Accounting Request is not required to be in writing, a written request will assist our Practice in providing a timely response. Provide the patient with a Request for Disclosure Accounting (F2.3D) and explain that it should be completed, signed, and provided to the Privacy Official.

Option B Explain that the Privacy Official is the contact person for making Disclosure Accounting Requests and explain how to contact the Privacy Official.

Step 1.3

Written Requests—What To Do

If the request is made in writing, forward it promptly to the Privacy Official. Make sure you tell the Privacy Official the date the written request was received.

Step 1.4

Privacy Official Takes Over

The Privacy Official is responsible for the remaining steps in these procedures.
Proceed to Step 2.

Step 2: Privacy Official Intake of Disclosure Accounting Request

---

Introduction

This procedure should be followed by the Privacy Official in order to facilitate the review of and response to a Disclosure Accounting Request.

Step 2.1

Follow the Procedures of Step 1

Follow the procedures of Step 1, Respond to the Disclosure Accounting Request.

Step 2.2

Step A Record the request in the Accounting Request Log (F2.3E), including the deadline for our response.

Step B Place the written Request for a Disclosure Accounting in the Patient HIPAA File. Documentation Policies and Procedures, PP3.4, describes the Patient HIPAA File.

Step 2.3

Initiate Review Process

Proceed to Step 3.

Step 3: Review of a Request For an Accounting

Introduction

This procedure should be used by the Privacy Official to review and determine the appropriate response to a Disclosure Accounting Request.

Step 3.1

Review Disclosure Logs

Step A Identify the disclosures contained in the Practice PHI Disclosure Log (F2.3A) relating to the PHI that are subject to the Disclosure Accounting Request.

Step B Review the patient's chart or any other Practice records as appropriate to identify any other disclosures that may be subject to an accounting.

Step 3.2

Review Business Associate Disclosure Logs

Disclosures of PHI by our Business Associates may also be subject to a patient's right to a Disclosure Accounting Request. Follow this procedure to identify Business Associate disclosures that are subject to an accounting.

Step A Contact Business Associates of the Practice who may have made disclosures of PHI about the patient subject to an accounting. Ask Business Associates to identify and produce to the Practice an accounting of disclosures subject to an accounting, including those contained in Business Associate PHI Disclosure Logs (F2.3B).

Note

The Privacy Official is required to provide a Business Associate PHI Disclosure Log (F2.3B) to Business Associates for their use in logging disclosures.

Step B Review the logs or lists provided by Business Associates.

Step 3.3

(If Applicable) Review Research Disclosure Logs

Step A Review the research disclosures contained in the Research Disclosure Logs (F2.3C) maintained by both the Practice and its Business Associates.

Step B Identify the disclosures occurring during the time frame specified in the Disclosure Accounting Request. Refer to the Research Accounting Procedures (PP2.3).

Step 3.4

Do Exceptions Apply?

Step A Determine if any of the disclosures identified in Steps 3.1 through 3.3 are subject to an exception.

The accounting provided by the Practice need not include disclosures:

- To carry out treatment, payment, or health care operations;
- To the patient;
- Pursuant to a HIPAA-compliant authorization;
- For a facility directory, or to persons involved in the patient's care, or for other notification purposes;
- For national security or intelligence purposes;
- Incident to disclosures in compliance with the HIPAA Privacy Rule;
- Of Limited Data Set information in compliance with our policies and procedures for Limited Data Set data;
- To correctional institutions or law enforcement officials having lawful custody of a patient; or
- That occurred prior to April 14, 2003.

Step B Mark Excepted Disclosures: If a disclosure listed in a Disclosure Log is subject to an exception from the accounting requirement, exclude it from the accounting provided to the requestor in Step 4 (the Privacy Official may waive as warranted in exceptional cases). Also mark and initial the disclosure in the log as being subject to an exception.

Step C Complete Disclosure Accounting Form. Unless a shorter time is specified in the request, use Response to Request for a Disclosure Accounting (F2.3F) to list all disclosures of PHI that occurred during the 6 years prior to the date of the request (but not before April 14, 2003).

Step 3.5

Respond to Request Within 60 Days

Step A Where reasonably practical, provide an accounting of disclosures no later than 60 days after the Practice receives the request.

Step B If the Practice is unable to provide an accounting within 60 days, it may extend the time to provide the accounting by no more than 30 days, provided that:

- No later than 60 days after the Practice receives the request for an accounting, it provides the patient with (1) a written statement of the reasons for the delay and (2) the date by which the Practice will provide the accounting; and
- To provide the requested accounting, the Practice is only entitled to one 30-day extension per request.

Proceed to Step 4.

Step 3.6

(If Applicable) Temporary Suspension

If a law enforcement official or a health oversight agency has requested a temporary suspension of an individual's right to an accounting, such disclosures may not be disclosed to the requestor. Temporary suspension requests will be handled according to the procedure set forth at the end of PP2.3.

Step 4: Provide the Requested Accounting

Introduction

This procedure applies where a decision has been made to provide a Disclosure Accounting to the patient. This procedure should be followed by the Privacy Official to provide the accounting.

Step 4.1

Letter Granting Request

Step A Provide the patient with the requested accounting by completing the Response to Request for a Disclosure Accounting (F2.3F) (and attaching, if applicable, a Summary Information Accounting (F2.3G) and a Research Accounting Form (F2.3H)).

Step B Make a copy of the forms that are provided to the patient. Place the copy in the Patient HIPAA File.

Step 4.2

Content of the Accounting

The accounting shall list all disclosures that are not subject to an exception or a temporary suspension request. The following information should be provided for each listed disclosure:

- Date of the disclosure;
- Name of the entity or person receiving the information and, if known, the address of the entity or person;
- A brief description of the PHI disclosed; and
- A brief statement of the purpose of the disclosure or, if applicable, a copy of a written request from HHS for disclosure to HHS (defined in PP1.1), or a written request for a "public purpose" disclosure (defined in PP1.8).

The Response to a Request for a Disclosure Accounting Response (F2.3F) contains each of these required elements and should be completed in its entirety.

Note

Summary information may be provided for multiple or routine disclosures to the same person or entity.

Note

Summary information may be provided for certain high-volume disclosures for research purposes.

Step 4.3

Determine Cost of Accounting

Step A Review the Disclosure Accounting Log to determine if the accounting is the first to the patient in any 12-month period.

Step B *First Accounting.* If it is the first requested accounting in any 12-month period, the accounting must be provided at no charge to the patient.

Step C *Additional Accountings.* Impose a reasonable, cost-based fee for additional accounting requests within a 12-month period.

Before imposing a fee for an additional accounting, inform the patient in advance of the fee and provide the patient with an opportunity to withdraw or modify his or her request in order to avoid or reduce the fee.

Step 4.4

Confirm Documentation

Proceed to Step 5.

Step 5: Confirm Documentation

Introduction

The Privacy Official should ensure the following documentation is maintained by the Practice consistent with the requirements of PP3.4.

Disclosures Subject to an Accounting

Use the Practice PHI Disclosure Log (F2.3A), Business Associate PHI Disclosure Log (F2.3B), and the Research Disclosure Log (F2.3C) to document all disclosures of PHI that are subject to an accounting.

Accountings Provided to Patients

Document all accountings provided to patients.

This documentation requirement may be met by maintaining a copy of the Response to Request for a Disclosure Accounting (F2.3F), and if applicable, any Summary Information Accountings (F2.3G), Research Accountings (F2.3H), or other documentation provided to the patient.

Contact for Receiving and Processing Requests for an Accounting

The Practice's Privacy Official is the contact person and is responsible for receiving and processing patients' requests for an accounting.

Other Documentation

Retain a copy of a patient's Disclosure Accounting Request (F2.3A). Refer to Step 2.

Regularly Review Accounting Request Log

The Privacy Official should regularly review the Accounting Request Log (F2.3E) for compliance with these policies, procedures, and deadlines.

PATIENT RIGHTS: ACCOUNTING PP2.3

(If Applicable) Suspend Right to an Accounting

Introduction

This Procedure describes the limited circumstances in which the Practice must suspend a patient's right to receive an accounting of disclosures to a law enforcement official or health oversight agency.

Scope of Limitation

This Procedure only limits a patient's right to receive an accounting of disclosures to:

- Law enforcement officials; or
- Health oversight agency.

Written Statement by Agency or Official

Our Practice shall temporarily suspend a patient's right to receive an accounting of disclosures that were made to a health oversight agency or a law enforcement official, if the agency or official provides the Practice with a written statement:

(1) that such an accounting would be reasonably likely to impede the agency's activities; and

(2) specifying the time for which such a suspension is required.

We will then maintain the suspension of the right to an accounting for the time specified by such agency or official.

Oral Statement by Agency or Official

If the agency's or official's statement is made orally, rather than in writing, the Privacy Official must:

Step A Document the statement, including the identity of the agency or official;

Step B Temporarily suspend the patient's right to an accounting of the disclosure subject to the statement; and

Step C Limit the temporary suspension to no longer than 30 days from the date of the oral statement, unless a written statement is then provided by the agency or official.

Document Temporary Suspension

Document any temporary suspension in the Patient HIPAA File, and if applicable, in the Accounting Request Log (F2.3E).

PATIENT RIGHTS: ACCOUNTING PP2.3

(If Applicable) Provide Summary Information For Multiple Disclosures

Introduction

This procedure describes how the Practice may provide summary information for certain types of multiple disclosures (this is optional).

Types of Disclosures

The Practice may provide summary information for multiple disclosures if such disclosures are to the same person or entity for a *single purpose* and the disclosures are either:

- To HHS at the request of HHS (see P1.1); or
- The type of "public purpose" disclosures described in PP1.8.

Content of Summary Information

Summary information must include all of the following:

- For the first disclosure, the Practice must provide the same information required for other ordinary disclosures. The specific content requirements for this disclosure are described in Step 4 and contained in the Response to Request for a Disclosure Accounting (F2.3F).
- The Practice must specify the frequency or number of such disclosures made during the accounting period.
- The Practice must specify the date of the last disclosure during the accounting period.

Providing Summary Information

Use the Summary Information Accounting Form (F2.3C) to provide summary information to a requesting patient.

PATIENT RIGHTS: ACCOUNTING PP2.3

(If Applicable) Provide Accounting for Certain High Volume Research Disclosures

Introduction

If the Practice makes disclosures of PHI about 50 or more patients for research purposes that do not require an authorization, the Practice may account for such disclosures by providing a requesting patient with general information about the research for which the patient's PHI may have been disclosed.

The special accounting provided for high-volume research disclosures is called a Research Accounting in these policies and procedures.

> **Note**
>
> A Research Accounting requires a Practice to provide general information about high-volume research disclosures, while allowing the Practice to reduce the administrative burden of accounting for each individual disclosure.

Disclosure Must Contain PHI For 50 or More Patients

A research disclosure must include PHI for 50 or more patients in order for the Practice to be able to provide a Research Accounting for that disclosure.

If the research disclosure is for fewer than 50 patients, the standard accounting procedures apply and each disclosure of PHI must be individually documented. Refer to Steps 3 through 5 of PP2.3.

Types of Research Disclosures

In addition to including 50 or more patients, Research Accounting disclosures must be made for research purposes that do not require an authorization. See PP1.8.

The Privacy Rule allows the Practice to disclose PHI for research without an authorization in the following circumstances:

- Disclosure of PHI based on an Institutional Review Board or Privacy Board waiver of authorization;
- Disclosure of PHI made to a researcher for reviewing information prior to conducting research; and
- Disclosure for research using PHI of deceased individuals.

Log/Document Disclosures

Use the Research Disclosure Log (F2.3C) to record research disclosures that meet the requirements for a Research Accounting.

The Practice is not required to use the standard Practice PHI Disclosure Log (F2.3A) to track individual disclosures if the requirements for a Research Accounting are met.

Content of Research Accounting

A Research Accounting must include all of the following:

- The name of the protocol or other research activity;
- A description, in plain language, of the research protocol or other research activity, including the purpose of the research and the criteria for selecting particular patient records;
- A brief description of the type of PHI that was disclosed;
- The date or period of time during which such disclosures occurred, including the date of the last such disclosure during the accounting period;
- The name, address, and telephone number of the entity that sponsored the research and of the researcher to whom the information was disclosed; and
- A statement that the PHI of the individual may or may not have been disclosed for a particular protocol or research activity.

Provide a Research Accounting	Step A	Review the Research Disclosure Log (F2.3C) and list on the Research Accounting Form (F2.3H) the research disclosures subject to a Research Accounting that occurred during the specified accounting period.
	Step B	Attach the Research Accounting Form (F2.3H) to the Response to Request for a Disclosure Accounting (F2.3F) provided to the requesting patient. Refer to Step 4.
	Step C	If the Practice provides a Research Accounting and if it is reasonably likely that the PHI of the requesting patient was disclosed for such research protocol or activity, the Practice shall, at the request of the individual, assist in contacting the entity that sponsored the research and the researcher.

F2.3A

Name of Practice:

Address:

Privacy Official:

Telephone:

Practice Protected Health Information Disclosure Log

Patient Name	Chart/ID Number	Date of Disclosure[1]	Name and Address (if known) of Person Receiving Disclosure	Description of the Protected Health Information Disclosed	Purpose of Disclosure[2]

1. Do not log disclosures that are made: (1) to carry out treatment, payment, or health care operations; (2) to the patient; (3) incidental to an otherwise permitted use or disclosure; (4) pursuant to a HIPAA-compliant authorization; (5) for a facility directory, to persons involved in the patient's care, or for other notification purposes; (6) for national security or intelligence purposes; (7) to correctional institutions or law enforcement officials having lawful custody of a patient; (8) in compliance with the Practice's Limited Data Set disclosure policy; or (9) prior to April 14, 2003. High-volume disclosures for research should be documented in the Research Disclosure Log.

2. As applicable, include a copy of any written request from HHS for disclosure to HHS (defined in PP1.1 or any written request for a "public good" disclosure (defined in PP1.8).

Name of Practice:	Business Associate:
Address:	Address:
Privacy Official:	Contact Person:
Telephone:	Telephone:

Business Associate Protected Health Information Disclosure Log

Patient Name	Chart/ID Number	Date of Disclosure[1]	Name and Address (if known) of Person Receiving Disclosure	Description of the Protected Health Information Disclosed	Purpose of Disclosure[2]

1. Business Associates of the Practice should use this form to log disclosures of PHI that are required to be accounted for under the Privacy Rule. Do not log disclosures that are made: (1) to carry out treatment, payment, or health care operations; (2) to the patient; (3) incidental to an otherwise permitted use or disclosure; (4) pursuant to a HIPAA-compliant authorization; (5) for a facility directory or to persons involved in the patient's care, or for other notification purposes; (6) for national security or intelligence purposes; (7) to correctional institutions or law enforcement officials having lawful custody of a patient; (8) in compliance with the Practice's Limited Data Set disclosure policy; or (9) prior to April 14, 2003. High-volume disclosures for research should be documented in the Research Disclosure Log.

2. The Business Associate should provide to the Practice a copy of any written request from HHS or any written request for a "public good" disclosure (defined in Policy PP1.8).

F2.3C

Name of Practice:

Address:

Privacy Official:

Telephone:

Research Disclosure Log

Conditions

Befor a disclosure of Protected Health Information (PHI) may be documented using this Research Disclosure Log, the Privacy Official or other Practice employee documenting the disclosure must certify that the disclosure meets the following conditions:

1. The disclosure(s) includes PHI about 50 or more patients; *and*
2. The disclosure(s) was made for research purposes that do not require an authorization.

Name of Protocol or Other Research Activity	Description of Protocol or Other Research Activity (Including Purpose of Research and Selection Criteria)	Description of Type of PHI Disclosed	Date (or Period of Time) During Which Disclosures Occurred/Date of Last Disclosure	Name, Address, Telephone Number of Researcher *and* Entity Sponsoring Research

F2.3D

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Request For Disclosure Accounting

Notice to Patient: Use this form to make a request to our Practice that we provide you with an accounting of certain disclosures of protected health information that have been made by or on behalf of our Practice during the specified time period.

In order for our Practice to respond promptly and accurately to your Disclosure Accounting Request, please complete this form in its entirety.

Patient Name: _____
[print or type]

Disclosure Accounting Request:

Time frame for Accounting

Please specify the dates between which you would like for our Practice to account for disclosures of protected health information. Under the HIPAA Privacy Rule, our Practice is not required to account for disclosures made prior to April 14, 2003, or more than 6 years prior to your Request.

Starting Date For Accounting: _____

Ending Date For Accounting: _____

Requested Limitations on Scope of Accounting

Please specify if you would like for our Practice to limit our accounting to certain types of disclosures.

_____

_____

_____

_____

Contact Person

Please contact our Practice's Privacy Official if you have any questions relating to your Disclosure Accounting Request.

Patient Information

Print Name of Patient: _____

Signature of Patient: _____

Date: _____

Date of Birth (for identification purposes):_____

For Personal Representative of the Patient (if applicable)

Print Name of Personal Representative: _____

Describe Personal Representative Relationship: _____

(parent, guardian, power of attorney, etc.)

I hereby certify that I have the legal authority under applicable law to make this request on behalf of the patient identified above.

Signature of Personal Representative: _____ Date: _____

F2.3E

Name of Practice:

Address:

Privacy Official:

Telephone:

Accounting Request Log

Patient Name	Chart/ID Number	Request Date	Response Deadline	Date Accounting Provided	Temporary Suspension/Date Suspension Ends (if applicable)

F2.3F

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Response to Request for Disclosure Accounting

[DATE]

Patient Name: _____

Address: _____

_____

Chart/ID Number: _____

Request Date: _____

Dear Patient:

You have made a request to our Practice for an accounting of disclosures of protected health information (PHI) about you that our Practice has made during a specified period of time. The accounting that follows is our response to your request. This includes all disclosures required to be accounted for under the HIPAA Privacy Rule.

Time Period Covered By Accounting:

FROM: _____

UNTIL: _____

Date of Disclosure	Name and Address (if known) of Person Receiving Disclosure	Description of the PHI Disclosed	Purpose of Disclosure

Our Practice's accounting of disclosures may include summaries of common disclosures made repeatedly to the same entity for the same purpose and summaries of large-volume disclosures made for research purposes and not requiring a specific authorization. Such summaries, if any, are attached.

Please contact me if you have any questions relating to your Request for an Accounting of Disclosures.

Privacy Official: _____

Signature: _____

Date: _____

Telephone: _____

Address: _____

_____

Attachments—If Applicable

[Attach Summary Accounting—If Applicable]

[Attach Research Accounting—If Applicable]

F2.3G

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Summary Information Accounting

This form provides summary information about multiple disclosures made by our Practice to the same person or entity for the same purpose during the time period covered by the Disclosure Accounting Request.

Patient Information

Name _____ Patient Chart/ID Number _____

First Disclosure

Date of Disclosure:

_____

Name and Address (if known) of Person/Entity Receiving Disclosure:

_____

_____

Description of Protected Health Information Disclosed:

_____

_____

_____

Purpose of Disclosure:

_____

_____

_____

_____

Number/Frequency of Additional Disclosures

Our Practice made additional disclosures to the same person/entity for the same purpose at the frequency or number specified below:

_____

_____

_____

Date of Last Such Disclosure

_____

Please contact me if you have any questions relating to this Summary Accounting.

Privacy Official: _____

Signature: _____

Date: _____

F2.3H

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Research Disclosure Accounting

This form provides summary information about disclosures made by our Practice for research purposes that did not require an authorization and that included PHI of 50 or more persons. The disclosures listed in this form were made during the time specified in the patient's Request for a Disclosure Accounting.

Patient Information

Name _____ Patient Chart/ID Number _____

Time Period Covered By Accounting:

FROM: _____

UNTIL: _____

Research Accounting

Name of Protocol/Research Activity:

_____

Description of Protocol or Other Research Activity
(Including Purpose of Research and Selection Criteria):

_____

_____

_____

Description of Type of PHI Disclosed:

_____

_____

Date (or Period of Time) During Which Disclosures Occurred/Date of Last Disclosure:

_____

Contact Information for Researcher

Name: _____ Address: _____ Telephone Number: _____

_____

Contact Information for Entity Sponsoring Research

Name: _____ Address: _____ Telephone Number: _____

_____

Please contact me if you have any questions relating to this Research Accounting.

Privacy Official: _____

Signature: _____

Date: _____

PATIENT RIGHTS: ALTERNATIVE COMMUNICATIONS PP2.4

Overview

Introduction

A patient has the right to request to receive communications of PHI by alternative means or at alternative locations. That request is called an Alternative Communications Request in these policies and procedures. The HIPAA Privacy Rule requires our Practice to accommodate reasonable Alternative Communications Requests.

Policies and Procedures

PP2.4 describes our policies and procedures relating to Alternative Communications Requests.

Every employee should be able to perform Step 1, Respond to the Alternative Communications Request.

Contact person

Our Privacy Official is the contact person for questions, suggestions, or complaints about our Practice's affairs relating to Alternative Communications Requests and our compliance with the Privacy Rule related to Alternative Communications Requests.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PATIENT RIGHTS: ALTERNATIVE COMMUNICATIONS PP2.4

General Policy

Policy

Our Practice's policy is to accommodate reasonable requests by patients to receive communications of PHI from our Practice by alternative means or at alternative locations, subject to the conditions described below.

These requests are called Alternative Communications Requests in these policies and procedures.

Request Must Meet Certain Conditions

It is our policy to require that a patient make an Alternative Communications Request in writing.

Our Practice may, when appropriate, condition its accommodation of an Alternative Communications Request on receiving information as to how payment will be handled.

Our Practice may, when appropriate, condition its accommodation of the patient's Alternative Communications Request on the patient's specifying an alternative address or other means of contact.

Request Procedures

To process Alternative Communications Requests, use the step-by-step process discussed in the following Index of Procedures.

PATIENT RIGHTS: ALTERNATIVE COMMUNICATIONS PP2.4

Index of Procedures

Introduction

Processing Alternative Communications Requests involves a multi-step process.

Every employee should be able to perform Step 1, Respond to an Alternative Communications Request, when such a request is presented to the employee.

The Privacy Official is responsible for Steps 2 through 6.

List of Procedures

Follow these steps when processing Alternative Communications Requests:

Step	Action
1	Respond to the Alternative Communications Request.
2	Receive Request.
3	Privacy Official Intake.
4	Grant Request (if applicable).
5	Deny Request (if applicable).
6	Confirm Documentation.

Step 1: Respond to the Alternative Communications Request

Introduction

This procedure should be followed by any Practice employee to respond to an Alternative Communications Request made to the employee. This applies to requests from a patient or from a person stating that he or she is acting on behalf of a patient.

Step 1.1

Do Not Disclose PHI Without Verifying Identity and Authority

Caution: Do not disclose any PHI to the person requesting the amendment without first following the Verification Policies and Procedures, PP1.12. This means you may only disclose PHI if:

1. You know the identity and authority of the person to receive the PHI, or
2. You first follow steps in the Verification procedure.

Note

Keep in mind that, in some cases, disclosure of PHI may occur simply by confirming that a person is a patient of our Practice.

What to say: Follow these steps:

Step A If the identity and authority of the person making the request are known to you, respond to oral and written requests as described in Step 1.2 (oral) or Step 1.3 (written) below.

Step B If the identity or authority of the person is not known to you, either follow the Verification Policies and Procedures, or respond to the request without disclosing any PHI.

For example, you may say: "*You need to present your request to our Practice's Privacy Official. It is our Practice's policy that I cannot discuss whether a person is or is not a patient. I also cannot discuss any alternative communications request that you make.*"

Step 1.2

Oral Requests—What To Do

Respond in one of the following two ways to Alternative Communications Requests that are made orally. Use your best judgment and follow Privacy Official guidance when determining which response is better under the circumstances.

Option A State that the Practice's policy is that an Alternative Communications Request must be in writing. Provide the patient with a Request for Alternative Communications (F2.4A) and explain that it should be completed, signed, and provided to Privacy Official.

Note

A patient does not have to use F2.4, provided that the patient does make the request in writing. However, using the form will make it easier for our Practice to process the request.

Option B State that the Privacy Official is the contact person for making Alternative Communications Requests. Explain how to contact the Privacy Official.

Step 1.3

Written Requests—What To Do

If the request is made in writing, forward it promptly to the Privacy Official. Make sure you tell the Privacy Official the date the written request was received.

Step 1.4

Privacy Official Takes Over

The Privacy Official is responsible for the remaining steps in these procedures.
Proceed to Step 2.

Step 2: Privacy Official Intake of Alternative Communications Request

Introduction

This procedure should be followed by the Privacy Official in order to facilitate the review of and response to an Alternative Communications Request.

Step 2.1

Follow the Procedures of Step 1

Follow the procedures of Step 1, Respond to the Alternative Communications Request.

Step 2.2

Document the Request

Step A Record the request in the Alternative Communications Request Log (F2.4B).

Step B Place the written Alternative Communications Request in the Patient HIPAA File. PP3.4, Documentation Policies and Procedures, describes the Patient HIPAA File.

Step 2.3

Do Not Require Patient to Explain Basis for Request

Do not require the requesting patient to provide a basis or reason for his or her Alternative Communications Request.

Step 2.4

Initiate Review Process

Proceed to Step 3.

Step 3: Review of an Alternative Communications Request

Introduction

The Privacy Official should use this procedure to determine if an Alternative Communications Request should be granted.

Step 3.1

Review the Request for Completeness

Review the Alternative Communications Request to make sure it contains sufficient information in order for the Practice to act on the request. Follow these steps.

Step A Determine whether the request includes information as to how payment, if any, will be handled.

- Check to make sure that the Payment Information section of the Request for Alternative Communications (F2.4A) has been completed.
- If payment information has not been provided, contact the patient and explain this requirement. Do not process the request until such information is provided, subject to Privacy Official discretion.
- If additional information is not provided, **proceed to Step 5.**

Step B Determine whether the request specifies an alternative address or other means of contact.

- Check to make sure that the Alternative Address or Other Means of Contact section of the Request for Alternative Communications (F2.4A) has been completed.
- If an alternative address or other means of contact has not been provided, contact the requestor and explain this requirement. Do not process the request until such information is provided.
- If additional information is not provided, **proceed to Step 5.**

Step 3.2

Determine Whether the Request is Reasonable

Our policy is to accommodate all reasonable requests to receive communications by alternative means or at alternative locations. Our Privacy Official is responsible for making the decision regarding whether a request is reasonable.

- *What is reasonable?* The reasonableness of a request is based on the administrative difficulty of complying with the request. A request may not be denied simply because the Practice does not believe that alternative communications are necessary.

Example: A reasonable Alternative Communications Request may include a request by a patient that certain treatment information be sent to the patient's work address or provided by telephone call to a work, rather than home, phone number.

Step 3.3

Implement Decision to Grant or Deny Request

To *grant* an Alternative Communications Request, **proceed to Step 4.**
To *deny* an Alternative Communications Request, **proceed to Step 5.**

Step 4: (If Applicable) Grant the Alternative Communications Request

Introduction

This procedure should be followed by the Privacy Official to grant an Alternative Communications Request. This procedure applies after the decision has been made to agree to a request.

An Alternative Communications Request that has been granted by our Practice is called an Alternative Communications Accommodation in these procedures.

Step 4.1

Step A Use the Response to Request for Alternative Communications (F2.4C) to document the Alternative Communications Accommodation.

Step B Record the Alternative Communications Accommodation in the Alternative Communications Request Log (F2.4B).

Step C Place a copy of the Response to Request for Alternative Communications (F2.4C) in the Patient HIPAA File (described in Documentation, PP3.4).

Step D Incorporate the information contained in the Response to Request for Alternative Communications (F2.4C) into the patient's records maintained in all other places where patient contact information is listed, including in paper charts and in the Practice's clinical and billing computer systems.

Note

Ensure that all relevant computer records or files are updated to comply with the Alternative Communications Accommodation. Place a link, marker, or "flag" in any electronic record maintained about the patient where patient contact information is listed.

Step 4.2

Inform Staff

Inform appropriate staff members of the Alternative Communications Accommodation. All staff members who may communicate with the patient should be informed of the Alternative Communications Accommodation.

Note

Communication with staff may be accomplished by direct communication and by attaching the Response to Request for Alternative Communications (F2.4C) to the patient's chart and by updating the Practice's computer system to highlight the Alternative Communications Accommodation.

Step 4.3 **Inform Patient**	Immediately after completing Step 4.2, use the Response to Request for Alternative Communications (F2.4C) to notify the patient of the Alternative Communications Accommodation—and of course—do this in compliance with the Alternative Communications Accommodation!
Step 4.4 **Inform Business Associates**	Communicate the Alternative Communications Accommodation to the Practice's Business Associates that may communicate with the patient on behalf of the Practice. Request that Business Associates abide by the Alternative Communications Accommodation if communicating with the patient on the Practice's behalf.
Step 4.5 **Confirm Documentation**	**Proceed to Step 6.**

Step 5: (If Applicable) Deny the Alternative Communications Request

Introduction	This procedure should be followed by the Privacy Official to deny an Alternative Communications Request. This procedure applies after the decision has been made to deny an Alternative Communications Request.
Step 5.1 **Document Denial of the Request**	Step A Record the denial in the Alternative Communications Request Log. Step B Place a copy of the Response to Request for Alternative Communications (F2.4C) in the Patient HIPAA File.
Step 5.2 **Notify the Patient of the Denial**	Use the Response to Request for Alternative Communications (F2.4C) to inform the patient of the Practice's denial. Use professional judgment in determining the means of providing this form to the patient, taking into consideration the information contained in the Alternative Communications Request.

Step 6: Confirm Documentation

Introduction	The Privacy Official should ensure the following documentation is maintained by the Practice. Such documentation shall be maintained in compliance with the requirements of PP3.4.
Contact for Alternative Communications Requests	The Practice's Privacy Official is the contact person for Alternative Communications Requests. The Privacy Official is also responsible for receiving and processing Alternative Communications Requests.
Document All Alternative Communications Requests	The Privacy Official shall retain copies of all Requests for Alternative Communications (F2.4A). Keep copies in the Patient HIPAA File.
Documentation Response	The Privacy Official shall also keep copies of all Responses to Request for Alternative Communications (F2.4C) provided to patients. Keep these copies in the Patient HIPAA File.
Place "Flags" at Patient Contact Information in Records	Pursuant to Step 4.1, an Alternative Communications Accommodation needs to be "flagged" in the Practice's records where patient contact information is affected.
Regularly Review Alternative Communications Request Log	The Privacy Official shall regularly review the Alternative Communications Request Log (F2.4B) for compliance with these policies and procedures.

F2.4A

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Request for Alternative Communications

Notice to Patient: Use this form to make a request to our Practice that we communicate with you by alternative means or alternative locations (Alternative Communications Request).

In order for our Practice to respond promptly and accurately to your Alternative Communications Request, please complete this form in its entirety.

Patient Name: _____
[print or type]

Proposed Alternative Communication

Please describe in detail your proposed alternative means or location for receiving communications from our Practice.

_____

_____

_____

_____

Payment Information

Your Alternative Communications Request may affect our Practice's normal procedure of mailing bills to your home address. Please specify an alternative method for handling payment.

_____

_____

Alternative Address or Other Means of Contact

Please specify an alternative address or other means of contact.

_____

_____

Contact Person

You may contact our Practice's Privacy Official if you have any questions relating to your Alternative Communications Request.

Patient Information

Print Name of Patient: _____

Signature of Patient: _____

Date: _____

Date of Birth (for identification purposes): _____

For Personal Representative of the Patient (if applicable):

Print Name of Personal Representative: _____

Describe Personal Representative Relationship: _____ (parent, guardian, power of attorney, etc.)

I hereby certify that I have the legal authority under applicable law to make this request on behalf of the patient identified above.

Signature of Personal Representative: _____ Date:_____

F2.4B

Name of Practice:

Last Updated:

Alternative Communications Request Log

Patient Name	Chart/ID Number	Request Date	Response Deadline	Response to Request; Date G=Grant D=Deny G/D=Both	Date Practice Notifies Staff/BAs About Accepted Request

F2.4C

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Response to Request for Alternative Communications

Patient Name: _____

Address: _____

_____

Chart/ID Number: _____

Request Date: _____

Dear Patient:

You have made a request to our Practice that you receive communications of health information about you by alternative means or at alternative locations. This is our response to your request.

As we explain below, your Alternative Communications Request is granted or denied to the extent specified below.

_____ Grant of Your Alternative Communications Request (In Whole or In Part)
[check only if applicable]

Our Practice *grants* your Alternative Communications Request to the extent specified below.

_____

_____

_____ Denial of Your Alternative Communications Request (In Whole of In Part)
[check only if applicable]

Our Practice *denies* your Alternative Communications Request to the *extent* and for the *reason(s)* specified below:

_____ Your Request failed to provide sufficient information related to how payment would be handled.

_____ Your Request failed to provide an alternative address or other means of contact.

_____ The administrative difficulty of complying with your Request was deemed unreasonable.

Contact Person

Please contact me if you have any questions relating to your Alternative Communications Request.

Privacy Official: _____

Signature: _____

Date: _____

Telephone: _____

Address: _____

_____

PATIENT RIGHTS: FURTHER RESTRICTIONS PP2.5

Overview

Introduction

The HIPAA Privacy Rule provides a patient with the right to request that our Practice agree to additional restrictions that go beyond what the Privacy Rule requires for uses and disclosures of PHI for treatment, payment, and health care operations. A patient also has the right to request further restrictions for "opt-out" disclosures to family and friends involved in the patient's care.

These types of requests by patients are called Further Restriction Requests in these policies and procedures. *Our Practice is not required to agree to these requests.*

Policies and Procedures

PP2.5 describes our policies and procedures regarding Further Restriction Requests.

Every employee in the Practice should read Further Restrictions—General Policy and be able to perform Step 1, Respond to the Further Restriction Request.

Contact Person

Our Privacy Official is the contact person for questions, suggestions, or complaints relating to Further Restriction Requests or our compliance with the Privacy Rule relating to Further Restriction Requests.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PATIENT RIGHTS: FURTHER RESTRICTIONS PP2.5

General Policy

Policy

Our Practice's policy is to permit a patient to make a Further Restriction Request.

Our Practice is *not* required to agree to a Further Restriction Request. It is our policy generally not to agree to Further Restriction Requests. We will only agree to such requests when exceptional circumstances exist, when the Practice can reasonably accommodate the request, and when the Privacy Official (or an authorized physician) determines that we should agree to the request.

Our criteria for reviewing Further Restriction Requests are described in PP2.5, Review of Further Restriction Requests.

Further Restriction Request Defined

This policy applies to patients' requests that we agree to restrictions that go beyond the Privacy Rule's requirements for:

- Uses or disclosures of PHI for treatment, payment, or health care operations (these terms are defined in PP1.3 and PP1.4); and
- "Opt-out" disclosures of PHI to family and friends involved in the patient's care (PP1.6).

These requests are called Further Restriction Requests in these policies and procedures.

Agreed Restriction Defined

If we do agree to a Further Restriction Request, our agreement is called an Agreed Restriction in these policies and procedures.

If Practice Agrees, It Will Comply

If the Practice agrees to a Further Restriction Request, our policy is to comply with the Agreed Restriction except under the circumstances that follow.

Exceptions to Agreed Restriction

It is our policy to include the following statement of our policy in all of our patient forms documenting Agreed Restrictions.

Our policy is that an Agreed Restriction does not apply to any uses or disclosures of PHI:

- to the patient;
- for facility directories;
- for any "public purpose" disclosures (under Privacy Rule § 164.512) (defined in PP1.8);
- to treat the patient in an emergency.

Note

If the Practice discloses PHI that is subject to an Agreed Restriction to another health care provider for emergency treatment, the Practice must request that such other health care provider not further use or disclose the information beyond what is necessary for the provision of the emergency treatment.

Request to Comply with Another Law

The HIPAA Privacy Rule establishes "federal floor" preemption. This basically means that other federal laws and stricter state laws can still apply and impose privacy restrictions beyond what the Privacy Rule requires.

It is our Practice's policy that when we are presented with a request that we do what a stricter law requires, our policy is to deny the Further Restriction Request to the extent made under the Privacy Rule. At the same time, we will explain to the person making the request that it is our intention to comply with other stricter laws that apply, but that we do not believe it is necessary or appropriate to agree with the patient to do so in the context of a Further Restriction Request under HIPAA.

Terminating an Agreed Restriction

PP2.5 contains procedures for terminating an Agreed Restriction.

PATIENT RIGHTS: FURTHER RESTRICTIONS PP2.5

Index of Procedures

Introduction

Processing Further Restriction Requests involves a multi-step process.

Every employee should be able to perform Step 1, Respond to the Further Restriction Request, when such a request is presented to the employee.

The Privacy Official is responsible for Steps 2 through 6.

List of Procedures

Follow these steps in processing Further Restriction Requests:

Step	Action
1	Respond to the Further Restriction Request.
2	Privacy Official Intake.
3	Review Request.
4	Grant Request (if applicable).
5	Deny Request (if applicable).
6	Confirm Documentation.

Other Procedures

Use this additional procedure as needed to terminate an Agreed Restriction:

Action
(If Applicable) Terminating an Agreed Restriction

Step 1: Respond to the Further Restriction Request

Introduction

This procedure should be followed by any Practice employee to respond to a Further Restriction Request made to the employee. This applies to requests made by a patient and to requests made by a person stating that he or she is acting on behalf of a patient.

Step 1.1

Do Not Disclose PHI Without Verifying Identity and Authority

Caution: Do not disclose any PHI to the person requesting the Further Restriction without first following the Verification Policies and Procedures, PP1.12. This means that you may only disclose PHI if:

1. You know the identity and authority of the person to receive the PHI, or
2. You first follow steps in the Verification procedure.

Note

Keep in mind that, in some cases, disclosure of PHI may occur simply by confirming that a person is a patient of our Practice.

What to say: Follow these steps:

Step A If the identity and authority of the person making the request are known to you, respond to oral and written requests as described in Step 1.2 (oral) or Step 1.3 (written) below.

Step B If the identity or authority of the person is not known to you, either follow the Verification Policies and Procedures, or respond to the request without disclosing any PHI.

For example, you may say: "*You need to present your request to our Practice's Privacy Official. It is our Practice's policy that I cannot discuss whether a person is or is not a patient. I also cannot discuss any request that you make regarding further privacy restrictions.*"

Step 1.2

Oral Requests—What To Do

Depending on the circumstances, respond in one of the following two ways to Further Restriction Requests that are made orally. Use your best judgment to determine what is better under the circumstances:

Option A	Explain that although a Further Restriction Request is not required to be in writing, a written request will assist our Practice in providing a timely response. Provide the requesting patient with the Request to Restrict Uses and Disclosures of Protected Health Information (F2.5A) and explain that it should be completed, signed, and provided to the Privacy Official.
Option B	State that the Privacy Official is the contact person for making Further Restriction Requests and explain how to contact the Privacy Official.

Step 1.3

Oral Requests—Clinical Personnel

Patients may make informal requests to restrict the use and disclosure of PHI to Practice clinical personnel during the course of treatment.

Explain that the Practice's general policy is to deny such requests, then ask the patient if he or she would like to make the informal request a formal Further Restriction Request under the HIPAA Privacy Rule.

If the patient is making a formal request under the Privacy Rule, provide the patient with a Request to Restrict Uses and Disclosures of Protected Health Information (F2.5A) and ask the patient to complete, sign, and provide it to the Privacy Official.

Step 1.4

Written Requests—What To Do

If the request is made in writing, forward it promptly to the Privacy Official. Make sure you tell the Privacy Official the date the written request was received.

Step 1.5

Privacy Official Takes Over

The Privacy Official is responsible for the remaining steps in these procedures.
Proceed to Step 2.

Step 2: Privacy Official Intake of Further Restriction Requests

Introduction

This procedure should be followed by the Privacy Official in order to facilitate the review of and response to a Further Restriction Request.

Step 2.1

Follow the Procedures of Step 1

Follow the procedures of Step 1, Respond to the Further Restriction Request. If the patient refuses to provide a written request, document the oral request using Request to Restrict Uses and Disclosures of Protected Health Information (F2.5A).

Step 2.2

Document the Request

Step A	Record the request in the Further Restriction Request Log (F2.5B).
Step B	Place the written Further Restriction Request in the Patient HIPAA File.

Note

PP3.4, Documentation Policies and Procedures, describes the Patient HIPAA File.

Step 2.3

Initiate Review Process

Proceed to Step 3.

Step 3: Review of Further Restriction Request

Introduction

The Privacy Official should use this procedure to determine if a Further Restriction Request should be granted.

Step 3.1

Determine if Request is Eligible

Determine if the Further Restriction Request applies to one of the following:

1. A use or disclosure of PHI for treatment, payment, or health care operations (defined in PP1.3 and PP1.4); or
2. An "opt-out" disclosure to family and friends involved in the patient's care (defined in PP1.6).

If the request *does* apply to one of these uses and disclosures, **proceed to Step 3.2.**

If the request *does not* apply to one of these uses or disclosures, the Privacy Official, at his or her discretion, may deny the request and **proceed to Step 5.**

Step 3.2

Determine if Practice Should Agree to the Further Restriction Request

The Practice is not required to agree to a Further Restriction Request.

The HIPAA Privacy Rule and other privacy laws provide patients with very substantial privacy protections. These laws require medical practices to do and document a lot of things relating to patient privacy.

It is our policy generally not to agree to Further Restriction Requests. We will only agree to such requests when exceptional circumstances exist, when the Practice can reasonably accommodate the request, and when the Privacy Official (or an authorized physician) determines that we should agree to the request.

The Privacy Official may use his or her professional judgment to determine if the Practice should agree to a Further Restriction Request.

Step 3.3

Implement Decision to Agree to or Deny Request

If the Practice *agrees* to a Further Restriction Request, **proceed to Step 4.**
If the Practice *does not agree* to a Further Restriction Request, **proceed to Step 5.**

Step 4: (If Applicable) Grant the Further Restriction Request

Introduction

This procedure should be followed by the Privacy Official if the Practice agrees to a Further Restriction Request. This procedure applies after the decision has been made to grant all or part of a Further Restriction Request.

The Practice's agreement to a requested restriction is called an Agreed Restriction in these policies and procedures.

Step 4.1

Document Agreed Restriction

Document the Agreed Restriction using the Response to Request to Restrict Uses and Disclosures of PHI (F2.5C).

Step A Record the acceptance in the Further Restriction Request Log (F2.5B).

Step B Place a copy of the Response to Request to Restrict Uses and Disclosures of PHI (F2.5C) in the Patient HIPAA File.

Step C Add relevant information regarding the Agreed Restriction to the patient's records contained in the patient's chart and in Practice's computer system to alert others as appropriate, unless doing so would unduly risk a breach of the Agreed Restriction terms by permitting unauthorized persons to have access to sensitive information. If available, use an electronic "flag" to highlight the Agreed Restriction.

Instead of the above steps, physicians and other clinical personnel may document particularly sensitive information subject to Agreed Restrictions in a sealed file or envelope that may be stored in the Patient HIPAA File or in another secure and appropriate place

designated by the Privacy Official. An example of an Agreed Restriction and related information that may be stored in such a manner would be an agreed-to request that a physician not share certain sensitive information with any other Practice employee.

Step 4.2

Notify Patient of the Agreed Restriction

Inform the patient of the Agreed Restriction using the Response to Request to Restrict Uses and Disclosures of PHI (F2.5C). Use professional judgment to determine how to inform the patient.

Step 4.3

Communicate Agreed Restriction to Appropriate Staff

As appropriate, communicate the Agreed Restriction to persons in the Practice who need such information to ensure that the Practice complies with the Agreed Restriction.

This communication may be accomplished, in part, by attaching form F2.5C to the patient's chart and by updating the Practice's computer records and systems to highlight the Agreed Restriction.

Do not communicate with other persons in the Practice if the Agreed Restriction prohibits communications of specified information to others.

However, even in such cases, the Privacy Official must document the existence of the Agreed Restriction in the Practice's records per Steps 4.1.B and 4.1.C.

Step 4.4

Communicate Agreed Restriction to Business Associates as Appropriate

As appropriate, communicate the Agreed Restriction to Business Associates of the Practice who might otherwise use or disclose PHI in a manner inconsistent with the Agreed Restriction. The Privacy Rule does not appear to require this step, but the Privacy Official should pursue this step at the Privacy Official's discretion. This step should not be pursued if communicating to Business Associates would breach the Agreed Restriction.

Step 4.5

Confirm Documentation

Proceed to Step 6 to confirm that all required documentation is maintained.

Step 5: (If Applicable) Deny the Further Restriction Request

Introduction

This procedure should be followed by the Privacy Official to implement a denial of a Further Restriction Request. This procedure applies when the decision has been made to deny a Further Restriction Request.

Step 5.1

Document the Denial

Record the denial in the Further Restriction Request Log, as appropriate (F2.5B). The Privacy Rule does not require documentation of denials of Further Restriction Requests.

- But maintain such records as appropriate and consistent with professional judgment. Exercise care to protect information and avoid actions that would unduly risk exposing sensitive personal health information that is the subject of the request.

Step 5.2

Notify Patient of Denial

As appropriate, send a letter informing the patient of the Practice's denial of the Further Restriction Request, or orally convey the information and document as appropriate. The Privacy Rule does not require the Practice to provide a reason for its denial. It also does not provide the patient with a right to appeal a denial of a Further Restriction Request.

Use professional judgment in determining how to provide the letter (in person, by mail, etc.).

Maintain a copy of the denial letter or other documentation in the Patient HIPAA File, Further Restriction Request File, or other place as appropriate.

Step 5.3	**Proceed to Step 6** to confirm that all documentation is maintained.

Confirm Documentation

Step 6: Confirm Documentation

Introduction	The Privacy Official shall confirm that the Practice has created and maintains the following documentation relating to Further Restriction Requests. This documentation must be maintained by the Practice according to the requirements of PP3.4.
Document Agreement to a Further Restriction Request	Document and retain all Responses to Requests to Restrict Uses and Disclosures of PHI (F2.5C).
Other Documentation	Although not expressly required by the Privacy Rule, the Practice should document and retain as appropriate all Requests to Restrict Uses and Disclosures of PHI (F2.5A) (do so consistent with the guidance on documentation provided in Step 5.1).
Further Restriction Request Log	The Practice shall record and maintain the information required in the Further Restriction Request Log (F2.5B). The Privacy Official shall regularly review this Log for compliance with our policies and procedures.

PATIENT RIGHTS: FURTHER RESTRICTIONS PP2.5

(If Applicable) Terminating a Restriction

Introduction

The Privacy Official shall use this procedure to terminate an Agreed Restriction. This procedure applies after the Privacy Official has determined that it is in the best interests of the Practice to terminate an Agreed Restriction.

Step 1

Seek Patient's Agreement

As appropriate, the Privacy Official should seek to obtain the patient's agreement to terminate an Agreed Restriction (see Step 2). However, the Practice may also terminate an Agreed Restriction without a patient's agreement, as described below in Step 3.

Step 2

Patient Agrees to Terminate Restriction (in writing or orally)

Step A If the patient agrees to or requests a termination in writing, document the patient's agreement using the Termination of Agreed Restriction on Use or Disclosure of Protected Health Information (F2.5D). If this form is not used to document the patient's agreement, retain the written agreement provided by the patient.

Attach the completed form F2.5D or the other written agreement to the copy of the Response to Request to Restrict Uses and Disclosures of Protected Health Information (F2.5C) maintained in the Patient HIPAA File.

Step B If the patient **orally agrees** to terminate the restriction, *document this oral agreement* by completing the Termination of Agreed Restriction on Use or Disclosure of PHI (F2.5D).

Attach completed form F2.5D to the copy of the Response to Request to Restrict Uses and Disclosures of PHI (F2.5D) in the Patient HIPAA File.

Step C Record the termination of the Agreed Restriction in the Further Restriction Request Log (F2.5B).

Note

If a patient agrees to terminate a restriction (either orally or in writing), such termination is *effective for all PHI created or received by the Practice both before and after the patient agrees to terminate the restriction*.

Step 3

Practice Terminates Restriction Without Patient's Agreement

Inform the patient that the Practice is terminating the Agreed Restriction without the patient's agreement. Do this by letter or other means if appropriate under the circumstances.

Step A Complete the template termination letter (F2.5E) (or prepare other documentation of the communication if not by letter) and ensure it includes the date when the Practice agreed to the original restriction and the date the Practice will terminate the restriction.

Step B Place a copy of the termination letter in the Patient HIPAA File.

Step C Record the termination of the Agreed Restriction in the Further Restriction Request Log (F2.5B). Specify the effective date of the termination.

Note

Termination of an Agreed Restriction without the patient's agreement is *only effective with respect to information created or received after the Practice has informed the patient of the termination* of the restriction. The original restriction continues to apply to all information created or received by the Practice prior to the termination of this restriction.

F2.5A

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Request to Restrict Uses and Disclosures of Protected Health Information

Notice to the Patient: You may use this form to request that our Practice agree to additional restrictions on the uses and disclosures of protected health information about you. We call this a Further Restriction Request. You may make such a request regarding uses and disclosures for treatment, payment, or health care operations, and uses and disclosures to family and friends involved in your care or payment for your care. The HIPAA Privacy Rule permits you to make a request, but it does not require us to agree to your request. This is described in our Practice's Notice of Privacy Practices.

To assist our Practice in responding promptly and accurately to your Further Restriction Request, please complete this form in its entirety.

Patient Name: _____
[print or type]

Requested Restriction

Please describe in detail how you would like for our Practice to further restrict the use and disclosure of protected health information about you.

_____

_____

_____

_____

Reason for Further Restriction Request

Please specify the reason(s) for your Further Restriction Request.

_____

_____

_____

Contact Person

Please contact our Practice's Privacy Official, listed above, if you have any questions relating to your Further Restriction Request.

Patient Information

Print Name of Patient: _____ Signature of Patient: _____

Date: _____ Date of Birth (for identification purposes):_____

For Personal Representative of the Patient (if applicable)

Print Name of Personal Representative: _____

Describe Personal Representative Relationship: _____ (parent, guardian, power of attorney, etc.)

I hereby certify that I have the legal authority under applicable law to make this request on behalf of the patient identified above.

Signature of Personal Representative: _____ Date: _____

Name of Practice:

Last Updated:

Further Restriction Request Log

Patient Name	Chart/ID Number	Request Date	Response to Request; Date G=Grant D=Deny	Date Practice Notifies Staff/BAs About Agreed Restriction (if applicable)	Termination of Agreed Restriction (if applicable)

F2.5C

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Response to Request to Restrict Uses and Disclosures of Protected Health Information

Patient Name: _____

Address: _____

_____

Chart/ID Number: _____

Request Date: _____

Dear Patient:

You have made a request that our Practice agree to further restrictions on how it uses and discloses protected health information about you. This letter is our response to your request.

Your Request is:

_____ Denied, as explained below. (It is our Practice's policy generally to deny Further Restriction Requests. Even where we deny a Further Restriction Request, the requirements of the HIPAA Privacy Rule and other requirements continue to limit how our Practice may use or disclose protected health information about you.)
[check only if applicable]

_____ Granted, in whole or in part, as explained below.
[check only if applicable]

_____

_____

_____

Note that this paragraph applies only if we have granted a request by indicating so in the space above: If our Practice grants any part of your request for further restrictions on the use or disclosure of protected health information (PHI) about you, we grant it only to the extent specified in this Notice. Any grant of your request is called an Agreed Restriction in this Notice. Our Practice is not required to comply with any Agreed Restriction for uses or disclosures of PHI that are made: (1) to the patient; (2) for facility directories; (3) for any "public-good" disclosures that we may make under the HIPAA Privacy Rule (45 C.F.R. § 164.512); or to treat the patient in an emergency. Our Practice may terminate an Agreed Restriction with either your oral or written consent. Our Practice may also terminate this Agreed Restriction without your consent for all future uses and disclosures of PHI by providing you with written notice of such termination.

Contact Person

Please contact me if you have any questions relating to your Access Request.

Privacy Official: _____

Signature: _____

Date: _____

Telephone: _____

Address: _____

_____

F2.5D

Name of Practice:

Address:

Privacy Official:

Telephone:

Termination of Agreed Restriction on Use or Disclosures of Protected Health Information

I hereby consent to terminate the additional restrictions on the use and disclosure of protected health information that were previously agreed to by the Practice ("Agreed Restriction") and the date specified below. I understand that the requirements of the HIPAA Privacy Rule will continue to limit when protected health information about me may be used and disclosed by the Practice.

Date Practice Agreed to Original Restriction: _____

Patient Agreement to Terminate Restriction:

Print Name of Patient: _____

Signature of Patient: _____

Date: _____

Date of Birth (for identification purposes):_____

For Personal Representative of the Patient (if applicable):

Print Name of Personal Representative: _____

Describe Personal Representative Relationship: _____

(parent, guardian, power of attorney, etc.)

I hereby certify that I have the legal authority under applicable law to consent to this termination on behalf of the patient identified above.

Signature of Personal Representative: _____ Date: _____

F2.5E

Name of Practice:

Address:

Privacy Official:

Telephone:

[Letter Terminating Agreed Restriction without Consent]

[DATE]

[PATIENT ADDRESS]

Dear [PATIENT NAME]:

This letter is to provide you with notice that our Practice is hereby terminating the additional restriction on the use and disclosure of protected health information that we agreed to on [INSERT DATE]. This notice of termination will be effective with respect to all protected health information created or received by the Practice after _____ ("Effective Date").

The original restriction will continue to apply to all protected health information created or received by the Practice prior to the Effective Date of this termination. Following termination of the original restriction, the requirements of the HIPAA Privacy Rule will continue to limit how protected health information may be used and disclosed by the Practice.

Please feel free to contact me if you have any questions.

Sincerely,
[PRIVACY OFFICIAL]

PATIENT RIGHTS: COMPLAINTS PP2.6

General Policy

It is the Practice's policy to provide a process whereby individuals may make complaints concerning the Practice's privacy policies and procedures, compliance with those policies and procedures, and compliance with the requirements of the HIPAA Privacy Rule. The Practice acknowledges that documenting and responding to privacy complaints is an important aspect of monitoring the Practice's compliance efforts with respect to the privacy of health information.

Privacy Complaint Defined

A privacy complaint includes any complaint, whether presented in person, by telephone, in writing, or electronically, made by any individual (including a member of the Practice's workforce) regarding the Practice's privacy policies and procedures, the Practice's compliance with those policies and procedures, or compliance with the HIPAA Privacy Rule in general.

For example, privacy complaints may include the following:

- A complaint about the way an individual's PHI has been used or disclosed by the Practice or the Practice's Business Associates; or
- A complaint regarding denial of access to PHI (Refer to Access Requests Procedure (PP2.1) for more details on the procedure for handling requests for access to PHI.)

About Whom May Someone Complain?

A privacy complaint may be made about the Practice, the Practice's employees, volunteers and trainees working in the Practice, or a Business Associate of the Practice.

Initial Intake of Complaints

Any staff member who is presented with a privacy complaint by any person should refer the individual to the Privacy Official, or inform the Privacy Official of the complaint, as appropriate. Except in unusual circumstances, the Privacy Official is in a preferred position to respond to privacy complaints.

Documentation of Complaints

Upon referral of a privacy complaint to the Privacy Official, the Privacy Official shall follow the procedure below to document the complaint and its disposition, if any.

Step	
1	Discuss complaint with the complainant.

> **Note**
>
> A complainant is not required to complain first to the Practice before taking the complaint to the HHS. The Practice wants to encourage individuals to complain to the Practice first so that the complaints can be resolved.

2	Document the complaint on the Privacy Complaint Form (F2.6A).
3	If the individual making the complaint presents documentation in support of the complaint, attach all such documentation to the Privacy Complaint Form.
4	Inform the individual that he or she will receive a response from the Practice after the Practice has reviewed and investigated the complaint.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

Possible Actions By Privacy Official

The Privacy Official may wish to consult with legal counsel regarding a complaint. This might occur, for example, if the Privacy Official has legal questions he or she wishes to discuss in confidence and pursuant to the attorney-client privilege. The Privacy Official may also conclude at any point that the privacy complaint should be reviewed for the possibility that Internal Sanctions (PP3.6) and/or Mitigation (PP3.7) are appropriate.

Responding to Complaints

Use the following procedure to respond to all privacy complaints:

	Step
1	The Privacy Official will review each privacy complaint received.
2	The Privacy Official will develop a response to the complaint.
3	The Privacy Official will respond, in writing, to the complainant after the Practice has reviewed and investigated the complaint.

Retention of Complaint Documentation

All Privacy Complaint Forms and any other documentation related to a privacy complaint, the investigation, or the disposition of the complaint shall be kept in the Privacy Official's files for such length of time as is required under the policy and procedure for Documentation (PP3.4).

Communications that are subject to the attorney-client privilege shall be maintained as directed by legal counsel, including in separate files as appropriate.

Anti-retaliation Policy

Responses to privacy complaints are subject to the policy and procedure for "No Retaliation" (PP3.8).

PATIENT RIGHTS: COMPLAINTS PP2.6

Following are two sample letters that could be used to respond to complaints.

Sample Response Letter 1—Generic Response

This is an example of a generic letter that could be used to acknowledge those complaints that are made but that do not otherwise result in a finding by the Practice that any violation of HIPAA or the Practice's policies and procedures has occurred or where the Practice has decided not to take any further action.

Dear _____

Thank you for bringing to our attention your concerns regarding _____ . Maintaining the privacy of health information is very important to us, and we appreciate the information you have provided. We will review your concerns and will take any necessary steps as part of our ongoing privacy compliance and improvement program. Again, thank you for your time and concern. If you have further questions about this matter, please contact _____ at _____.

Sample Response Letter 2—Specific Response

This is an example of a letter that could be used to both acknowledge a complaint and explain any steps taken by the Practice in response to the complaint.

Dear _____

Thank you for bringing to our attention your concerns regarding _____ . Maintaining the privacy of health information is very important to us and we appreciate the information you have provided. We have reviewed your concerns and [will take/have taken] the following steps to address this issue:

Again, thank you for your time and concern. If you have further questions about this matter, please contact _____ at _____.

F2.6A

Practice Name: _____

Last Updated: _____

Privacy Complaint

For Internal Practice Use and Legal Counsel Use Only

_____ ___/___/___

Initials Date

Important Note: Initial and date here if this document is prepared in anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. (See Step 3.3 in PP2.1.)

Date: _____

Name of Complainant(s): _____

_____

Address: _____

_____

Phone: _____

Patient ID No. (if applicable):_____

Description of Complaint:

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

_____

Name of person completing this form: _____ Date: _____

PRIVACY MANAGEMENT: GENERAL POLICY PP3.0

Introduction

The Privacy Rule imposes Privacy Management requirements on our Practice. For more background basics on what the Privacy Rule requires regarding Privacy Management, read Appendix A, Lesson 4.

General Policy

Our policy is to comply with the Privacy Management requirements of the HIPAA Privacy Rule. The Practice's Privacy Management will be coordinated and monitored by the Practice's Privacy Official. The Privacy Official will periodically report to the Practice's governing body or board regarding the status of the Practice's Privacy Management.

Policies for Privacy Management

Following is the list of our policies for Privacy Management:

Policy/Procedure	Section
General Policy	PP3.0
Privacy Official/Privacy Contact	PP3.1
Notice of Privacy Practices—Development and Distribution	PP3.2
Policies and Procedures	PP3.3
Documentation	PP3.4
Workforce Training	PP3.5
Internal Sanctions	PP3.6
Mitigation	PP3.7
No Retaliation	PP3.8
No Waiver	PP3.9
Safeguards	PP3.10

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PRIVACY MANAGEMENT: PRIVACY OFFICIAL/PRIVACY CONTACT PP3.1

Introduction

The HIPAA Privacy Rule requires that we designate a Privacy Official who is responsible for developing and implementing the privacy policies and procedures of our Practice. We are also required to designate a contact person or office who is responsible for receiving complaints and who is able to provide further information about matters covered by the Practice's Notice of Privacy Practices.

Privacy Official Designation

The person identified below is the person designated to be our Practice's Privacy Official. The Privacy Official is the person responsible for developing and implementing the privacy policies and procedures of the Practice. The Privacy Official's job description is attached to this procedure as Form F3.1A.

Privacy Official Name: _____

Effective Date of Appointment: _____

Contact Person

Our Privacy Official is designated to be the contact person responsible for receiving complaints. The Privacy Official is also the person to contact for more information about matters covered by our Practice's Notice of Privacy Practices.

Privacy Official Delegation

The Privacy Official may delegate various tasks to properly trained persons, provided that the Privacy Official remains responsible for the functions and tasks assigned to the Privacy Official in these policies and procedures.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

F3.1A

Practice Name: _____

Last Updated: _____

Privacy Official Job Description

Title:	Privacy Official
General Duties:	Coordinate all activities of the Practice relating to maintaining the privacy of individually identifiable health information consistent with federal and state law. Report periodically to the Practice's management.
Specific Duties:	The Privacy Official has the following specific duties: ■ Work with the Practice's management and lawyer in achieving compliance with federal and state laws and regulations governing the privacy and security of individually identifiable health information. Stay abreast of developments in information privacy and security, including modifications to applicable laws and regulations, changes in any accreditation standards, and progress in privacy technology. Work cooperatively with outside organizations in any compliance investigation or review. ■ Chief responsibility (in coordination with the group's management and lawyer) for the creation of information privacy policies and procedures and the integration of such policies and procedures into the operations of the Practice. Oversee the Practice's efforts to maintain compliance with applicable laws and the Practice's policies and procedures. Coordinate consideration of sanctions where appropriate for individuals who fail to comply with privacy and security requirements. ■ Coordinate baseline and periodic assessments of information privacy and security risks and compliance and determine the degree to which the Practice's privacy initiatives are integrated with its other compliance efforts and administrative functions. Participate in the creation, execution, and oversight of all contracts with Business Associates and other contracts as appropriate to ensure that privacy issues are managed appropriately. ■ Cooperate with other Practice personnel in overseeing individuals' requests to the Practice, including requests for access to, amendment of, and accounting of disclosures of protected health information. Coordinate initial and ongoing privacy training for all physicians, staff, and other appropriate third parties. Serve as a privacy resource within the Practice, including addressing patient questions concerning the Practice's privacy initiatives. ■ Implement and manage effective methods to handle complaints regarding the Practice's standards and protocols, including documentation and investigation of such complaints. Ensure that such efforts are coordinated with other Practice personnel and the group's lawyer, if necessary. Educate Practice management about HIPAA's prohibitions of retaliatory actions against persons who assert privacy rights. Develop an effective process for communicating compliance concerns.
Qualifications:	Familiarity with clinical and administrative functions of the practice. Willingness to learn on a fast track about laws and regulations relating to privacy of health information. High integrity. Very detail-oriented. Strong organizational and communications abilities. Can work well with other Practice personnel.

PRIVACY MANAGEMENT: NOTICE OF PRIVACY PRACTICES—DEVELOPMENT AND DISTRIBUTION PP3.2

Overview

Introduction

This section contains our Practice's policies and procedures related to how our Practice provides notice of our privacy practices to patients and others. This notice is called a Notice of Privacy Practices or NPP.

Policies and Procedures

PP3.2 describes our Practice's policies and procedures relating to the NPP.

Every Practice employee should develop a basic understanding of our NPP. Many of our patients will take the time to study and learn more about our NPP and what it means to them. Your understanding the basics of our NPP will help our patients have greater confidence in our ability and commitment to protect their privacy.

Contact Person

Our Privacy Official is the designated contact person for questions, suggestions, or complaints relating to our NPP and our compliance with the Privacy Rule related to the NPP. Complaints made regarding the NPP should be received and documented in accordance with the policy and procedure for Complaints (PP2.6).

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PRIVACY MANAGEMENT: NOTICE OF PRIVACY PRACTICES—DEVELOPMENT AND DISTRIBUTION
PP3.2

General Policy

Policy

It is our Practice's policy to provide adequate notice of:

- The uses and disclosures of PHI that may be made by the Practice;
- An individual's rights with respect to PHI; and
- The Practice's legal duties with respect to PHI.

This notice shall be provided in an NPP that complies with these policies and procedures. It is also our policy that we will not use or disclose PHI in a manner inconsistent with the NPP (see PP1.18, Special Requirements: Consistent With Notice of Privacy Practices).

Required Content of NPP

The Privacy Official will coordinate and adopt the NPP that the Practice will use. Our NPP must contain certain information specified by the Privacy Rule regarding the uses and disclosures of PHI and the rights of an individual with respect to PHI, as governed by both HIPAA as well as more stringent state laws.

The NPP that will be used for our Practice is Form F3.2A, *after this form has been reviewed by legal counsel and modified to include required statements regarding stricter privacy protections under state and other laws, as applicable.*

Note

After consultation with legal counsel, the Privacy Official may choose to prepare a cover sheet for the NPP that summarizes briefly the NPP contents.

PRIVACY MANAGEMENT: NOTICE OF PRIVACY PRACTICES—DEVELOPMENT AND DISTRIBUTION PP3.2

List of Procedures

List of Procedures

Follow the procedures listed below in distributing, documenting, and revising the NPP.

Step	Action
1	Distributing the Notice of Privacy Practices.
2	Documenting the Patient's Receipt of the Notice of Privacy Practices.
3	Using a Joint Notice of Privacy Practices.
4	Revising the Notice of Privacy Practices.

Step 1: Distributing the Notice of Privacy Practices

What is the Difference Between a "Direct" and an "Indirect" Treatment Relationship?

The manner in which the NPP must be distributed depends, in part, on whether the Practice has a "direct" or "indirect" treatment relationship with an individual.

- An "indirect treatment relationship" is a relationship between an individual and a health care provider in which:
  - ☐ The health care provider delivers health care to the individual *based on the orders of another health care provider;* and
  - ☐ The health care provider *typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider,* who provides the services or products or reports to the individual.
- A "direct treatment relationship" is a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

When to Distribute the NPP

The NPP will be distributed to the following persons at the following times:

Make the NPP available to . . .	**When . . .**
persons with whom we have a direct treatment relationship	■ no later than the first time of service delivery after April 14, 2003; or ■ as soon as reasonably practicable after an emergency treatment situation.
persons with whom we have an indirect treatment relationship	upon request.
any person, whether a patient or not	upon request.
individuals who first receive health care service electronically	automatically and simultaneously in response to the individual's first request for service.
individuals who first receive health care service by phone	by mail on the day that service by phone was provided.

Other Required or Permitted Means of Providing the NPP

Use the following table to determine whether some other means of providing the NPP is required or permitted.

If . . .	Then . . .
the Practice has **a physical treatment site and a direct treatment relationship** with a patient	■ we will post our NPP in a prominent where it is reasonable to expect that the patients will be able to read it; and ■ the NPP will be made available for patients to take with them
the individual agrees to **electronic notice** and has not withdrawn such agreement	the Practice may provide the NPP by email (in compliance with Safeguard, PP3.10).

Note

If the Practice knows that the e-mail transmission has failed, the Practice must provide a paper copy of the NPP. Individuals who receive the NPP electronically still have the right to obtain a paper copy.

the Practice maintains a Web site that provides information about the Practice's services or benefits	the Practice will prominently post the NPP on the Web site and make it available electronically through the Web site.
a patient has some challenge, such as illiteracy, vision impairment, or a language barrier, that would restrict his or her ability to read our English language NPP	the Practice will consult with legal counsel regarding legal requirements and evaluate the feasibility and practicality of making the NPP available in some other format.

Step 2: Using a Joint Notice of Privacy Practices

Introduction

The Practice may agree to abide by a Joint Notice of Privacy Practices used by an Organized Health Care Arrangement (OHCA) in which the Practice participates. Where the Practice has agreed to abide by a Joint NPP, the Practice is not required to provide an NPP to a patient in the OHCA treatment setting where it has already been provided and documented by another covered entity participating in the OHCA.

What Is an Organized Health Care Arrangement?

The Privacy Rule defines five types of OHCAs. The two types of OHCAs that are most applicable to our Practice operations are:

(1) A clinically integrated care setting in which individuals typically receive health care from more than one health care provider (such as in hospitals); or

(2) An organized system of health care in which more than one covered entity participates (such as physician IPAs), and in which the participating covered entities:

- ■ Hold themselves out to the public as participating in a joint arrangement; and
- ■ Participate in joint activities that include at least one of the following:
  - □ Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
  - □ Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; *or*

- ☐ Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangement and if PHI created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.

Procedure for Using a Joint Notice of Privacy Practices

When a Joint NPP includes the Practice by agreement of the Practice, the Privacy Official will take the following actions:

Step A Review and approve any agreements to abide by a Joint NPP prior to the Practice making an agreement.

Step B Document the other covered entities or classes of covered entities participating in the OHCA.

Step C Document that one or more other covered entities are responsible for providing the NPP to patients of the Practice.

Step D Obtain adequate assurances that the Joint NPPs are in fact provided to patients through all OHCAs in which the Practice agrees to use a Joint NPP.

Step E Periodically audit or verify that the NPP is being appropriately provided and documented by other covered entities in the OHCA.

Step F Document the joint activities of the OHCA. (Note: This relates to the scope of the Permission to disclose PHI for the health care operations of OHCAs, PP1.5, and to whether a Business Associate Amendment is required for services relating to the joint activities of the OHCA, PP1.14.)

Step 3: Documenting the Patient's Receipt of the Notice of Privacy Practices

NPP Receipt Procedure

Where the Practice has a direct treatment relationship with a patient, we will ask the patient to sign a document acknowledging the patient's receipt of our NPP. Use the following procedure to provide the NPP to the patient:

Step A Provide the patient with a copy of the NPP.

Step B Ask patient to read and sign the NPP Receipt Form (F3.2B).

Step C Retain the signed NPP Receipt Form in the Patient HIPAA File (see Documentation, PP3.4).

Step D In the NPP Provision Log (F3.2C), enter the patient's name and ID/chart number, the date NPP provided, the version of the NPP provided, and whether patient signed NPP Receipt Form or refused to sign.

When Signed NPP Receipt Form Is Not Obtained

Use the following table to determine how to handle circumstances where a signed NPP Receipt Form is not obtained.

If . . .	**Then . . .**
the patient refuses to sign the NPP Receipt Form	document that patient has refused and the reason for the refusal, if known, at the bottom of the NPP Receipt Form in the space marked "For Practice Use Only."
it is not possible to obtain a signature on the NPP form due to an emergency treatment situation	document the nature of the emergency on the NPP Receipt Form and obtain a signature as soon as reasonably practicable.
the NPP was provided by e-mail	follow the procedure for acknowledgement of NPPs provided by e-mail outlined below.

the NPP was provided by mail on the day that service was provided by telephone	send a copy of the NPP Receipt Form by mail along with the NPP requesting that the individual return it to the Practice.
a Joint NPP has already been provided by another covered entity in an OHCA in which the Practice participates and the Practice has agreed to abide by that Joint NPP	do not request that the patient sign the NPP Receipt Form because the Practice's obligation to provide an NPP is satisfied.

Note

Consult with legal counsel regarding whether the Practice should provide its own NPP if the patient is receiving care from the Practice that is not related to the OHCA or if the Practice's own Notice of Privacy Practices is different from the Joint Notice of Privacy Practices for the OHCA.

Patient Acknowledgment of NPP by E-mail

Follow the procedure below to obtain an acknowledgment of an NPP provided by e-mail (also comply with Safeguards, PP3.10, Technical Security, Section 3):

Step A Ask the patient to return by e-mail an acknowledgment that the NPP was received.

Step B If such electronic acknowledgment is not received within 2 business days of the provision of the NPP by e-mail, mail a paper copy of the NPP and the NPP Receipt Form to the individual's address.

Retention of NPP Documentation

The following documents should be retained to document the provision of the NPP:

Retain . . .	**For . . .**
all versions of the NPP	6 years after the expiration date of each NPP version.
NPP Receipt Forms	6 years after the date of last delivery of services to the patient.
NPP Receipt Logs	indefinitely.

Documentation regarding the NPP should also be maintained in compliance with the policy and procedure for Documentation (PP3.4).

Step 4: Revising the Notice of Privacy Practices

Revisions to the NPP

The NPP must be revised whenever a material change occurs in any of the following:

- The uses or disclosures of PHI made by the Practice;
- An individual's rights with respect to PHI;
- The Practice's legal duties with respect to PHI; or
- Other privacy practices stated in the NPP.

A material change to any term of the NPP may not be implemented prior to the effective date of the NPP in which such a material change is reflected. For the specific procedure for revision of the Practice's policies and procedures that are stated in the NPP, see Policies and Procedures (PP3.3).

Distribution of Revised NPP

Use the following table to determine how a revised NPP must be distributed.

If the older version of the NPP was . . .	Then the new version of the NPP should . . .
distributed to patients with either a direct or indirect treatment relationship	be made available upon request.
posted on the Practice's web site	replace the older version on the Web site.
posted in a prominent location at a physical treatment site	replace the older version that was posted.
made available for patients to take with them at a physical treatment site	be made available for patients to take with them.

F3.2A

Note: This document is designed as a general outline for discussion purposes and is not intended as legal advice. This document does not address requirements under other federal or state laws that may need to be described in a Notice of Privacy Practices.

[INSERT NAME OF PRACTICE]

Notice of Privacy Practices

THIS NOTICE DESCRIBES HOW MEDICAL INFORMATION ABOUT YOU MAY BE USED AND DISCLOSED AND HOW YOU CAN GET ACCESS TO THIS INFORMATION. PLEASE REVIEW IT CAREFULLY.

Original Effective Date: April 14, 2003

Last Revised: _____

A federal regulation, known as the HIPAA Privacy Rule, requires that we provide detailed notice in writing of our privacy practices. We know that this Notice is long. The HIPAA Privacy Rule requires us to address many specific things in this Notice.

I. OUR COMMITMENT TO PROTECTING HEALTH INFORMATION ABOUT YOU

In this Notice, we describe the ways that we may use and disclose health information about our patients. The HIPAA Privacy Rule requires that we protect the privacy of health information that identifies a patient, or where there is a reasonable basis to believe the information can be used to identify a patient. This information is called protected health information or PHI. This Notice describes your rights as our patient and our obligations regarding the use and disclosure of PHI. We are required by law to:

- Maintain the privacy of PHI about you;
- Give you this Notice of our legal duties and privacy practices with respect to PHI; and
- Comply with the terms of our Notice of Privacy Practices that is currently in effect.

As permitted by the HIPAA Privacy Rule, we reserve the right to make changes to this Notice and to make such changes effective for all PHI we may already have about you. If and when this Notice is changed, we will post a copy in our office in a prominent location. We will also provide you with a copy of the revised Notice upon your request made to our Privacy Official.

You will be asked to sign a form to show that you received this Notice. Even if you do not sign this form, we will still provide you with treatment.

II. HOW WE MAY USE AND DISCLOSE PROTECTED HEALTH INFORMATION ABOUT YOU

[CAUTION: You should consult with legal counsel to make sure this section includes required descriptions of any additional prohibitions or limitations on the described uses and disclosures under other federal laws or state laws.]

USES AND DISCLOSURES FOR TREATMENT, PAYMENT, AND HEALTH CARE OPERATIONS

The following categories describe the different ways we may use and disclose PHI for treatment, payment, or health care operations without your consent or authorization. The examples included in each category do not list every type of use or disclosure that may fall within that category.

Treatment: We may use and disclose PHI about you to provide, coordinate, or manage your health care and related services. We may consult with other health care providers regarding your treatment and coordinate and manage your health care with others. For example, we may use and disclose PHI when you need a prescription, lab work, an X-ray, or other health care services. In addition, we may use and disclose PHI about you when referring you to another health care provider. For example, if you are referred to another physician, we may disclose PHI to your new physician regarding whether you are allergic to any medications. In emergencies, we may use and disclose PHI to provide the treatment you need.

We may also disclose PHI about you for the treatment activities of another health care provider. For example, we may send a report about you to a physician that we refer you to so that the other physician may treat you.

Payment: We may use and disclose PHI so that we can bill and collect payment for the treatment and services provided to you. Before providing treatment or services, we may share details with your health plan concerning the services you are scheduled to receive. For example, we may ask for payment approval from your health plan before we provide care or services. We may use and disclose PHI to find out if your health plan will cover the cost of care and services we provide. We may use and disclose PHI to confirm you are receiving the appropriate amount of care to obtain payment for services. We may use and disclose PHI for billing, claims management, and collection activities. We may disclose PHI to insurance companies providing you with additional coverage. We may disclose limited PHI to consumer reporting agencies relating to collection of payments owed to us.

We may also disclose PHI to another health care provider or to a company or health plan required to comply with the HIPAA Privacy Rule for the payment activities of that health care provider, company, or health plan. For example, we may allow a health insurance company to review PHI for the insurance company's activities to determine the insurance benefits to be paid for your care.

Health Care Operations: We may use and disclose PHI in performing business activities that are called health care operations. Health care operations include doing things that allow us to improve the quality of care we provide and to reduce health care costs. We may use and disclose PHI about you in the following health care operations:

- Reviewing and improving the quality, efficiency, and cost of care that we provide to our patients. For example, we may use PHI about you to develop ways to assist our physicians and staff in deciding how we can improve the medical treatment we provide to others.
- Improving health care and lowering costs for groups of people who have similar health problems and helping to manage and coordinate the care for these groups of people. We may use PHI to identify groups of people with similar health problems to give them information, for instance, about treatment alternatives and educational classes.
- Reviewing and evaluating the skills, qualifications, and performance of health care providers taking care of you and our other patients.
- Providing training programs for students, trainees, health care providers, or non-health care professionals (for example, billing personnel) to help them practice or improve their skills.
- Cooperating with outside organizations that assess the quality of the care that we provide.
- Cooperating with outside organizations that evaluate, certify, or license health care providers or staff in a particular field or specialty. For example, we may use or disclose PHI so that one of our nurses may become certified as having expertise in a specific field of nursing.
- Cooperating with various people who review our activities. For example, PHI may be seen by doctors reviewing the services provided to you, and by accountants, lawyers, and others who assist us in complying with the law and managing our business.
- Assisting us in making plans for our practice's future operations.
- Resolving grievances within our practice.
- Reviewing our activities and using or disclosing PHI in the event that we sell our practice to someone else or combine with another practice.
- Business planning and development, such as cost-management analyses.
- Business management and general administrative activities of our practice, including managing our activities related to complying with the HIPAA Privacy Rule and other legal requirements.
- Creating "de-identified" information that is not identifiable to any individual, and disclosing PHI to a business associate for the purpose of creating de-identified information, regardless of whether we will use the de-identified information.
- Creating a "limited data set" of information that does not contain information directly identifying a patient. Our ability to disclose this information to others under limited conditions is discussed later in this Notice.

If another health care provider, company, or health plan that is required to comply with the HIPAA Privacy Rule also has or once had a relationship with you, we may disclose PHI about you for certain health care operations of that health care provider or company. For example, such health care operations may include: reviewing and improving the quality, efficiency, and cost of care provided to you; reviewing and evaluating the skills, qualifications, and performance of health care providers; providing

training programs for students, trainees, health care providers, or non-health care professionals; cooperating with outside organizations that evaluate, certify, or license health care providers or staff in a particular field or specialty; and assisting with legal compliance activities of that health care provider or company.

We may also disclose PHI for the health care operations of any "organized health care arrangement" in which we participate. An example of an organized health care arrangement is the joint care provided by a hospital and the physicians who see patients at the hospital.

Communication From Our Office: We may contact you to remind you of appointments and to provide you with information about treatment alternatives or other health-related benefits and services that may be of interest to you.

OTHER USES AND DISCLOSURES WE CAN MAKE WITHOUT YOUR WRITTEN AUTHORIZATION FOR WHICH YOU HAVE THE OPPORTUNITY TO AGREE OR OBJECT

Individuals Involved in Your Care or Payment for Your Care: We may use and disclose PHI about you in some situations where you have the opportunity to agree or object to certain uses and disclosures of PHI about you. If you do not object, we may make these types of uses and disclosures of PHI.

- We may disclose PHI about you to your family member, close friend, or any other person identified by you if that information is directly relevant to the person's involvement in your care or payment for your care.
- If you are present and able to consent or object (or if you are available in advance), then we may only use or disclose PHI if you do not object after you have been informed of your opportunity to object.
- If you are not present or you are unable to consent or object, we may exercise professional judgment in determining whether the use or disclosure of PHI is in your best interests. For example, if you are brought into this office and are unable to communicate normally with your physician for some reason, we may find it is in your best interest to give your prescription and other medical supplies to the friend or relative who brought you in for treatment.
- We may also use and disclose PHI to notify such persons of your location, general condition, or death. We also may coordinate with disaster relief agencies to make this type of notification.
- We may also use professional judgment and our experience with common practice to make reasonable decisions about your best interests in allowing a person to act on your behalf to pick up filled prescriptions, medical supplies, X-rays, or other things that contain PHI about you.

OTHER USES AND DISCLOSURES WE CAN MAKE WITHOUT YOUR WRITTEN AUTHORIZATION OR OPPORTUNITY TO AGREE OR OBJECT

We may use and disclose PHI about you in the following circumstances without your authorization or opportunity to agree or object, provided that we comply with certain conditions that may apply.

Required By Law: We may use and disclose PHI as required by federal, state, or local law to the extent that the use or disclosure complies with the law and is limited to the requirements of the law.

Public Health Activities: We may use and disclose PHI to public health authorities or other authorized persons to carry out certain activities related to public health, including the following activities:

- To prevent or control disease, injury, or disability;
- To report disease, injury, birth, or death;
- To report child abuse or neglect;
- To report reactions to medications or problems with products or devices regulated by the federal Food and Drug Administration (FDA) or other activities related to qualify, safety, or effectiveness of FDA-regulated products or activities;
- To locate and notify persons of recalls of products they may be using;
- To notify a person who may have been exposed to a communicable disease in order to control who may be at risk of contracting or spreading the disease; or
- To report to your employer, under limited circumstances, information related primarily to workplace injuries or illnesses, or workplace medical surveillance.

[NOTE: Consult with legal counsel to determine additional disclosures that may be made for public health purposes under state laws that survive HIPAA preemption and incorporate these additions into the above list.]

Abuse, Neglect, or Domestic Violence: We may disclose PHI in certain cases to proper government authorities if we reasonably believe that a patient has been a victim of domestic violence, abuse, or neglect.

Health Oversight Activities: We may disclose PHI to a health oversight agency for oversight activities including, for example, audits, investigations, inspections, licensure and disciplinary activities, and other activities conducted by health oversight agencies to monitor the health care system, government health care programs, and compliance with certain laws.

Lawsuits and Other Legal Proceedings: We may use or disclose PHI when required by a court or administrative tribunal order. We may also disclose PHI in response to subpoenas, discovery requests, or other required legal process when efforts have been made to advise you of the request or to obtain an order protecting the information requested.

Law Enforcement: Under certain conditions, we may disclose PHI to law enforcement officials for the following purposes where the disclosure is:

- About a suspected crime victim if, under certain limited circumstances, we are unable to obtain a person's agreement because of incapacity or emergency;
- To alert law enforcement of a death that we suspect was the result of criminal conduct;
- Required by law;
- In response to a court order, warrant, subpoena, summons, administrative agency request, or other authorized process;
- To identify or locate a suspect, fugitive, material witness, or missing person;
- About a crime or suspected crime committed at our office; or
- In response to a medical emergency not occurring at the office, if necessary to report a crime, including the nature of the crime, the location of the crime or the victim, and the identity of the person who committed the crime.

Coroners, Medical Examiners, Funeral Directors: We may disclose PHI to a coroner or medical examiner to identify a deceased person and determine the cause of death. In addition, we may disclose PHI to funeral directors, as authorized by law, so that they may carry out their jobs.

Organ and Tissue Donation: If you are an organ donor, we may use or disclose PHI to organizations that help procure, locate, and transplant organs in order to facilitate an organ, eye, or tissue donation and transplantation.

Research: We may use and disclose PHI about you for research purposes under certain limited circumstances. We must obtain a written authorization to use and disclose PHI about you for research purposes, except in situations where a research project meets specific, detailed criteria established by the HIPAA Privacy Rule to ensure the privacy of PHI.

To Avert a Serious Threat to Health or Safety: We may use and disclose PHI about you in limited circumstances when necessary to prevent a threat to the health or safety of a person or to the public. This disclosure can only be made to a person who is able to help prevent the threat.

Specialized Government Functions: Under certain conditions, we may disclose PHI:

- For certain military and veteran activities, including determination of eligibility for veterans benefits and where deemed necessary by military command authorities;
- For national security and intelligence activities;
- To help provide protective services for the President of the United States and others;
- For the health or safety of inmates and others at correctional institutions or other law enforcement custodial situations or for general safety and health related to correctional facilities.

Workers' Compensation: We may disclose PHI as authorized by workers' compensation laws or other similar programs that provide benefits for work-related injuries or illness.

[Note: The above list of uses and disclosures that can be made without authorization or opportunity to agree or object should be edited to address any uses or disclosures that are not permitted under more stringent state laws that survive preemption.]

Disclosures Required by HIPAA Privacy Rule: We are required to disclose PHI to the Secretary of the United States Department of Health and Human Services when requested by the Secretary to review our compliance with the HIPAA Privacy Rule. We are also required in certain cases to disclose PHI to you upon your request to access PHI or for an accounting of certain disclosures of PHI about you (these requests are described in Section III of this Notice).

Incidental Disclosures: We may use or disclose PHI incident to a use or disclosure permitted by the HIPAA Privacy Rule so long as we have reasonably safeguarded against such incidental uses and disclosures and have limited them to the minimum necessary information.

Limited Data Set Disclosures: We may use or disclose a limited data set (PHI that has certain identifying information removed) for the purposes of research, public health, or health care operations. This information may only be disclosed for research, public health, and health care operations purposes. The person receiving the information must sign an agreement to protect the information.

OTHER USES AND DISCLOSURES OF PROTECTED HEALTH INFORMATION REQUIRE YOUR AUTHORIZATION

All other uses and disclosures of PHI about you will only be made with your written authorization. If you have authorized us to use or disclose PHI about you, you may later revoke your authorization at any time, except to the extent we have taken action based on the authorization.

III. YOUR RIGHTS REGARDING PROTECTED HEALTH INFORMATION ABOUT YOU

Under federal law, you have the following rights regarding PHI about you:

Right to Request Restrictions: You have the right to request additional restrictions on the PHI that we may use or disclose for treatment, payment, and health care operations. You may also request additional restrictions on our disclosure of PHI to certain individuals involved in your care that otherwise are permitted by the Privacy Rule. *We are not required to agree to your request.* If we do agree to your request, we are required to comply with our agreement except in certain cases, including where the information is needed to treat you in the case of an emergency. To request restrictions, you must make your request in writing to our Privacy Official. In your request, please include (1) the information that you want to restrict; (2) how you want to restrict the information (for example, restricting use to this office, only restricting disclosure to persons outside this office, or restricting both); and (3) to whom you want those restrictions to apply.

Right to Receive Confidential Communications: You have the right to request that you receive communications regarding PHI in a certain manner or at a certain location. For example, you may request that we contact you at home, rather than at work. You must make your request in writing. You must specify how you would like to be contacted (for example, by regular mail to your post office box and not your home). We are required to accommodate only *reasonable* requests.

Right to Inspect and Copy: You have the right to request the opportunity to inspect and receive a copy of PHI about you in certain records that we maintain. This includes your medical and billing records but does not include psychotherapy notes or information gathered or prepared for a civil, criminal, or administrative proceeding. We may deny your request to inspect and copy PHI only in limited circumstances. To inspect and copy PHI, please contact our Privacy Official. If you request a copy of PHI about you, we may charge you a reasonable fee for the copying, postage, labor, and supplies used in meeting your request.

Right to Amend: You have the right to request that we amend PHI about you as long as such information is kept by or for our office. To make this type of request, you must submit your request in writing to our Privacy Official. You must also give us a reason for your request. We may deny your request in certain cases, including if it is not in writing or if you do not give us a reason for the request.

Right to Receive an Accounting of Disclosures: You have the right to request an "accounting" of certain disclosures that we have made of PHI about you. This is a list of disclosures made by us during a specified period of up to 6 years, *other than* disclosures made: for treatment, payment, and health care operations; for use in or related to a facility directory; to family members or friends involved in your care; to you directly; pursuant to an authorization of you or your personal representative; for certain notification purposes (including national security, intelligence, correctional, and law enforcement purposes); as incidental disclosures that occur as a result of otherwise permitted disclosures; as part of a limited data set of information that does not directly identify you; and before April 14, 2003. If you wish to make such a request, please contact our Privacy Official identified on the last page of this Notice. The first list that you request in a 12-month period will be free, but we may charge you for our reasonable costs of providing additional lists in the same 12-month period. We will tell you about these costs, and you may choose to cancel your request at any time before costs are incurred.

Right to a Paper Copy of this Notice: You have a right to receive a paper copy of this Notice at any time. You are entitled to a paper copy of this Notice even if you have previously agreed to receive this Notice electronically. To obtain a paper copy of this Notice, please contact our Privacy Official listed in this Notice.

IV. COMPLAINTS

If you believe your privacy rights have been violated, you may file a complaint with us or the Secretary of the United States Department of Health and Human Services. To file a complaint with our office, please contact our Privacy Official at the address and number listed below. We will not retaliate or take action against you for filing a complaint.

V. QUESTIONS

If you have any questions about this Notice, please contact our Privacy Official at the address and telephone number listed below.

VI. PRIVACY OFFICIAL CONTACT INFORMATION

You may contact our Privacy Official at the following address and phone number:

Privacy Official
[address]
[telephone number]

This notice was published and first became effective on _____ [INSERT A DATE WHICH IS NO LATER THAN APRIL 14, 2003].

[*Note:* Portions of this document are from a working draft document prepared by a task force of the North Carolina Healthcare Information and Communications Alliance, Inc., and are used with NCHICA's permission (www.nchica.org).]

F3.2B

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Notice of Privacy Practices Receipt

I acknowledge that I was provided with the Notice of Privacy Practices of the Medical Practice named at the top of this page.

Print Name of Patient: _____

Signature of Patient: _____

Date: _____

Patient's Date of Birth: _____

Patient's ID/Chart Number: _____

For Personal Representative of the Patient (if applicable)

Print Name of Personal Representative: _____

Describe Personal Representative Relationship: _____

(parent, guardian, etc.)

Signature of Personal Representative: _____

Date: _____

For Practice Use Only:

_____

_____

_____

_____

_____

_____ _____

Signature of Practice Employee Date

F3.2C

Name of Practice:

Last Updated:

Notice of Privacy Practices Provision Log

Patient's Name	Patient ID/ Chart No.	Date NPP Provided	Version of NPP Provided (Date)	NPP Receipt Acknowledgment: S: Patient signature on file R: Patient refused to sign

Page ___ of ___

PRIVACY MANAGEMENT: POLICIES AND PROCEDURES PP3.3

General Policy

Policies and Procedures	It is our policy to implement policies and procedures with respect to PHI that are reasonably designed to ensure compliance with the standards, implementation specifications, or other requirements of the HIPAA Privacy Rule. These policies and procedures shall also be consistent with applicable state law and other laws that are not preempted by HIPAA.
Documentation of Policies and Procedures	All policies and procedures will be documented in either written or electronic format. Documentation of policies and procedures will be in compliance with the policy and procedure for Documentation (PP3.4).
Effective Dates of Policies and Procedures	Each policy and procedure will display the effective date of the document. A list of and copies of the most current versions of all policies and procedures will be maintained by the Privacy Official for reference by Practice employees. The Privacy Official will use the Checklist of Phase II Policies and Procedures (F3.3A) to track the dates each policy and procedure is adopted and modified.
Revisions to Policies and Procedures	Changes to the Practice's policies and procedures will be made when necessary and appropriate to comply with changes in the law, including the standards, requirements, and implementation specifications of the HIPAA Privacy Rule. When such changes in the law occur, the Practice will promptly revise and implement the affected policy or procedure using the Policy/Procedure Modification Form (F3.3B).
Revisions to the Notice of Privacy Practices	When revisions to the Practice's policies and procedures affect a practice stated in the Notice of Privacy Practices, F3.2A, the NPP must be revised accordingly. Revisions to the NPP will be made in accordance with Notice of Privacy Practices—Development and Distribution (PP3.2). The effective date of a revised policy and procedure may not be prior to the effective date of the revised NPP.
Training for Revisions to Policies and Procedures	Training of Practice employees on the revisions, if necessary, will be conducted in accordance with the policy and procedure for Workforce Training (PP3.5).
Privacy Official Responsibilities	The Practice's Privacy Official is the designated person for maintenance and revision of all policies and procedures.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

F3.3A

Name of Practice:

Address:

Privacy Official:

Telephone:

Last Updated: _____

Checklist of Phase II Policies and Procedures

Number	Title	Date Adopted	Date(s) Modified	Privacy Official Notes
	PHI Permissions			
PP1.0	General Policy			
Permissions				
PP1.1	Required Disclosures			
PP1.2	Disclosures to the Patient			
PP1.3	Our Treatment, Payment, Operations			
PP1.4	Others' Treatment, Payment, Operations			
PP1.5	Operations of Organized Health Care Arrangement			
PP1.6	Family, Friends, and Disaster Relief Organizations			
PP1.7	Incidental Disclosures			
PP1.8	Public Purpose			
PP1.9	Authorization			
PP1.10	De-Identification			
PP1.11	Limited Data Set			
Special Requirements				
PP1.12	Verification			
PP1.13	Minimum Necessary			
PP1.14	Business Associates			
PP1.15	Personal Representatives			
PP1.16	Marketing			
PP1.17	Psychotherapy Notes			
PP1.18	Consistent with Notice of Privacy Practices			
PP1.19	Consistent with Other Documents			
PP1.20	Consent			

	Patient Rights
PP2.0	General Policy
PP2.1	Access
PP2.2	Amendment
PP2.3	Accounting
PP2.4	Alternative Communications
PP2.5	Further Restrictions
PP2.6	Complaints
	Privacy Management
PP3.0	General Policy
PP3.1	Privacy Official/Privacy Contact
PP3.2	Notice of Privacy Practices—Development and Distribution
PP3.3	Policies and Procedures
PP3.4	Documentation
PP3.5	Workforce Training
PP3.6	Internal Sanctions
PP3.7	Mitigation
PP3.8	No Retaliation
PP3.9	No Waiver
PP3.10	Safeguards

F3.3B

Name of Practice: _____

Address: _____

Privacy Official: _____

Telephone: _____

Policy/Procedure Modification Form

Policy/Procedure Modified: _____

Reason for Modification: ☐ State law or other legal requirements
☐ Other _____

Effective Date of Modification: _____

Describe Modification:

Modification Approved By: _____ Date: _____

PRIVACY MANAGEMENT: DOCUMENTATION PP3.4

Introduction

The HIPAA Privacy Rule contains specific requirements for maintaining documentation related to our Practice's compliance with the HIPAA Privacy Rule. Our policies for complying with these requirements are described below.

General Policies

1. It is our policy to comply with the documentation requirements contained in the HIPAA Privacy Rule.
2. Where the Privacy Rule requires a communication to be in writing, our Practice must maintain a written or electronic copy as documentation.
3. If an action, activity, or designation is required by the Privacy Rule to be documented, our Practice must maintain a written or electronic record of that action, activity, or designation.
4. Our Practice must maintain the policies and procedures required under the Privacy Rule in written or electronic form.
5. Our Practice will maintain the required documentation for 6 years from the later of the date the record was created or the date when the record was last in effect.

Patient HIPAA File

HIPAA documentation that relates to a particular patient will be kept in a separate Patient HIPAA File for that patient unless otherwise specified in the Practice's policies and procedures or as otherwise determined by the Privacy Official. (Note to Privacy Official: For example, the Patient HIPAA File may be maintained in a two-hole punched file folder that is the patient chart, with the HIPAA documents filed on the left side of the folder at the back, separated by a divider.)

In our Practice, the Patient HIPAA File will be maintained as follows:

_____

_____

_____

_____

_____

_____

_____

Policy: HHS Requests to See Records

We will keep records and submit compliance reports, in such time and manner containing such information, as the Secretary of the United States Department of Health and Human Services (HHS) may determine to be necessary to enable HHS to determine whether we have complied or are complying with the Privacy Rule.

We will permit access by HHS during normal business hours to our facilities, books, records, accounts, and other sources of information that are pertinent to the Secretary's determining compliance with the Privacy Rule. If the Secretary determines that exigent circumstances exist, such as when documents may be hidden or destroyed, we must permit access by the Secretary at any time and without notice.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

Nothing within these policies relating to HHS will prohibit our Practice from asserting before a court of competent jurisdiction any rights that we may have, including Constitutional rights, with respect to the Secretary's request for access to and right of access to our records.

Discuss Attorney-Client Privilege With Legal Counsel

The Privacy Official should discuss any attorney-client privilege issues related to HIPAA documentation with the Practice's legal counsel.

PRIVACY MANAGEMENT: WORKFORCE TRAINING PP3.5

General Policy

It is the Practice's policy to train all members of the Practice's workforce on the Practice's policies and procedures with respect to PHI as necessary and appropriate for the members of the workforce to carry out their functions within the Practice.

Definition of Workforce

Workforce members include employees, volunteers, trainees, and other persons whose conduct, in the performance of work for the Practice, is under the direct control of the Practice, whether or not they are paid by the Practice.

The Privacy Official will use the Workforce Log (F3.5A) to document those individuals who are included in the Practice's workforce.

Sometimes, members of the Practice's workforce may provide services on their own behalf and not on behalf of the Practice. For example, if a nurse employed by the Practice volunteers to provide nursing services at a local school, the nurse, in providing those services, may not be acting as a member of the Practice's workforce. The Privacy Official will use the Workforce Exclusions Log (F3.5B) to document the circumstances (if any) where an employee provides health care services but is not acting as a member of the Practice's workforce.

Privacy Official's Responsibility for Training

The Privacy Official will develop, coordinate, and participate in initial and continuing training to ensure that all personnel are properly trained on the Practice's privacy policies and procedures. The Privacy Official will determine who needs training, the type of training that is appropriate, and the frequency with which training will occur. The Privacy Official will document the training required for each person on the Personal HIPAA Training Profile (F3.5C).

Training Schedule

Training will occur according to the following schedule:

Training for . . .	**Will occur . . .**
current employees as of April 14, 2003	by April 14, 2003 (HIPAA compliance deadline).
new employees	within a reasonable time following employee's start date.
employees whose functions are affected by a material change to any policy or procedure	within a reasonable period of time following the effective date of the material change.

Documentation of Training

Use the following forms to document training:

Use . . .	**To . . .**
Personal HIPAA Training Profile and Training Record (F3.5C)	document each instance of training for individual employees.
Training Session Documentation Form (F3.5D)	"sign in" documentation of attendance of employees at a training session.

Documentation of training should be created and retained in compliance with the policy and procedure for Documentation (PP3.4).

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

Confidentiality Agreement

Upon the completion of training on the Practice's privacy policies and procedures, each employee will sign the Confidentiality Agreement (F3.5E).

> **Note**
>
> Consult with legal counsel to determine under applicable state law if additional monetary or other consideration is required or if continued employment is sufficient consideration to support "contract consideration" for this Confidentiality Agreement.

Personal HIPAA Training Profile

The Privacy Official will complete the Personal HIPAA Training Profile (F3.5C) for each workforce member. Using this form, the Privacy Official will assign policies and procedures, or parts of policies and procedures, to each employee. Each employee must read each policy and procedure assigned to the employee.

F3.5A

Name of Practice:

Address:

Privacy Official:

Telephone:

Workforce Log

The following persons are employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of the Practice.

Name	Job Title

Page ___ of ___

F3.5B

Name of Practice:

Address:

Privacy Official:

Telephone:

Workforce Exclusions Log

Describe below the circumstances in which a member of the Practice's workforce provides services on his or her own behalf (or someone else's behalf) and not on behalf of the Practice.

Name	Description of Services Not Provided on Behalf of the Practice

Page ___ of ___

F3.5C

Practice Name: _____

Last Updated: _____

Personal HIPAA Training Profile

Employee Name: _____

Employee ID No.: _____

Title/Position: _____

The following policies and procedures apply to your job responsibilities. You must receive training on the policies and procedures listed in the table below.

Policy/Procedure			
Number Description	Date Assigned	Date Read by Employee	Date Training Completed

Page ___ of ___

F3.5D

Name of Practice:

Address:

Privacy Official:

Telephone:

Training Session Documentation Form

Date(s) Training Conducted: _____

Name of Person(s)/Company Conducting Training:

_____

Length of Training Program: _____

Title of Training Seminar (include Policy or Procedure No(s).):

Attendee Name (Please print): Attendee Signature: Date:

Forward this completed form to the Privacy Official.

F3.5E

Confidentiality Agreement

EMPLOYEE
CONFIDENTIALITY AGREEMENT

THIS CONFIDENTIALITY AGREEMENT is made and entered into by and between:

Employee: _____("Employee")

Medical Practice: _____("Practice")

Effective Date of these Terms and Conditions:_____

WHEREAS, the services the Practice performs for its patients are confidential; and

WHEREAS, by reason of employment with the Practice, Employee will have access to, will be provided with, and will, in some cases, prepare confidential and proprietary business information, such as patient services and diagnoses, employee information, financial data, and operations information, which must remain confidential for the protection of the Practice, its patients and its employees; and

WHEREAS, Employee acknowledges that he or she has received training by the Practice on all privacy policies and procedures applicable to the Employee's job function; and

WHEREAS, Employee understands that, by virtue of this Confidentiality Agreement ("Agreement"), it is hereafter a condition of employment with the Practice that all confidential information be maintained as confidential in compliance with the Practice's privacy policies and procedures as well as all applicable state and federal laws and regulations.

NOW, THEREFORE, in consideration of compensation paid in conjunction with the execution of this Agreement, and intending to be legally bound hereby, the Practice and Employee agree as follows:

1. Contract Consideration. The following provision that is initialed and dated by both parties is hereby incorporated into this Agreement (initial and date only *one* provision, and *only* the initialed and dated provision is made part of these Terms and Conditions):

   _____ _____ A. In consideration of employment, Employee agrees to the Terms and Conditions as provided herein.
   Employee Initials/Date | Practice's Initials/Date

   _____ _____ B. In consideration of _____ dollars ($_____.00) paid to Employee at the time of execution of this Agreement, Employee agrees to the Terms and Conditions as provided herein.
   Employee Initials/Date | Practice's Initials/Date

2. Confidentiality. Employee shall not, at any time during or following employment with the Practice, disclose or use, except as required in the course of employment, any confidential or proprietary information of the Practice whether such information is in memory or embodied in writing or other physical form. Confidential or proprietary information (i) is information that is not generally available to the general public, or competitors, or ascertainable through common sense or general business knowledge; and (ii) includes, but is not limited to: corporate information and patient information.

3. Property. All records, files, or other objects maintained by or under the control, custody, or possession of the Practice, including, without limitation, medical records, shall be and remain property of the Practice. Upon termination of employment, Employee shall return all such property received in connection with Employee's employment.

4. Breach. Disclosure or use of confidential or proprietary information, except as permitted under this Agreement, shall constitute a breach of this Agreement and a breach of a condition of employment with the Practice.

5. REMEDIES. ANY BREACH OF THIS AGREEMENT MAY RESULT IN DISCIPLINARY ACTION, UP TO AND INCLUDING IMMEDIATE DISMISSAL. IN THE EVENT OF A BREACH OF THIS AGREEMENT, MONEY DAMAGES ALONE MAY NOT BE ADEQUATE TO COMPENSATE THE PRACTICE FOR ITS LOSSES, AND, THEREFORE, EMPLOYEE AGREES THAT THE PRACTICE SHALL BE ENTITLED TO INJUNCTIVE RELIEF, IN ADDITION TO ANY OTHER REMEDIES PROVIDED BY LAW OR IN EQUITY.

6. Further Information. If at any time during or after employment, Employee believes he or she needs further information regarding the Practice's confidentiality policies and procedures or how confidentiality relates to the Practice's business, Employee shall request such information from a supervisor or other appropriate representative of the Practice.

7. Amendment. This Agreement may not be changed, modified, or terminated except in writing signed by both Employee and an authorized Practice representative.

8. Law. This Agreement shall be governed by and construed in accordance with the laws of the State where the principal Practice office in which the Employee works is located.

IN WITNESS WHEREOF, the parties have caused this Agreement to be executed by their duly authorized representatives on the date first above written.

EMPLOYEE

By: _____

Name (Print): _____

Title: _____

MEDICAL PRACTICE

By: _____

Name (Print): _____

Title: _____

PRIVACY MANAGEMENT: INTERNAL SANCTIONS PP3.6

Overview

Introduction

The Privacy Rule requires our Practice to have and apply appropriate sanctions (Internal Sanctions) against members of our workforce if we, or one of our Business Associates, use or disclose PHI in violation of our Practice's policies and procedures or the requirements of HIPAA.

Under the Privacy Rule, Internal Sanctions are not to be applied against whistleblowers, workforce member crime victims, or others by reason of conduct that is in good faith and protected from retaliation.

Policies and Procedures

PP3.6 describes our policies and procedures regarding Internal Sanctions.

The Privacy Official and Practice management will be responsible for implementing Internal Sanctions policies and procedures.

All Practice employees should understand that the Privacy Rule requires that we have and apply these Sanctions policies and procedures.

Contact Person

Our Privacy Official is designated to be the contact person for questions, suggestions, or complaints relating to Internal Sanctions, and our compliance with the Privacy Rule relating to Internal Sanctions for privacy violations.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PRIVACY MANAGEMENT: INTERNAL SANCTIONS PP3.6

General Policy

Policy

Our Practice's policy is to take disciplinary action (Internal Sanctions), if appropriate and as approved by our president or governing board (or other person designated by the president or governing board to take action), against any member of the Practice's workforce who has improperly used or disclosed health care information in violation of our Practice's privacy policies and procedures or HIPAA or state privacy law requirements.

As required by the Privacy Rule, no Internal Sanctions will be applied against whistleblowers, workforce member crime victims, or others by reason of conduct that is in good faith and protected from retaliation.

Employees Are Employed At Will

This policy does not alter or change in any way the fact that Practice employees are employed on an at-will basis (unless there is an individual written contract that says otherwise), nor does this policy limit the Practice's ability to terminate any employee at any time, with or without cause or advance notice, for any reason not prohibited by law.

Document Internal Sanctions

When Internal Sanctions are undertaken by our Practice, a record of the Internal Sanctions will be maintained in the Privacy Official's records.

PRIVACY MANAGEMENT: INTERNAL SANCTIONS PP3.6

Index of Procedures

Introduction

Our Practice's obligation to have and apply Internal Sanctions for a violation of our privacy policies and procedures or violation of the Privacy Rule is subject to a practical and flexible standard. The Privacy Official and Practice management will determine what procedures and actions are appropriate when our Practice undertakes Internal Sanctions.

Inquiry/Action Steps

Follow these steps with respect to Internal Sanctions:

Step	Inquiry/Action
1	Identify situations where a violation of our Practice's policies and procedures or violation of the Privacy Rule might have occurred.
2	The Privacy Official will review and investigate the complaint or report that a violation of our Practice's policies and procedures or a violation of the Privacy Rule has occurred.
3	The Privacy Official will review whether exceptions to Internal Sanctions apply.
4	(If applicable) the Privacy Official will consider Business Associate actions.
5	Determination regarding Internal Sanctions.
6	The Privacy Official will document the complaint or report, the investigation and disposition, and the Internal Sanctions imposed, if any.

Step 1: Identify Situations Where a Violation of Our Practice's Policies and Procedures or Violation of the Privacy Rule Might Have Occurred

Introduction

Our Practice is obligated to have and apply as appropriate Internal Sanctions related to a use or disclosure of PHI only if the use or disclosure is a violation of our policies and procedures or a violation of the Privacy Rule.

This procedure can be used by the Privacy Official and supervisory employees of our Practice to identify situations where Internal Sanctions might be required.

Step 1.1

Identify the Use or Disclosure of PHI

If you learn that a use or disclosure of information has occurred under questionable circumstances or if someone (whether a member of our workforce or not) informs you about such a use or disclosure of PHI, ask sufficient questions to understand exactly what information was used or disclosed in order to confirm that the information was really PHI.

Step A If the person is making a complaint, refer the matter immediately to the Privacy Official. See Complaints, PP2.6. Otherwise, **proceed to Step B.**

Step B If the information was PHI, **proceed to Step 1.2.**

Step C If the information was not PHI, no violation of our HIPAA policies and procedures or of the Privacy Rule has occurred and you can so inform the individual questioning the use or disclosure. If the individual is not a member of our Practice's workforce or if a member of our workforce continues to question the use or disclosure, refer the matter to our Privacy Official so that he or she can continue with Step 2.

Step 1.2

Determine Whether the Use or Disclosure Might Be a Violation of Our Policies and Procedures or of the Privacy Rule

If PHI was used or disclosed, consider whether the use or disclosure might be a violation of our Practice's HIPAA policies and procedures or a violation of the Privacy Rule.

Step A If the use or disclosure might be a violation, refer the matter to our Privacy Official.

Step B If the use or disclosure appears to be in compliance with our Practice's HIPAA policies and procedures and with the Privacy Rule, so inform the individual questioning the use or disclosure and **proceed to Step 1.3.** If the individual is not an employee of our Practice or if an employee of our Practice continues to question the use or disclosure, refer the matter to our Privacy Official, who will proceed to Step 2.

Step 1.3

Report the Incident to the Privacy Official

Even if you believe the incident has been satisfactorily resolved, make a brief oral report of the incident to the Privacy Official as appropriate.

Step 2: The Privacy Official Will Review and Investigate the Complaint or Report That a Violation of Our Practice's Policies and Procedures or a Violation of the Privacy Rule Has Occurred

Introduction

When the Privacy Official receives a complaint or a report of a possible violation of our Practice's policies and procedures or a violation of the Privacy Rule, he or she will follow this procedure in order to facilitate the Internal Sanctions process required if our Practice's policies and procedures are violated or the Privacy Rule is violated.

If the Privacy Official is absent or unable to act, the Privacy Official or the president of our Practice or the governing board of our Practice, as appropriate, may designate another trained employee or member of our Practice to review and investigate a complaint or report that the Internal Sanctions procedures might apply. Such designated individual will "stand in the shoes" of the Privacy Official for purposes of this procedure.

Step 2.1

The Privacy Official Reviews the Procedures of Step 1

The Privacy Official will review the procedures of Step 1, Determine Whether a Violation of Our Practice's Policies and Procedures or a Violation of the Privacy Rule Might Have Occurred, and will determine whether he or she believes that a violation has occurred giving rise to the possibility of Internal Sanctions.

Step 2.2

The Privacy Official Investigates the Complaint or Report

If the circumstances surrounding a complaint or report of a possible violation of our Practice's policies and procedures or possible violation of the Privacy Rule are unclear, the Privacy Official will investigate the facts underlying the possible violation of our Practice's policies and procedures or violation of the Privacy Rule.

The procedure for the investigation will be determined by the Privacy Official, in consultation with the president of our Practice, taking into account the facts and circumstances of the alleged violation. The Privacy Official may consult with legal counsel, particularly if there are questions of law he or she wishes to discuss in confidence. The Privacy Official will conduct the procedures, which may include one or more of the following actions, in cooperation with the individual workforce member's supervisor:

- provide suspected workforce member with adequate and complete notice of allegation of violation or breach;
- determine whether workforce member should take leave of absence during investigation;

- investigate workforce member's conduct by revisiting the analysis under Step 1, questioning witnesses, reviewing documentation related to the alleged violation or breach, and taking such other actions as the Privacy Official deems appropriate to learn the facts surrounding the allegations of improper disclosure of PHI;
- hold a meeting with the suspected workforce member and his or her supervisor or another member of management; and/or
- determine whether the facts can support a finding that the workforce member committed the alleged violation or breach.

Step 2.3

The Privacy Official Confirms Whether the Facts Can Support a Finding That a Violation Has Occurred

Step A If the Privacy Official believes that the facts cannot support a finding that a violation or breach of our Practice's privacy policies and procedures or violation of the Privacy Rule has occurred, the Privacy Official will **proceed to Step 6** to document the complaint or report and the Privacy Official's findings and disposition.

Step B If the Privacy Official believes the facts can support a finding that a violation of our Practice's privacy policies and procedures or violation of the Privacy Rule has occurred, the Privacy Official will **complete Steps 3 through 6.**

Step 3: The Privacy Official Will Review Whether Exceptions to Internal Sanctions Apply

Introduction

Our Practice cannot impose Internal Sanctions against whistleblowers, workforce member crime victims, or others who have engaged in conduct that is in good faith and protected from retaliation because of such conduct. The Privacy Official makes a report and recommendations regarding whether these exceptions apply and whether Internal Sanctions can be applied with respect to a particular violation, except for violations by the Privacy Official himself or herself.

If the Privacy Official is absent or unable to act, the Privacy Official or the president of our Practice or the governing board of our Practice, as appropriate, may designate another trained employee or member of our Practice to make a report and recommendations regarding whether exceptions to the Internal Sanctions rules apply. Such designated individual will "stand in the shoes" of the Privacy Official for purposes of this procedure.

Step 3.1

Privacy Official Determines Whether Exceptions Apply

The Privacy Official will follow Steps 3.2 through 3.5 to determine, in consultation with counsel, whether an exception to the requirement to impose Internal Sanctions applies.

Step 3.2

Exception for Disclosure By a Whistleblower

No Internal Sanctions may be applied against a "whistleblower" based on the fact that he or she is or was a whistleblower. The Privacy Official will review, in consultation with counsel, whether the disclosure was made by a Whistleblower under circumstances giving rise to an exception from Internal Sanctions.

A A "Whistleblower" is a member of the workforce or a business associate who discloses PHI in the good faith belief that either:

- our Practice has engaged in conduct that is unlawful or otherwise violates professional or clinical standards; or
- the care, services, or conditions provided by our Practice potentially endanger one or more patients, workers, or the public.

B A member of the workforce or a business associate who is a "Whistleblower" can disclose *only* to:

- a health oversight agency or public health authority authorized by law to investigate or otherwise oversee the relevant conduct or conditions of our Practice, or an appropriate health care accreditation organization for the

purpose of reporting the allegation of failure to meet professional standards or misconduct by our Practice; or

- an attorney retained by or on behalf of the Whistleblower for the purpose of determining the legal options of the Whistleblower with regard to impermissible or unlawful conduct by the Practice described in Step A.

Step 3.3

Exception for Disclosure By a Workforce Member Crime Victim

If a member of our Practice's workforce who is a victim of a criminal act discloses PHI to a law enforcement official, no Internal Sanctions may be applied by reason of such disclosures. The Privacy Official will review, in consultation with counsel, whether the exception for disclosure by a workforce member crime victim applies. The exception will apply *if*:

Step A The Privacy Official determines that the PHI disclosed is about the suspected perpetrator of the criminal act *and*

Step B The Privacy Official determines that the PHI disclosed is limited to:

- name and address;
- date and place of birth;
- social security number;
- ABO blood type and rh factor;
- type of injury;
- date and time of treatment;
- date and time of death, if applicable; and
- description of distinguishing physical characteristics, including height, weight, gender, race, hair and eye color, presence or absence of facial hair (beard or moustache), scars, and tattoos.

Step 3.4

Exception for Disclosure By an Employee Engaging in Conduct Subject to Retaliation

If an employee of our Practice engages in conduct that is protected from retaliation, no Internal Sanctions may be applied because of such conduct.

The Privacy Official, in consultation with counsel, will review whether this exception applies. This exception will apply if the Privacy Official, upon investigation, determines that the disclosure was directly related to conduct of the individual employee when he or she was:

- filing a complaint with the Secretary of HHS due to the belief that our Practice is not complying with HIPAA; or
- testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing under Part C of Title XI of the Social Security Act; or
- opposing any act or practice made unlawful by HIPAA, provided the individual has a good faith belief that the practice opposed is unlawful, and the manner of the opposition is reasonable and does not involve a disclosure of PHI in further violation of HIPAA.

Step 3.5

Consider Business Associates

Step A If a Business Associate is involved in the privacy violation, **proceed to Step 4.**

Step B If no Business Associate is involved in the privacy violation, **proceed to Step 5.**

Step 4: (If Applicable) the Privacy Official Will Consider Business Associate Actions

---

Introduction

While our Practice is not required constantly to monitor the privacy compliance activities of its Business Associates, our Policy is to take steps to address problems of which we become aware. PP1.14, Business Associates, sets forth our relationship with our Business Associates.

Step 4.1

Examine Business Associate Agreement

When our Practice learns of a violation of our Practice's policies and procedures or violation of the Privacy Rule that involves a Business Associate of our Practice, the Privacy Official will review the relevant Business Associate Agreement. See Business Associates, PP.1.14.

Step 4.2

Privacy Official Reviews Whether Business Associate Violated Its Agreement

The Privacy Official, taking into account the facts and circumstances of the violation of our Practice's policies and procedures or violation of the Privacy Rule and in consultation with counsel for the Practice, the president and/or the governing board of our Practice, as appropriate, and with the Business Associate will review whether the Business Associate breached its Business Associate Agreement.

Step 4.3

Privacy Official Will Determine Appropriate Action With Respect to Business Associate

The Privacy Official will notify the Business Associate of the complaint or report of a privacy violation.

Step A If the Business Associate has breached its agreement, resulting in a violation of our Practice's policies and procedures or violation of the Privacy Rule, the Privacy Official, in consultation with the president or governing board of our Practice, as appropriate, will notify the Business Associate and inform the Business Associate of the actions required to mitigate the violation.

Step B If the violation is serious or repeated, the Privacy Official may undertake to monitor the Business Associate's behavior for a trial period.

Step C If the Privacy Official believes that the Business Associate cannot be relied upon to maintain the privacy of PHI provided to it under its Business Associate Agreement, the Privacy Official will report to the president and governing board of our Practice, who may cause the Practice to terminate the agreement or, if termination of the agreement is not feasible, may report the matter to HHS.

Step 5: Determination Regarding Internal Sanctions

Introduction

Our Practice will follow this procedure to reach a determination regarding whether Internal Sanctions should be applied and, if so, what sanctions should be applied.

The final decision regarding Internal Sanctions will be made by an individual ("Review Official") appointed by the president of our Practice or our governing board, as appropriate to the severity of the issue, the employees or workforce members involved, and the structure of our Practice.

Although not specified by the Privacy Rule, Internal Sanctions could range from verbal warning to termination, but our Practice determines its own sanctions and when to apply them.

Step 5.1

Our Practice Will Impose Internal Sanctions

When our Practice becomes aware of a violation of our policies and procedures or a violation of the Privacy Rule, the Practice will impose Internal Sanctions with respect to the violation, if appropriate. The Practice may choose to consult with its legal counsel prior to imposing Internal Sanctions.

Step 5.2

Review Official Will Consider Factors and Goals in Determining Internal Sanctions

In determining whether to impose Internal Sanctions and in determining the Internal Sanctions appropriate to a particular violation, the Review Official will consult with the Privacy Official and the individual workforce member's supervisor, and may, in the Review Official's discretion, consider such factors as:

- severity of the violation,
- whether the violation was intentional or unintentional, and
- whether the violation indicated a pattern of repeated improper use or disclosure of PHI, and
- the workforce member's overall performance.

Note

HIPAA does not prescribe the required Internal Sanctions. Depending upon the factors identified by the Review Official and the circumstances of the infraction, the disciplinary action deemed appropriate by the Review Official should accomplish the following objectives:

- communicate the importance of the violation to the affected individual,
- deter the affected individual from similar actions,
- improve compliance with Practice policies and procedures, and HIPAA requirements, and
- prevent future recurrence of the violation.

Step 5.3

Privacy Official and Practice Management Applies Internal Sanctions and Existing Sanctions In Their Discretion

Step A The Privacy Official and management of our Practice will review existing sanctions for employee violations of policies and procedures of our Practice, and will determine, in their sole discretion, how Internal Sanctions for privacy violations will be applied, taking into account our Practice's other existing sanctions.

Step B The Privacy Official and management of our Practice will disclose this Internal Sanctions policy and any other sanction policies to workforce members upon request.

Step 5.4

Review Official Imposes Internal Sanctions In the Review Official's Discretion

Our Practice, through the appointed Review Official, may apply appropriate Internal Sanctions at its discretion.

The Internal Sanctions imposed might take the form of:

- issuance of a written warning or admonition;
- requiring a workforce member to take immediate corrective measures, if practicable;
- re-education of workforce members;
- loss of privileges;
- loss of rights to bonus;
- leave of absence with pay;
- leave of absence without pay;
- reassignment; or
- termination of employment.

Step 5.5

Privacy Official Issues Written Notice of Internal Sanctions to Workforce Member

The Privacy Official will issue written notice to the affected workforce member of Internal Sanctions determined by the Review Official, unless oral notification is directed by the Review Official.

Except in cases of immediate termination, the written notice of Internal Sanctions will also include notice of the workforce member's opportunity to appeal the Privacy Official's determination to the governing board of our Practice or to an appeals committee appointed by the governing board.

Step 5.6

Privacy Official Takes Steps to Confirm Compliance with Internal Sanctions

The Privacy Official will take other steps to confirm compliance with Internal Sanctions, such as:

- informing the workforce member's supervisor of the Internal Sanctions imposed;
- meeting at regular intervals with the workforce member to receive reports of compliance with the Internal Sanctions;
- witnessing actions taken by the workforce member in compliance with the Internal Sanctions imposed; and/or
- such other actions as the Privacy Official deems appropriate to confirm compliance with Internal Sanctions imposed on a workforce member.

Step 5.7

Privacy Official Reports Egregious Conduct to Enforcement Officials

If the Privacy Official or Practice management determines that the conduct of the workforce member is intentional, unlawful, and egregious, the Privacy Official or Practice management, as they respectively deem appropriate with advice of counsel, may report a workforce member's conduct to the police, HHS, or other government agencies with enforcement jurisdiction.

Example of potentially reportable conduct: A Practice employee regularly steals and sells PHI and other information for his or her personal gain (eg, identity theft). No Permission applies and the patients are not aware of and have not authorized the use or disclosure. This may be a clear, intentional, and repeated violation of the Privacy Rule for personal gain.

Step 6: The Privacy Official Will Document the Complaint or Report, the Investigation and Disposition, and the Internal Sanctions Imposed, If Any

Introduction

The Privacy Official will maintain a record of each privacy complaint or report, of documentation related to the review of the privacy complaint or report, the Privacy Official's investigation, and the disposition of the complaint or report for a period of 6 years from the date of the Practice's final disposition of the complaint or report.

> Note
>
> At the Privacy Official's discretion, our Practice may communicate with legal counsel regarding legal advice about report or complaints, and we may so communicate with the intention of doing so under attorney-client privilege, as legal counsel may advise or recommend.

Step 6.1

Privacy Official Establishes a Log of Complaints and Reports

The Privacy Official will establish a log to record the circumstances of each complaint or report of a violation of our Practice's privacy policies and procedures or the Privacy Rule that results in Internal Sanctions.

Step 6.2

Privacy Official Maintains File of Documentation Related to the Log

The Privacy Official will maintain a file containing the following items with respect to each logged complaint or report of a privacy violation:

- a copy of the written complaint or report, or a transcribed version or written summary of a verbal complaint or report of a violation of our Practice's policies and procedures or violation of the Privacy Rule;
- copies of all letters of inquiry and a list of all such inquiries and other steps taken in the investigation;
- a written statement of the Privacy Official's findings and recommendation with respect to matters in the complaint or report; and
- a report by the Privacy Official of Internal Sanctions imposed and actions undertaken, if any, and the reason for the actions or the reason for the absence of Internal Sanctions if none is undertaken.

Step 6.3

Confidential Personnel File

When Internal Sanctions involve a violation by an employee of our Practice, a record of the Internal Sanctions actions will be filed in a special confidential personnel file for the employee for employment-related purposes.

Step 6.4

Privacy Official Retains Items in Log and File for 6 Years

The Privacy Official will retain the log of complaints and reports of violations of privacy and the related document files for a period of 6 years from the date of the Practice's final disposition of the specific complaint or report.

PRIVACY MANAGEMENT: MITIGATION PP3.7

Overview

Introduction

If our Practice, or one of our Business Associates, uses or discloses PHI in violation of our policies and procedures or the requirements of HIPAA, the HIPAA Privacy Rule requires our Practice to mitigate, to the extent practicable, any harmful effect that we know about. This process is called Mitigation in these policies and procedures.

The Mitigation requirements are intended to be flexible enough to avoid imposing an undue burden on our Practice.

Policies and Procedures

PP3.7 describes our policies and procedures regarding Mitigation.

Contact Person

Our Privacy Official is designated to be the contact person for questions, suggestions, or complaints relating to Mitigation, and our compliance with the Privacy Rule relating to Mitigation of privacy breaches.

PRIVACY MANAGEMENT: MITIGATION PP3.7

General Policy

Policy

Our Practice will mitigate, to the extent practicable and required by the Privacy Rule, any harmful effect that is known to the Practice of a use or disclosure of PHI by the Practice or its Business Associates in violation of the Practice's privacy policies and procedures or in violation of requirements of the Privacy Rule.

Any employee or workforce member may report to the Privacy Official or Practice management the employee's concerns or questions regarding whether our Practice and its workforce are complying with our privacy policies and procedures or applicable legal requirements.

The Privacy Official, the president of our Practice, and our governing board will be responsible for responding to such complaints, inquiries, or concerns, including determining and implementing mitigation where warranted.

Mitigation is Practical and Flexible

"To the extent practicable" is not defined in the Privacy Rule, nor does the Privacy Rule specify what reasonable steps our Practice must take to mitigate harm from a privacy breach. Instead, the Privacy Rule allows for flexibility by relying upon the judgment of those familiar with the circumstances in our Practice to dictate the best approach for mitigating the harm from the improper use or disclosure of PHI. Our Privacy Official and our Practice will act based on knowledge of where the PHI was disclosed, how it might be used to cause harm to the patient or another individual, and what steps can actually have a mitigating effect in that specific situation.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

Document Mitigation

When Mitigation is undertaken by our Practice, a record of the Mitigation efforts will be maintained in the Privacy Official's records.

PRIVACY MANAGEMENT: MITIGATION PP3.7

Index of Procedures

Introduction

Our Practice's obligation to mitigate harm caused by a breach of our privacy policies and procedures or a breach of the Privacy Rule is subject to a practical and flexible standard.

The Privacy Official and Practice management will determine what actions are appropriate for our Practice to take regarding Mitigation.

Inquiry/Action Steps

Follow these steps with respect to Mitigation:

Step	Inquiry/Action
1	Identify situations where a breach of privacy might have occurred.
2	The Privacy Official will review and investigate the complaint or report that a breach of privacy has occurred.
3	The Privacy Official will recommend Mitigation actions.
4	The Privacy Official will document the complaint or report, the investigation and disposition, and the Mitigation actions undertaken, if any.
5	(If applicable) the Privacy Official will consider Business Associate actions.

Step 1: Identify Situations Where a Breach of Privacy Might Have Occurred

Introduction

Our Practice is obligated to mitigate harm from a use or disclosure of PHI only if the use or disclosure is a breach of our policies and procedures or a breach of the Privacy Rule.

This procedure can be used by supervisory employees of our Practice to identify situations where Mitigation might be required.

Step 1.1

Identify the Use or Disclosure of PHI

If you learn that a use or disclosure of information has occurred under questionable circumstances, or if someone (whether a member of our workforce or not) informs you about such a use or disclosure of PHI, ask sufficient questions to understand exactly what information was used or disclosed in order to confirm that the information was really PHI.

Step A If the person is raising a complaint, refer the matter immediately to the Privacy Official. See Complaints, PP2.6. Otherwise, **proceed to Step B.** Likewise, at any point where the issue appears to require Mitigation, refer the matter directly to the Privacy Official who will **proceed with Step 2.**

Step B If the information was PHI, **proceed to Step 1.2.**

Step C If the information was not PHI, no breach of our HIPAA policies and procedures or of the Privacy Rule has occurred and you can so inform the individual questioning the use or disclosure. If the individual is not an employee of our Practice, or if an employee of our Practice continues to question the use or disclosure, refer the matter to our Privacy Official so that he or she can continue with Step 2.

Step 1.2

Determine Whether the Use or Disclosure Might Be A Violation of Our Policies and Procedures or of the Privacy Rule

If PHI was used or disclosed, consider whether the use or disclosure might be a violation of our Practice's HIPAA policies and procedures or a violation of the Privacy Rule.

Step A If the use or disclosure might be a violation, refer the matter to our Privacy Official.

Step B If the use or disclosure appears to be in compliance with our Practice's policies and procedures and with the Privacy Rule, so inform the individual questioning the use or disclosure and **proceed to Step 1.3.** If the individual is not an employee of our Practice or if an employee of our Practice continues to question the use or disclosure, refer the matter to our Privacy Official, who will **proceed to Step 2.**

Step 1.3

Report the Incident to the Privacy Official

Even if you believe the incident has been satisfactorily resolved, make a brief oral report of the incident to the Privacy Official.

Step 2: The Privacy Official Will Review and Investigate the Complaint or Report That a Breach of Privacy Has Occurred

Introduction

When the Privacy Official receives a report of a possible breach of privacy, he or she will follow this procedure in order to facilitate the Mitigation process required if our Practice's policies and procedures are violated or the Privacy Rule is violated.

Step 2.1

The Privacy Official Reviews the Procedures of Step 1

The Privacy Official will review the procedures of Step 1, Identify Situations Where a Breach of Privacy Might Have Occurred, and will determine whether he or she believes that a breach of privacy has occurred giving rise to the possibility of a need to mitigate.

Step 2.2

The Privacy Official Investigates the Complaint or Report

If the circumstances surrounding a complaint or report of a breach of privacy are unclear, the Privacy Official will investigate the facts underlying the alleged breach of privacy giving rise to a possible need to mitigate. The Privacy Official may consult with legal counsel for the Practice, particularly if there are questions of law he or she wishes to discuss in confidence.

Step 2.3

The Privacy Official's Belief

Step A If the Privacy Official believes that no breach of privacy has occurred, the Privacy Official will proceed to Step 5 to document the complaint or report and the Privacy Official's findings and disposition.

Step B If the Privacy Official believes that a breach of privacy has occurred, the Privacy Official will complete Steps 3 through 5.

Step 3: The Privacy Official Will Recommend Mitigation Actions

Introduction

The Privacy Official generally is the only employee or member of the Practice who may make recommendations regarding Mitigation with respect to a particular breach, except for breaches by the Privacy Official himself or herself. If the Privacy Official is absent or unable to act, the Privacy Official, the president of our Practice, or our Practice's governing board may designate another trained employee or member of our Practice to "stand in the shoes" of our Privacy Official and make recommendations regarding Mitigation.

Step 3.1

Take Reasonable and Practicable Steps to Mitigate Breaches

When our Practice knows of a breach of our policies and procedures or a breach of the Privacy Rule, the Practice will take reasonable steps to mitigate the breach.

In determining the Mitigation steps to be undertaken, the Privacy Official will consider the nature of the privacy breach, where the information was disclosed, how it might be used to cause harm to the patient or another individual, and what steps can actually have a mitigating effect in that specific situation. The Privacy Official will recommend appropriate Mitigation actions to the president or governing board of our Practice for final approval, as appropriate to the circumstances. The governing board may delegate its authority hereunder to a committee of the board.

Mitigation may include the following actions, or other actions appropriate to the situation, in the discretion of the Privacy Official as approved by the president or governing board of our Practice (or an authorized committee of the board), as appropriate to the circumstances:

- an apology to the patient, or additional action directly with the patient intended to mitigate the harm to the patient;
- retrieval of the information, where possible, to prevent further use or disclosure by others;
- adoption of policies and procedures by our Practice to avoid a similar breach;
- notification to the recipient, directly or through legal counsel, that the information is confidential and requesting or demanding that the information be returned and neither used nor disclosed to others;
- in egregious cases, such as a patient who is a public figure, seeking an injunction to prevent the impermissible further use or disclosure or damages for an impermissible use or disclosure;
- retraining workforce members to prevent further harm from the breach;
- workplace sanctions against workforce members responsible for the breach, in consultation with the supervisors of the workforce members;
- in consultation with the workforce members' supervisors, dismissal of workforce members responsible for the breach; or
- reporting egregious cases to the proper authorities.

Note

In order to reduce the burden of compliance, HIPAA does not prescribe the required Mitigation policies and procedures. The only requirement is that our Practice must mitigate the harm done "to the extent practicable." This does not require that our Practice completely eliminate the harm done, but it does require we do what is reasonable and practicable.

For example, if an employee of the Practice inadvertently provides PHI to a third party without authorization in a domestic abuse situation, the Practice is expected promptly to contact the patient and the appropriate authorities to apprise them of the potential danger.

Step 3.2

Monitor and Continue Mitigation if Necessary

The Privacy Official will monitor Mitigation and continue Mitigation of privacy breaches to the extent practicable.

Note

Continuing Mitigation does not mean taking Mitigation procedures indefinitely, unless such a process continues to provide legitimate results. Though HIPAA does not define what is "practicable," this term has been utilized to allow flexibility for practices to move on after privacy breaches, once reasonable steps have been taken to mitigate the harm done.

Step 3.3

Consider Business Associates

Step A If a Business Associate is involved in the privacy breach, **proceed to Step 4.**

Step B If no Business Associate is involved in the privacy breach, **proceed to Step 5.**

Step 4: The Privacy Official Will Document the Complaint or Report, the Investigation and Disposition, and the Mitigation Actions Undertaken, if any

Introduction

The Privacy Official will maintain a record of each privacy complaint or report, of documentation related to the review of the privacy complaint or report, the Privacy Official's investigation, and the disposition of the complaint or report, for a period of 6 years from the date of the Practice's final disposition of the complaint or report.

Step 4.1

Privacy Official Establishes a Log of Complaints and Reports

The Privacy Official will establish a log to record the circumstances of each complaint or report of a breach of our Practice's privacy policies and procedures or the Privacy Rule that results in Mitigation.

Step 4.2

Privacy Official Maintains File of Documentation Related to the Log

The Privacy Official will maintain a file containing the following items with respect to each logged complaint or report of a privacy breach:

- a copy of the written complaint or report, or a transcribed version or written summary of a verbal complaint or report of a breach of privacy;
- copies of all letters of inquiry and a list of all such inquiries and other steps taken in the investigation;
- a written statement of the Privacy Official's findings and recommendations with respect to matters in the complaint or report; and
- a report by the Privacy Official of Mitigation actions undertaken, if any, and the reason for the actions or the reason for no Mitigation if none is undertaken.

Step 4.3

Confidential Personnel File

When Mitigation involves a breach by an employee of our Practice, a record of the Mitigation actions will be filed in a special confidential personnel file for the employee for employment-related purposes.

Step 4.4

Privacy Official Retains Items in Log and File for 6 Years

The Privacy Official will retain the log of complaints and reports of breaches of privacy, and the related document files, for a period of 6 years from the date of the Practice's final disposition of the specific complaint or report.

Step 5: (If Applicable) the Privacy Official Will Consider Business Associate Actions

Introduction

While our Practice is not required constantly to monitor the activities of its Business Associates, it is required to and will take steps to address the problems of which it becomes aware. PP1.14, Business Associates, sets forth our relationship with our Business Associates.

Step 5.1

Examine Business Associate Agreement

When our Practice learns of a breach of privacy that involves a Business Associate of our Practice, the Privacy Official will review the relevant Business Associate Agreement. See Business Associates, PP1.14.

Step 5.2

Privacy Official Reviews Whether Business Associate Breached Its Agreement

The Privacy Official, taking into account the facts and circumstances of the breach of privacy and in consultation with the Business Associate, if appropriate in the Privacy Official's judgment, will review whether the Business Associate breached its Business Associate Agreement.

Step 5.3

Privacy Official Will Determine Appropriate Action With Respect to Business Associate

The Privacy Official, after consulting with the president and/or governing board of our Practice, as appropriate, will notify the Business Associate of the disposition of the complaint or report of a privacy breach.

Step A If the Business Associate has breached its Agreement, resulting in a breach of privacy, the Privacy Official will notify the Business Associate and inform the Business Associate of the actions required by our Practice to mitigate the breach.

Step B If the breach is serious or repeated, the Privacy Official may undertake to monitor the Business Associate's behavior for a trial period.

Step C If the Privacy Official believes that the Business Associate cannot be relied upon to maintain the privacy of PHI provided to it under its Business Associate Agreement, the Privacy Official will report to the president and governing board of our Practice, who may cause our Practice to terminate the agreement or, if termination is not feasible, may report the matter to HHS.

PRIVACY MANAGEMENT: NO RETALIATION PP3.8

General Policy

It is our Practice's policy to refrain from intimidating or retaliatory acts against patients or other persons, as required by the Privacy Rule.

Scope of Policy

This policy applies to intimidating or retaliatory acts against both patients and other persons.

No Retaliation Against Patients

It is our Practice's policy not to intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient for the exercise of any rights under the Privacy Rule, including filing a complaint.

No Retaliation Against Patients or Other Persons

It is our Practice's policy not to intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any patient or other person for:

- Filing a complaint with the Secretary of HHS;
- Testifying, assisting, or participating in an investigation, compliance review, proceeding, or hearing; or
- Opposing any act or practice made unlawful by the Privacy Rule, provided the patient or other person (1) has a good faith belief that the practice is unlawful and (2) the manner of opposition is reasonable and does not involve the disclosure of PHI in violation of the Privacy Rule.

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PRIVACY MANAGEMENT: NO WAIVER OF RIGHTS PP3.9

General Policy

It is our Practice's policy that we will **not** require an individual to waive his or her rights under the Privacy Rule, including the right to make a complaint to the Secretary of HHS, as a condition of treatment, payment, enrollment in a health plan, or eligibility for benefits.

The terms "treatment" and "payment" are explained in PP1.3.

Scope of Policy

This policy applies to rights provided to individuals under the Privacy Rule, including the rights to make the following requests:

Policy	Policy Number
Access	PP2.1
Amendment	PP2.2
Accounting	PP2.3
Alternative Communications	PP2.4
Further Restrictions	PP2.5
Complaints	PP2.6

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PRIVACY MANAGEMENT: SAFEGUARDS PP3.10

Overview of Policies and Procedures for Safeguards	Policy Number	Page Number
Safeguards—Index of Policies and Procedures	PP3.10	336
Administrative Procedures (AP)		345
Safeguards Documentation	AP1	345
Security Management Process	AP2	345
Certification of Compliance	AP3	347
Contingency Plans	AP4	349
Formalized Record Processing	AP5	351
Access Control/Personnel Security/Termination Procedures	AP6	352
Internal Audit/Security Incident	AP7	355
Workforce Security Training	AP8	358
Common Sense Protections	AP9	359
Physical Security (PS)		361
Assigned Security Responsibility	PS1	361
Media Controls	PS2	362
Physical Access Controls	PS3	365
Workstation Policy and Guidelines	PS4	368
Technical Security (TS)		371
Data Integrity Controls	TS1	371
Computer Access, Audit, and Authorization Controls	TS2	372
Data and Entity Authentication	TS3	375
Safeguards Glossary		379

Effective Date: _____

Approved: _____

Last Revised: _____

Amended by Attachment (date): _____

PRIVACY MANAGEMENT: SAFEGUARDS PP3.10

Overview

Introduction

The Practice has an obligation to implement appropriate administrative, technical, and physical Safeguards to protect the privacy of protected health information (PHI).

This PP3.10 is designed to assist the Privacy Official or the Security Official to develop appropriate policies and procedures regarding Safeguards. Each Practice will be different in the approach it chooses. As a beginning, the appropriate official can recommend the Practice adopt the general Safeguards Policy and proceed, using the chart, Safeguards Development and Documentation, F3.10, to track progress through the fundamental steps of security. It is the effort of the Practice and its workforce that determines the success or failure of the Safeguards policy and procedures.

Definition

"Safeguards" generally means rules and specific mechanisms designed to protect PHI from being (a) accessed by unauthorized persons; (b) accidentally or intentionally used, disclosed, transmitted, or altered; or (c) inadvertently or incidentally disclosed to persons not intended and/or not authorized to receive the PHI.

Safeguards Policy

The Practice and all Practice employees will install, use, and update appropriate Safeguards to ensure the integrity and confidentiality of PHI; to protect against any reasonably anticipated (i) threat or hazard to the security or integrity of PHI, and (ii) unauthorized uses or disclosures of the information; and otherwise to ensure compliance with relevant HIPAA regulations by the Practice.

Scope of Policy

This policy applies to PHI that is used, maintained, or transmitted by the Practice, and PHI received from or disclosed to our Business Associates, and can apply to other persons or organizations outside of the Practice. The policy covers the following implementation areas:

- Administrative Procedures (AP);
- Physical Safeguards (PS); and
- Technical Security (TS).

Detailed policies and procedures for each of these areas follow this overview.

Quick Reference Guide—Safeguards

The Quick Reference Guide in Chapter 2 includes examples of permitted incidental disclosures. It also includes examples of Safeguards. The Quick Reference Guide should provide guidance for the most common day-to-day situations in a medical practice setting.

Assigned Security Responsibility

Policy PS1 describes the process for assigning responsibility for Safeguards. The Practice must designate a specific person (the "Security Official") to manage and supervise (a) the use of security measures to protect data, and (b) the conduct of workforce members that has something to do with protecting data. The Privacy Official should supervise the development and implementation of appropriate Safeguards, and in most cases, will be the person assigned responsibility for security. A practice may also elect to appoint an outside consultant or contractor. Alternatively, if a practice member or employee has significant expertise in information technology (IT) or another applicable area, that person may make an appropriate Security Official even if he or she is not the Privacy Official for the Practice.

Approach to Developing, Implementing, and Updating Safeguards

At present, no bright line requirements exist to determine what is an appropriate safeguard. Even the proposed security rule requirements are at best a guide to the measures a practice will need to put in place to meet its obligation to provide protections for PHI. The Practice will make determinations about safeguard measures through a process of risk management. Recognizing that information can never be completely secure, each practice will need to make determinations about the risks presented by its systems, operations, and information use practices, and identify the types of Safeguards that provide the best protection against those risks without unduly compromising the Practice's ability to operate and provide efficient, high-quality services to its patients.

To be effective, Safeguards must be customized to the Practice's information storage practices, usage, and access practices. A practice that is primarily paper-based and does not maintain patient information electronically within the Practice will not need to implement all of the same types of Safeguards as a practice that maintains patient information in an electronic medical record and includes physicians who correspond with patients via e-mail or access patient information using a handheld PDA device. As a result, a practice will need to take a more active approach to adopting Safeguards than to complying with other HIPAA privacy requirements.

These policies and procedures use the proposed security rule as a starting place and offer a step-by-step approach to developing various types of Safeguards that are described in the Privacy Rule. HIPAA does not require a practice to adopt or implement each specific element in the proposed security regulations, and each practice will have to make a decision about those efforts that are reasonable and appropriate to protect PHI. To that end, the following specific activities can help a practice.

- Obtain the information necessary to identify reasonable and appropriate Safeguards ("Survey and Assessment");
- Identify and compare options and select a safeguard that strikes an appropriate balance between risk and damage reduction and cost (eg, financial and quality of care) ("Evaluation");
- Document, implement, and verify the policy or procedure ("Documentation," "Implementation," and "Certification"); and
- Make sure the policy or procedure is working over time ("Audit and Update").

Each of these areas is discussed in more detail in the following pages.

Survey and Assessment

To be best equipped to make defensible decisions about Safeguards, the Practice needs to conduct a Survey and Assessment to know as much as possible about the following:

- How, why, and from whom is PHI received?
- How, why, and to whom is PHI transmitted?
- In which media are PHI stored and where are those media kept?
- Who has access to PHI within the Practice and why?
- Who needs access to PHI, for what purpose(s), and how much PHI do they need?
- How could an unauthorized person gain access to PHI and why might someone want to do so?
- How much control does the Practice have over individuals entering and leaving its facilities (especially areas containing PHI storage media, and how and how well does the Practice keep track of the identities of individuals granted access to the facilities/systems)?
- What resources (financial, human, etc.) does the Practice have available to develop, implement, monitor, and maintain Safeguards?
- How could unauthorized access to, or use or disclosure of, PHI affect practice operations?
- How might loss of access to PHI affect the Practice's operations?

- What Business Associates or vendors have access to PHI and for what purposes?
- What assistance can vendors offer the Practice in implementing Safeguards, and which vendors' help is needed?

Evaluation

Armed with the information gathered in the Survey and Assessment process, the Practice is poised to identify potential Safeguards and determine which ones best balance the Practice's responsibility to protect PHI with its responsibility to provide effective health care services efficiently and in a manner that does not compromise the quality of care offered to patients. This is the Evaluation process.

While only a few solutions may exist for certain security threats, in most cases, the Practice will need to choose between several options, all of which reduce, but do not completely eliminate, the risk posed by the threat. The trick is to get the best result for the cost. Some solutions may be inexpensive and easy to implement, but may eliminate a bare majority of the risk. Other solutions may eliminate much more of the risk, but may be very expensive themselves, or may cost a great deal indirectly by substantially reducing efficiency within the Practice. In many cases, the best solution will be one that neither costs the least nor the most, but that provides the greatest protection against unauthorized use, access, or disclosure at a reasonable cost, with the least amount of impact on the quality of care and practices offered by the Practice.

To weigh these considerations, the Practice should perform a cost-benefit analysis. In this way, the Practice can assess potential Safeguard options to determine which provides the most suitable balance between burden on the Practice and effective reduction of risk of a likely security breach.

In conducting a cost-benefit analysis, the Practice should take into account the following with respect to each Safeguard under consideration:

- Costs: financial cost, effect on efficient treatment practices, effect on patient care, administrative burdens, length of anticipated period of effectiveness, and vulnerability of the Safeguard itself.
- Threats: ease of access, value of information held by the Practice, number of potential motives for obtaining the information, special knowledge or skills required to accomplish the threat, potential damage if the threat is carried out.
- Benefits: potential for reducing risk of unauthorized access, use, or disclosure; potential to shift liability to another party; the longevity and resilience of the Safeguard; and any improvements in access to information, efficient treatment, or patient care.

Based on its analysis, the Practice should select the most effective Safeguards to meet its needs.

Documentation

All decisions regarding appropriate Safeguards for the Practice must be documented. To make sure this occurs, approval of Safeguards must be centralized and all individuals with responsibility for developing independent policies or procedures must be required to create and submit written policies.

Once completed and approved, Documentation of Safeguards must be appropriately distributed, including to all individuals with responsibility for implementing any of the policies and procedures. The Practice may choose to require such individuals to document their implementation of the policies and procedures.

Storing Documentation of Safeguards in a central location will make it easier to (a) make the policies and procedures available, (b) review and update them on a regular basis, and (c) maintain the Documentation in accordance with HIPAA's document retention requirements and any other applicable state or federal standards.

Implementation

When the Practice has decided on a particular Safeguard and documented it, it must take steps to implement the Safeguard within the operations of the Practice. Implementation of the Safeguard requires that the Practice accomplish the following goals:

- Develop and document Safeguards, see F3.10
- Distribution of Safeguards documentation to affected employees
- Training of employees to comply with appropriate policies and procedures
- Performance of specific security mechanisms, such as locking file cabinets or repositioning workstations and monitors
- Testing of policies, procedures, and security mechanisms
- Development, dissemination, and imposition of sanctions for failure to follow applicable Safeguards policies or procedures

Certification

When the Practice has fully implemented its Safeguards, it may wish to make sure that each safeguard works as anticipated, and that the combination of Safeguards provides reasonable and appropriate protection for PHI. The Practice may perform this Certification assessment itself, or it may contract with an outside entity. The Certification should assess how well the Safeguards perform under normal and stress conditions, as well as live and simulated conditions.

The goal of the Certification is to ensure that the Safeguards meet or exceed the Practice's minimum expectations. This means that the Safeguards reduce the risk of a security breach to a level that the Practice previously determined to be acceptable.

A Certification process should involve a report measuring performance of the Safeguards in quantitative terms, which will provide a reference point for future audits. If Certification is performed, the report should be submitted and approved by the governing body of the Practice.

Audit and Update

After the Safeguards have been in place for a certain period of time, the Practice may wish to perform or contract with an outside entity to perform an assessment to see how well the Safeguards have been implemented, whether they perform as anticipated, and to identify changes that may be necessary, advisable, or desirable to further enhance the protection the Practice can provide for PHI.

Any changes the Practice makes in its policies and procedures will require a repeat of the steps from Documentation through Certification. Regardless of whether the Practice has altered its security arrangements, workforce members should receive additional training regarding their responsibilities under the Practice's Safeguards policies and procedures.

QUICK REFERENCE GUIDE

Examples of Common Safeguards

The following Quick Reference Guide—Examples of Common Safeguards includes examples of different types of security mechanisms that may provide useful solutions to the Practice's need to provide reasonable and appropriate Safeguards. These are only examples. Adopting and implementing these Safeguards alone will not be sufficient for the Practice's obligation to protect PHI.

No.	Safeguard Category	Examples of Safeguards
AP	Administrative Procedures	
AP1	Safeguard Documentation	Written designation of Security Official, and other written security policies and procedures
AP2	Security Management Process	Controls for installation/maintenance of equipment Inventory of hardware and software assets Workstation policies/mandatory password change Periodic virus-checking policy/procedure
AP3	Certification of Compliance	Certification review by self or third-party expert
AP4	Contingency Plans	Arrangements for disaster recovery and emergency mode services
AP5	Formalized Record Processing	Designating a secure fax machine to receive PHI
AP6	Access Control/Personnel Security/Termination Procedures	Maintain access/authorization records Personnel/security clearance—background/reference checks Sanctions and termination policies and procedures for security violations
AP7	Internal Audit	Regular review of access activity records Regular inventories of storage media for PHI Security incident response procedures
AP8	Workforce Security Training	Orientation/regular workforce security training
AP9	Common Sense Protections	Staff to talk in low voices when discussing PHI Procedures for loud speaker communications *See* Permitted Incidental Disclosures in Quick Reference Guide
PS	Physical Security	
PS1	Assigned Security Responsibility	Written designation of Security Official Allocation of responsibility between Privacy and Security Officials if not the same person
PS2	Media Controls	Locked doors, cabinets, drawers Data backup, storage, and disposal procedures
PS3	Physical Access Controls	Facility security plan Visitor sign-in/escort requirements
PS4	Workstation Policy and Guidelines	Automatic logoff/screen time-out requirements Secure workstation locations

No.	Safeguard Category	Examples of Safeguards
TS	Technical Security	
TS1	Data Integrity Controls	Firewalls/virus protection/alarm
TS2	Computer Access, Audit, and Authorization Controls	Access controls and audit trail Encryption
TS3	Data and Entity Authentication	Unique user identifier Automatic logoff/screen time-out requirements Password/personal identification number (PIN)

PRIVACY MANAGEMENT: SAFEGUARDS PP3.10

Index of Policies and Procedures

Introduction

Accomplishing the goal of limiting physical access to the Practice itself, and to PHI created, stored, and used within the Practice in particular, requires the collection and analysis of information about the Practice and the development of specific rules to govern the behavior of Practice workforce members in their daily routines, as well as in unusual or emergency circumstances.

The Security Official is responsible for handling or overseeing the tasks described in the policies and procedures below. In some cases, the Security Official may need to work with individuals within or outside of the Practice who have specific knowledge or responsibilities that relate to the goals of a particular policy or procedure.

Policies and Procedures

Adopt the following policies and implement the following procedures to develop and institute mechanisms to adequately safeguard PHI created, received, stored, used, and disclosed by the Practice.

Form F3.10, Documentation

Immediately following this Index is Form F3.10, "Safeguards Development and Documentation." This form is designed to capture the work of our Practice in developing and adopting appropriate Safeguards.

The Privacy Official or Security Official, as the case may be, can use Form F3.10 for project management and to record the name of each document that describes aspects of our Practice's Safeguards. When our Practice has fully implemented adequate Safeguards, Form F3.10 will provide a listing of the policies and procedures the Practice has adopted related to Safeguards. Form F3.10 can also constitute a record of any changes to or revocations of the Practice's Safeguards policies and procedures.

Physical Security (PS)

Policy/Procedure	Title
PS1	Assigned Security Responsibility
PS2	Media Controls (paper and electronic)
PS3	Physical Access Controls (physical and electronic)
PS4	Workstation Use

Administrative Procedures (AP)

Policy/Procedure	Title
AP1	Safeguards Documentation
AP2	Security Management Process
AP3	Certification of Compliance
AP4	Contingency Plans
AP5	Formalized Record Processing
AP6	Access Control/Personnel Security/ Termination Procedures
AP7	Internal Audit/Security Incident
AP8	Workforce Security Training
AP9	Common Sense Protections

Technical Security (TS)

Policy/Procedure	Title
TS1	Data Integrity Controls
TS2	Computer Access, Audit, and Authorization Controls
TS3	Data and Entity Authentication

F3.10A

Safeguards Development and Documentation

Policy/ Procedure	Title	Status	Timeframe	Document Title	Comments
Administrative Procedures (AP)					
AP1	Safeguards Documentation				
	Document Retention Policy				
	Document Destruction Protocol				
AP2	Security Management Process				
	Procedure for Developing/ Implementing Security Management				
	Perform a risk analysis				
	Perform risk management				
	Specific penalties and enforcement mechanisms				
	Develop a security policy				
	Procedure for Security Configuration Management				
	Documentation				
	Procedures for hardware and software				
	Inventory procedures				
	Regular security testing				
	Regular virus checking				

Policy/ Procedure	Title	Status	Timeframe	Document Title	Comments
AP3	Certification of Compliance				
	Procedure for Certifying Compliance				
	Role of legal counsel				
	Identify requirements for Certification process				
	Self-certification: Practice policies and procedures				
	Self-certification: Commercial products				
	Contracted Certification: Vendor RFQ				
	Contracted Certification: Vendor selection process				
	Review and approval of certification report				
AP4	Contingency Plans				
	Procedure for Developing/ Implementing Contingency Plans				
	Disaster threat and resource identification				
	Evaluation of potential effects of disaster				
	Alternatives for access to information				
	Arrangements for disaster recovery services				

Policy/ Procedure	Title	Status	Timeframe	Document Title	Comments
AP5	Formalized Record Processing				
	Procedure for Developing/ Implementing Record Processing				
	Identify sources from which the Practice receives or may receive PHI				
	Process for securing PHI by storing or recording				
	Develop policies and procedure with security in mind				
AP6	Access Control/Personnel Security/Termination Procedures				
	Procedure for Implementing Access Controls				
	Information access control				
	Revision of access status				
	Procedure for Implementing Personnel Security				
	Access authorization records				
	Supervision of technical and maintenance personnel				
	Training for personnel				
	Procedure for Implementing Termination Procedures				
	Notification of termination				
	Review of applicable access controls				

Policy/ Procedure	Title	Status	Timeframe	Document Title	Comments
	Schedule for revision/ repossession of access controls				
	Notification of other employees				
AP7	Internal Audit/Security Incident				
	Procedure for Developing/ Implementing Internal Audits				
	Review access activity report				
	Documentation of review				
	Investigation and reporting				
	Procedure for Developing/ Implementing Security Incident Response				
	Steps to respond to security incidents				
	Documentation—audit record				
	Security incident report				
AP8	Workforce Security Training				
	Procedure for Implementing Workforce Security Training				
	Awareness training for all personnel				
	Periodic security reminders				
	User education concerning virus protection				
	User education in discrepancies				
	User education in password management				

Policy/ Procedure	Title	Status	Timeframe	Document Title	Comments
AP9	Common Sense Protections				
	Procedure for Identifying Common Sense Protections				
	Protections for oral communications				
	Protections for visual displays				
	Protections for clinic operations practices				
	Structural protections				
	Protections for patient communications				
Physical Security (PS)					
PS1	Assigned Security Responsibility				
	Procedure for Developing/ Implementing Policy				
	Allocation of responsibility for security				
	Privacy Official develops a work plan				
	Job description or specifications for the Security Official position				
	Work plan approved by executive or governing body				
	Chain of authority and reporting responsibility				
	Procedure If the Security Official Is Not the Privacy Official				
	Select Security Official				
	Interview candidates or issue RFP to vendors				

Policy/ Procedure	Title	Status	Timeframe	Document Title	Comments
	Evaluate candidate or vendor submissions				
	Acknowledgment by Security Official				
PS2	Media Controls (paper and electronic)				
	Procedure for Developing/ Implementing Media Controls				
	Provide for access control				
	Maintain accountability				
	Regular data backup protocol				
	Secure, organized data storage				
	Create a secure disposal regime				
PS3	Physical Access Controls (physical and electronic)				
	Procedure for Developing/ Implementing Physical Access Controls				
	Procedure for Creating a Disaster Recovery System and Providing for Emergency Mode Operation				
	Procedure for Developing a Facility Security Plan				
	Procedure for Creating Processes to Verify Access Authorizations Before Granting Physical Access				
	Procedure for Developing a System to Organize and Review Maintenance Records				

Policy/ Procedure	Title	Status	Timeframe	Document Title	Comments
	Procedure for Instituting Need-To-Know Access				
	Procedure for Creating Testing and Revision Protocols				
PS4	Workstation Use				
	Procedure for Developing/ Implementing Workstation Policies and Guidelines				
	Procedure for Developing a Policy and Guidelines on Workstation Use				
	Procedure for Providing Secure Workstation Locations				
Technical Security (TS)					
TS1	Data Integrity Controls				
	Procedure for Developing/ Implementing Technical Security Mechanisms				
	Network inventory and classification				
	Development/ identification of security mechanisms				
	Data access and integrity controls				
	Network control features				
	Monitoring and education				
TS2	Computer Access, Audit, and Authorization Controls				
	Procedure for Developing/ Implementing Computer Controls				
	Emergency access				
	Access and authorization controls				

Policy/ Procedure	Title	Status	Timeframe	Document Title	Comments
	Encryption				
	Audit controls				
TS3	Data and Entity Authentication				
	Procedure for Developing/ Implementing Data and Entity Authentication				
	Provide for data authentication				
	Provide for entity authentication				

PRIVACY MANAGEMENT: SAFEGUARDS PP3.10

Administrative Procedures (AP)

Introduction

Administrative procedures are the documented, formal practices in operations management to assure that adequate Safeguards are established and implemented.

Index of Administrative Procedures:

Policy/Procedure	Title	Page No.
AP1	Safeguards Documentation	345
AP2	Security Management Process	345
AP3	Certification of Compliance	347
AP4	Contingency Plans	349
AP5	Formalized Record Processing	351
AP6	Access Control/Personnel Security/ Termination Procedures	352
AP7	Internal Audit/Security Incident	355
AP8	Workforce Security Training	358
AP9	Common Sense Protections	359

Administrative Procedures (AP): Safeguards Documentation AP1

Policy

It is the Practice's policy that all decisions regarding appropriate Safeguards for the Practice be documented. Documentation relating to safeguard decisions shall be maintained by the Privacy Official. Documentation must be retained for 6 years from the date of any final decision about a security measure. After the 6-year retention period, Safeguard-related documentation shall be destroyed in the manner prescribed by the Practice's document retention policy.

Scope of Policy

This policy applies to all policies, procedures, and mechanisms that the Practice decides to adopt as Safeguards for PHI.

Administrative Procedures (AP): Security Management Process AP2

Introduction

To facilitate effective coordination, oversight, and management of the Practice's efforts to provide Safeguards, while also providing an incentive to the Security Official to manage relationships with vendors as cost-effectively as possible, the Practice should develop policies and procedures that facilitate the detection and correction of security breaches, and coordination of activities relating to security.

Policy

The Practice shall develop policies and procedures and implement measures to preserve and enhance the security of PHI stored by the Practice, and to correct security breaches and enforce other policies. The policies and procedures shall address coordination with other system management configuration practices. Specifically, the Practice shall coordinate its efforts with respect to vendor submissions and routine system changes to hardware or software with its security needs.

Scope of Policy

This policy would apply to the development and implementation of all Safeguards with respect to PHI maintained within or used by the Practice.

Procedure for Developing/ Implementing Security Management

1. Perform a risk analysis.
   - ■ Analyze the vulnerabilities of the Practice's PHI systems and information that passes through the Practice. This analysis should include:
     - ☐ Value of information assets; and
     - ☐ Funding and computing resources.
   - ■ Evaluate ways in which and reasons why the Practice's systems might be attacked, including:
     - ☐ Motives for attack;
     - ☐ Types of threat;
     - ☐ Methods for system access; and
     - ☐ Technical capability necessary for unlawful access.
   - ■ Consider consequences to Practice of unlawful access to information systems, including:
     - ☐ Physical losses;
     - ☐ Economic losses; and
     - ☐ Cost of mitigation after the fact.
   - ■ Consider costs of methods of providing adequate Safeguards for the Practice and decide on an acceptable level of risk based on this cost-benefit analysis of liabilities, threats, costs of security breach, and prevention cost.
2. Perform risk management:
   - ■ Decide on a security regime that will maintain the already-decided acceptable level of risk.
   - ■ Implement the security regime and put in place a maintenance regime consisting of targeted updates and training programs.
3. Incorporate specific penalties and enforcement mechanisms for safeguard-related breaches as part of the Practice's Internal Sanctions policies and procedures under PP3.6.
4. Develop a security policy. It is important that the Privacy Official or Security Official, as the case may be, continue to develop the Practice's policies and procedures regarding Safeguards.

Procedure for Security Configuration Management

1. Documentation
   - ■ The Security Official refers to the information regarding information storage developed through the Media Controls Policy and PS2.
   - ■ The Security Official confirms that agreements, such as Business Associate Agreements, are in place to address security and Safeguards with entities with whom the Practice exchanges information. The Practice negotiates such provisions as amendments to agreements that do not already contain such requirements.
2. The Security Official, working with IT staff and/or with vendors, develops procedures for hardware and software installation and maintenance review and testing for security features. This means formal, documented procedures for:
   - ■ Connecting and loading new equipment and programs;
   - ■ Periodic review of the maintenance occurring on equipment and programs; and
   - ■ Periodic security testing of the security attributes of that hardware/software.
3. The Security Official takes inventory and provides for inventory procedures to track hardware and software assets.
4. The Security Official provides for regular security testing.
5. The Security Official provides for regular virus checking.

Cross-References

Media Controls, PS2

Verification, PP1.12

Workforce Training, PP3.5

Mitigation, PP3.7

Administrative Procedures (AP): Certification of Compliance
AP3

Introduction

The Practice should evaluate and certify that appropriate security measures have been implemented to protect data on any computer systems or communication networks used by the Practice. The Certification may be provided by an outside entity.

Policy

The Practice will take steps to verify that Safeguards have been implemented and that such protections are performing as anticipated.

Scope of Policy

This policy applies to the entire set of measures implemented by the Practice to safeguard the confidentiality of PHI. The Evaluation and Documentation of performance process should take place once all measures are in place and functioning, and at least annually thereafter to ensure that the system continues to function at the appropriate level.

Procedure for Certifying Compliance

1. The Security Official consults with senior executives and/or members of the Practice's governing body to determine whether to conduct Certification through legal counsel. Depending upon state law and the circumstances, this may permit the Practice to take advantage of the protections of the attorney-client privilege to insulate the Practice against the effect of improper inferences from the Certification document in any subsequent litigation based on security breaches.

2. Identify requirements for an effective Certification process.

- The Security Official determines whether any Updates to the Privacy Rule are available. As of this writing, the federal government has not decided what criteria would be required for an appropriate certification of Safeguards under the Privacy Rule. The Security Rule under HIPAA remains in proposed form (see Preamble, 63 *Fed. Reg*. 43242, 43251 (Aug. 12, 1998)).
- The Security Official, together with the representative of the Practice in charge of IT, should determine whether it is possible for the Practice to provide Certification itself. This assessment should be based on the technical sophistication of Practice employees, staffing considerations, and the extent to which the Practice relies on products or services from third parties (eg, consultants or vendors) for its compliance with the physical and technical security standards.
- If self-Certification is a possibility for the Practice, the decision whether to self-certify or contract for Certification should be made in conjunction with senior executives and possibly the governing body of the Practice (depending on the Practice's usual process). The Practice may wish to consult with legal counsel to determine any additional risks associated with self-Certification.
- If the Practice elects to self-certify, it should follow the procedure set forth in Steps 3 and 6 of this procedure. If the Practice elects to hire an outside entity to perform the Certification, it should follow Steps 4, 5, and 6 of this procedure.

3. Self-Certification: Practice policies and procedures. If the Practice decides to self-certify, the following procedures may assist in documenting compliance with adequate Safeguards and security program requirements:
   - Certification Plan. The Security Official and Practice IT representative should develop a detailed document with the following elements:
     - ☐ Description of computer system and network configuration;
     - ☐ Scope of project and schedule of activities to be performed;
     - ☐ Allocation of responsibility for each activity;
     - ☐ Timeline for completion of review.
   - Certification Procedures. The Security Official and Practice IT representative develop detailed instructions describing how to conduct each piece of the Certification review. These procedures should include the following elements for each element to be tested:
     - ☐ Description of test methods and conditions, which may include normal, stress, simulation, live-user/site tests, structural testing, functional testing, and network, system, or program build testing.
     - ☐ Minimum performance benchmarks
     - ☐ Range of anticipated performance
   - Certification Report. At the conclusion of the review, the Security Official and Practice IT representative prepare a report documenting the results of the testing. Wherever possible, the results should be expressed in quantitative terms that will permit independent evaluation and comparison with later performance. The Practice may wish to require that the Certification report be reviewed and approved by its chief executive or chief operating officer.
4. Self-Certification: Commercial products: The following steps may assist the Practice in certifying that it has met one or more of its security obligations through the use of commercially available products:
   - Identify the functions that the Practice needs each product to perform and develop specifications from that process. Obtain a copy of the developer's specifications for comparison. Software vendors will have products with varying levels of emphasis or security. More recent products are likely to be more sophisticated with respect to security capabilities.
   - Conduct research into ways in which the product has been used in the past to identify and evaluate known product limitations, known problems, and resolution.
   - Test all functions of the product under normal conditions and stress conditions designed to simulate maximum user load and emergency situations. Tests should include its independent functionality, and how well the product works with the rest of the data systems and networks used by the Practice.
   - Evaluate the test results to determine whether the performance meets the Practice's requirements under all applicable situations.
5. Contracted Certification: If the Practice elects to contract with an entity to perform the Certification, the Security Official and Practice IT representative should review and evaluate potential vendors for the Certification service. If the Practice has contracted with one or more vendors to supply solutions for its compliance obligations under the Security Rule, an independent vendor should be considered for the project. Appropriate criteria for selection would be:
   - Demonstrated experience with security issues
   - Knowledge/experience in working with and evaluating electronic data systems
   - Familiarity with and ability to conduct the self-certification procedures set forth in Steps 2 and 3

- Experience with health care practice environments and business needs
- Law enforcement or other security-related experience
- Capacity to staff project appropriately and work efficiently
- Cost-effectiveness
- References

6. Contracted Certification process:

- The Security Official and Practice IT representative interview candidates or issue a Request for Proposals (RFP) to competing vendors.
- The Security Official and Practice IT representative evaluate candidates and/or review submissions and select a vendor to perform the Certification.
- The selected vendor performs the certification process and issues its report to the Practice for review by the Security Official and Practice IT representative.

7. Review and approval:

- The Certification report, along with documentation of any corrective action steps taken in response to the report, is submitted to the Practice's board or governing body for review and approval.
- The board should review the certification report to determine whether the level of risk the report identifies with respect to Safeguards is consistent with the level of risk that the Practice determined was reasonable to accept. The Board may consider the following in its review:
  - ☐ Consistency of performance
  - ☐ Nature of Safeguards implemented
  - ☐ Costs of further enhancements
  - ☐ Likelihood of threats to which information is exposed
  - ☐ Harm from threats
  - ☐ Availability of insurance or other mechanisms for shifting risk of loss in the event of a privacy breach
  - ☐ Board decides whether to accept report and whether to require that (additional) corrective action steps be taken to further reduce risk

Administrative Procedures (AP): Contingency Plans AP4

Introduction

A contingency plan, such as the creation and maintenance of off-site, hard copy backups of electronic information, will allow for continuity of record keeping, security, and care in the aftermath of a natural disaster, a failure of the network uniting the Practice's computers with stored information, or other situations that prevent electronic access to the Practice's medical data. A contingency plan for emergency mode operation will allow the smaller practice group to continue to operate while separated from its usual information storage systems, including any networks.

Policy

The Practice will develop and maintain appropriate policies to provide for a backup and to permit access to data necessary for emergency functions and certain Practice operations in the event of reasonably anticipated threats. The Practice also will develop and maintain a policy and procedure to reconstruct data that is lost or damaged in the event of a disaster or other threat.

Scope of Policy

This policy applies to all sources, uses, and storage media for data within the Practice.

Procedure for Developing/ Implementing Contingency Plans

The following procedures should be developed at the same time and in connection with the procedures for emergency operations and Disaster Recovery in the Physical Access Control procedures, PS3.

1. Threat and resource identification and classification.
- Security Official identifies potential disasters (eg, fire, flood, extended power outage) that may affect Practice operations.
- Security Official reviews current Practice operations, including current information access, storage, and use practices (see Media Controls Procedure, PS2).

2. Evaluation of potential effects.
- For each type of potential disaster, the Security Official identifies the following direct impacts on the Practice:
  - ☐ Possible impacts on availability of the records and data systems routinely used by the Practice
  - ☐ Possible impacts on the security of all media, and data storage
  - ☐ Possible impacts on Practice operations during and after the disaster that do not specifically relate to data access
  - ☐ Special data the Practice may need to operate during or after the disaster
  - ☐ Operations for the Practice to be able to provide services (the "Critical Operations")
  - ☐ Operations or functions within the Practice that support or are supported by other Practice operations or functions (the "Interdependent Functions")
- For each type of potential disaster, the Security Official identifies potential indirect impacts on the Practice. Such impacts may include:
  - ☐ Loss of power from damage or destruction of powerlines/utilities
  - ☐ Loss of communications ability from damage to communication lines, transmitters, and facilities, or excess demand on communication systems

3. Develop alternatives for access to information.
- For each type of disaster, the Security Official must develop alternative solutions to maintain each Critical Operation or Interdependent Function in light of the assumptions about impacts of each particular disaster.
- Each alternative should contain all of the following elements:
  - ☐ Identify the person responsible for initiating the plan in the event of a disaster
  - ☐ Describe specific actions to be taken to make the alternative possible before and during the disaster
  - ☐ Describe specific actions to reduce damage or impact of the disaster
  - ☐ Allocate responsibility for required activities
  - ☐ Address contingencies if Interdependent Functions are unavailable
  - ☐ Describe actions to maintain or minimize impacts to protections for data resources

4. Develop arrangements for Disaster Recovery services.
- For each record used in the Practice, the Security Official develops a data recovery plan that contains all of the following elements:
  - ☐ Alternative sources of the data contained in the record, along with their locations
  - ☐ The method for recovering any lost data
  - ☐ Access controls and other Safeguards to prevent unauthorized use or disclosure of the records being constructed

- The Security Official investigates Disaster Recovery specialists, issues an RFP for Disaster Recovery plans, and selects a vendor for Disaster Recovery services.
- The Security Official evaluates vendor submissions and selects an entity to be responsible for Practice security.
- The Practice contracts with the vendor for Disaster Recovery services. The contract should include appropriate Business Associate and security provisions.
- The Security Official should test the disaster and emergency operations plan for each Critical Operation or Interdependent Function.

Cross-References

Security Management, AP3

Media Controls Procedures, PS2

Physical Access Control Procedures, PS3

Administrative Procedures (AP): Formalized Record Processing AP5

Introduction

The Practice should incorporate security considerations into its documented policies and procedures regarding the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of sensitive information. The purpose for incorporating these considerations is to avoid the inadvertent loss or disclosure of sensitive information because of a failure in the process.

Policy

The Practice shall take security considerations into account in crafting its policies and procedures relating to the routine and nonroutine receipt, manipulation, storage, dissemination, transmission, and/or disposal of sensitive information.

Scope of Policy

Applies to all PHI received, used, maintained, or disclosed by the Practice.

Procedure for Developing/ Implementing Record Processing

1. The Security Official will identify sources from which the Practice receives or may receive PHI.
2. With respect to each source, the Security Official will identify a recipient or class of recipients for the PHI.
3. To the extent that PHI received from identified sources is not received through channels secured under the Technical Security Mechanisms in Procedure TS1, or the Technical Security Services in Procedures TS2 and TS3, the Security Official shall establish a process for securing such information by storing or recording it in an appropriately secure storage medium.
   - For example, where the Practice receives PHI by facsimile transmission from other providers, the Practice may elect to designate a specific fax machine for receiving such transmissions. The fax machine could be located in a secure area (eg, the same location where patient records are stored), with an individual employee designated for monitoring the fax and promptly removing faxed materials to the appropriate files or otherwise bringing them to the attention of the appropriate party in a secure fashion.
   - The costs and benefits of each alternative should be assessed before committing to any particular approach.
4. With respect to use, storage, and disclosure of PHI, information security considerations and the Practice's information security system structure should be taken into account in developing policies and procedures under the Minimum Necessary, Verification, and other standards required by the Privacy Rule.

Cross-References

Media Controls, PS2

Verification, PP1.12

Minimum Necessary, PP1.13

Administrative Procedures (AP): Access Control/ Personnel Security/Termination Procedures AP6

Introduction

To prevent unnecessary, unauthorized, or inadvertent access to sensitive information, the Practice should develop a process for granting different levels of access to sensitive information, and for modifying such access as needed after the initial granting of access. This is critical to compliance with Minimum Necessary, PP1.13. All personnel accessing sensitive information should have appropriate clearance authorizing access to PHI before any PHI is made available.

Policy

The Privacy Official is responsible for granting access to sensitive information, including PHI. Upon written request describing the reason from the office administrator or a supervisor with respect to an identified practice employee or contractor, or class of employees or contractors, the Privacy Official may modify the scope of access for such employee(s) or contractor(s) as the Privacy Official deems necessary and appropriate to meet the need described in the request.

Where an employee is terminated from the Practice, the office administrator shall coordinate termination actions with the Privacy Official so that termination of access to sensitive information is accomplished as nearly as practicable to the actual termination.

Scope of Policy

This policy applies to all grants of access to PHI by any member, employee, or contractor of the Practice.

Procedure for Implementing Access Controls

1. Information access control

- The Security Official, with approval of the Practice, adopts policies and procedures for controlling access to sensitive information, including PHI used within the Practice.
- Such policies and procedures include those adopted under the Media Control, Physical Access Control, Data Access and Computer Access Control policies and procedures contained in this Desk Reference.
- The Security Official identifies the circumstances that create access authorization requirements (eg, new hires, new vendor relationships).
- The Security Official reviews the potential threats of unauthorized access or disclosure of information received, stored, used, transmitted, or disclosed by the Practice and identifies a range of options for restricting access to specific types of storage, display, or other media.
- Where an individual requires access to sensitive information, the Security Official takes such steps as he or she deems appropriate to verify that the individual is suitable for access to PHI. Methods for obtaining such information could include the following:
  - ☐ Criminal background checks
  - ☐ Credit/financial history
  - ☐ Professional discipline
  - ☐ Employment history/references
- The Security Official consults with the Practice's legal counsel to understand the legal implications of any strategies he or she intends to adopt as part of an access control strategy.

- Working with the office administrator or other persons within the Practice responsible for such circumstances, the Security Official develops a procedure for identifying the access needs of individual Practice personnel and implementing background checks or other control strategies as part of the hiring process.
- The Security Official works with the office administrator or other person(s) within the Practice responsible for situations involving access needs, to establish an action plan for evaluating individuals for access clearance and establishing the appropriate access for individuals to function within their positions in the Practice.
- The Security Official maintains a documentary record of the access authority granted to all individuals within the Practice.

2. Revision of access status

- The Security Official identifies circumstances within the Practice where individuals may need revisions to access privileges. Such situations might include
  - ☐ Promotion
  - ☐ Termination
  - ☐ Consolidation of staff/RIFs
  - ☐ Temporary reassignment
  - ☐ Establishing new services
- For each circumstance, the Security Official requires that all supervisors or individual(s) responsible in the circumstance submit a written request to the Security Official for a change in access authorization sufficiently in advance of the intended effective date to allow the Security Official to assess the request and provide for the additional access.
- In evaluating each request, the Security Official revisits any background check or other information retained by the Practice to determine whether the individual is suitable for the additional access requested. If a significant amount of time has elapsed since the information was collected, the Security Official may wish to update the Practice's information. The Security Official may wish to consult with legal counsel for the Practice to determine whether legal or regulatory requirements mandate updating of information.
- Upon completion of the review of background information, the Security Official determines whether to grant or deny the modification request.
  - ☐ If the modification request is granted, the Security Official takes the necessary steps to implement the modifications requested. He or she also documents the modification and its effective date on the Practice's record of access authorizations.

Procedure for Implementing Personnel Security

1. Access authorization records

- The Security Official should maintain a documentary record of access authorizations for all individuals with access to sensitive information within the Practice
- Documentation of access authorization includes:
  - ☐ The name and position of the individual
  - ☐ The individual's user account and user ID
  - ☐ The scope of the individual's access authorization by type of information, storage media, position, access purpose, or any other information that would assist in identifying an event of unauthorized access by the individual
  - ☐ The date the individual's access commenced

- ☐ Identifying information regarding any keys, cards, tokens, or combination access provided to the individual

2. Supervision of technical and maintenance personnel

- ■ The Security Official provides a process for ensuring that all technical and maintenance personnel with access to the Practice's storage media or sensitive information are monitored or supervised by a representative of the Practice, or that an appropriate Business Associate agreement is in place, and that such individuals are adequately supervised by the Business Associate.
- ■ These steps can be taken in conjunction with the Media Control policies and procedures developed under PS2.

3. Training for personnel

- ■ Personnel will be trained in implementation of security policies and procedures with respect to access controls.
- ■ Training can be incorporated in regular updates received by the Practice workforce.

Procedure for Implementing Termination Procedures

1. Notification of termination

- ■ When any workforce member of the Practice or a Business Associate of the Practice who has access to PHI is to be terminated, the Practice office administrator or other person responsible for the termination notifies the Security Official sufficiently in advance of the termination to provide adequate opportunity to identify and terminate the affected individual's access to PHI.
- ■ The Practice requires such notification of termination in its Business Associate Agreements with any individuals or entities who will be provided access to PHI.

2. Review of applicable access controls

- ■ Upon receipt of notification that an individual is to be terminated, the Security Official shall notify the Privacy Official (if that position is filled by an individual other than the Security Official).
- ■ The Security Official reviews the Practice's records of access authorization to determine the scope of the affected individual's access to sensitive information within the Practice and the mechanisms available to the individual to obtain such access. Access mechanisms that should be considered include:
  - ☐ Combination locks
  - ☐ Keys, cards or other tokens
  - ☐ User accounts
  - ☐ Authorization lists
  - ☐ Other employees
- ■ The Security Official creates a document listing each access mechanism and identifying the effect on the level of access the affected individual will have once the mechanism is rendered ineffective. For example, if paper medical records are kept in a locked room, accessible only to individuals who have a certain key or access code, the effect of changing the access code or repossessing the key (or changing the locks) would be to eliminate the individual's access to paper medical records.

3. Schedule for revision/repossession of access controls

- ■ The Security Official creates an action plan for putting the appropriate changes in place with respect to mechanisms maintained by the Practice. The action plan is reviewed with the office administrator or other individual responsible for termination to coordinate timing.

- A list of the items (eg, keys, cards, or tokens) to be recovered from the affected individual upon termination is delivered to the office administrator or other individual responsible for the actual termination of the employee.
- The Security Official takes appropriate steps to implement the action plan.

4. Notification of other employees

- The Security Official prepares a list of key employees to be informed of the termination and its impact on their security obligations, and shares the list with the office administrator or other individual responsible for the termination. The responsible person and the Security Official agrees between them on an appropriate allocation of responsibility for informing the affected employees.
- At the appropriate time, the person responsible for reporting the termination notifies other affected employees of the termination and their responsibility not to provide access to the terminated individual. If notice initially must be provided orally, a written notice is to be distributed as soon as practicable thereafter.

Cross-References

Workforce Security Training, AP8

Internal Sanctions, PP3.6

Administrative Procedures (AP): Internal Audit/Security Incident AP7

Introduction

Once the Practice has Safeguard mechanisms in place to protect PHI and other sensitive information, it will need to monitor the operation and performance of the Safeguards on an on-going basis to ensure that the mechanisms are working to provide adequate protection and to identify potential security violations. The purpose of the monitoring and review is to provide the Practice with a reporting channel and to assign accountability for responding to unauthorized access to PHI.

The audit should employ a review of the records of activity (eg, access logs, file accesses) and any security incidents that arise. If a potential security violation is discovered, the Practice must also have in place policies and procedures for reporting and taking corrective action regarding the breach.

Policy

The Practice will implement procedures for monitoring operations and the performance of Safeguards, and for identifying, reporting, and responding to potential security breaches. In the event of an actual security breach, the Practice will take steps to (a) implement Safeguards to prevent such a breach from occurring in the future, and (b) address any negative effects resulting from the violation.

Scope of Policy

This policy applies to all activity in the Practice that involves access to PHI, and to all personnel who work with or provide support for systems or storage media containing PHI, or who have responsibility for implementing Safeguards.

Procedure for Developing/ Implementing Internal Audits

1. Review Access Activity Records

- The Security Official should identify the reports and other documentation regarding the system generated through normal operations. In addition to such documents, the Security Official should regularly receive the Documentation created specifically for the Safeguards.
- The Security Official reviews or designates an individual to review the records of activity maintained by the Practice. The review should take place on a periodic basis, as determined by the Security Official, but not less than weekly.

- If the volume of Documentation created is so great that the periodic review would place a significant burden on Practice operations, the Security Official should develop a mechanism to review a manageable amount of Documentation. Such mechanisms might include:
  - ☐ In-depth review of specific types of records (eg, access logs) selected at random
  - ☐ Random spot-checks across each type of Documentation

2. Documentation of review

- The Security Official should develop a form (an "Audit Record") for documenting the review that permits the Practice to maintain a record of the relevant information, including the following:
  - ☐ The specific documents reviewed
  - ☐ The portion of documents reviewed, if all documents are not reviewed
  - ☐ The existence and nature of any irregularities identified (eg, inappropriate login station, unidentified access to PHI)
  - ☐ Any pattern or combination of activities that suggests a potential security violation (eg, excessive after-hours logins)
  - ☐ For each activity identified, whether the activity identified in each provision represents a security violation or simply an unusual occurrence
  - ☐ Identifies the individual assigned responsibility for resolving the concern
  - ☐ Action taken to investigate/substantiate concern
  - ☐ Corrective action taken, if any

3. Investigation and reporting

- Any potential security violations or suspicious behavior or activity identified in the document review should be reported immediately to the Security Official.
- If the Security Official and the Privacy Official are not the same person, the Security Official should inform the Privacy Official as soon as possible of any potential security violations that may result or may have resulted in privacy breaches.
- The Security Official should investigate or designate an individual to investigate the circumstances surrounding the potential violation or suspicious activity. The person responsible for the investigation should determine whether the facts and circumstances indicate that a security incident has occurred.
- Where no security incident has occurred, the person responsible for the investigation should document the explanation for the suspicious activity in the Audit Record.
- Where a security incident appears to have occurred, the person responsible for the investigation should initiate the security incident response procedure below.

Procedure for Developing/ Implementing Security Incident Response

1. The Security Official can take the following steps to respond to security incidents. He or she should consider consulting with counsel for the Practice and should also review Internal Sanctions, PP3.6.

- The Security Official should determine whether the security incident involves a violation of one or more of the Practice's policies and procedures relating to Safeguards or simply a breach of security.
- The Security Official should determine the extent of potential exposure to the Practice, individual patients, or PHI of any entities for which the Practice

functions as a Business Associate. Potential risks and exposures might include the following:

- ☐ Improper use or disclosure of PHI
- ☐ Alteration or other corruption of PHI
- ☐ Enhanced penalties/exposure to patients flowing from nature of the PHI (eg, AIDS, mental health, minor, genetic information)
- ☐ Identity theft, credit card fraud, or other crimes associated with patient identity
- ☐ Crimes related to dispensation of controlled substances
- ☐ Reliance by a potential transferee on inaccurate, corrupted, or incomplete information transmitted without authorization

- If appropriate, the Security Official should notify parties affected by the security incident of any definite threats resulting from the incident.
- If the security incident involves a breach of privacy, the Privacy Official should take practicable steps to lessen the effect or harm potentially caused by the breach.
- Where the security incident involves a violation of a Practice policy or procedure, the Security Official should determine the identity of each member of the Practice personnel implicated in the incident. Such individuals should be assigned to remedial training and the Security Official should follow the Practice's policy and procedures for Internal Sanctions, PP3.6, to determine whether additional sanctions should be imposed.
- In all cases, the Security Official should identify and evaluate any and all appropriate measures to prevent similar incidents from occurring in the future or to restore the integrity of data or repair any damage to the Safeguards infrastructure resulting from the security incident.

2. Documentation

- The Security Official should complete the audit record with the nature and timeframe of the corrective actions taken to address the security incident.
- If the corrective actions taken require revisions or additions to the Practice's policies and procedures, the Security Official should attach a copy of the revisions or additions to the Audit Record.
- The Security Official, in consultation with counsel as appropriate, should prepare a report (each a Security Incident Report) for the Practice's governing body regarding the security incident, including anticipated exposure and any corrective action measures taken in response to the incident.
- If appropriate, the Security Official can file a record of actions taken with the Privacy Official under Mitigation, PP3.7.

3. For security incidents identified outside of the audit process, the Security Official should create a Security Incident Report with the following information in addition to the information described for the Audit Record:

- Source of the initial report,
- Date and time of the initial report, and
- Contact information for follow up

Cross-References

Internal Sanctions, PP3.6

Mitigation, PP3.7

Administrative Procedures (AP): Workforce Security Training
AP8

Introduction

All of the Practice's workers should be trained in security policies and procedures through a formal training program. This will enhance compliance with the security regime adopted by the Practice and will minimize the risks of unauthorized access, use, or disclosure of PHI.

Policy

The Practice's policy is to provide training in security policies and procedures adopted by the Practice to all workforce members on a routine basis. Attendance at training is mandatory for all employees and failure to attend training is subject to sanction.

Existing employees shall receive training prior to implementation of the Privacy Rules on April 14, 2003. Employees hired after April 14, 2003, will receive training within a reasonable period after their hiring date. All employees shall receive periodic updates and refresher courses on at least an annual basis.

Definitions

Workforce Security Training: Education in which all employees, agents, and contractors must participate concerning the vulnerabilities of the health information in an entity's possession and ways to ensure the protection of that information. This training should include, based on job responsibilities, customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security.

Password Management: Rules to be followed in creating and changing passwords and the need to keep them confidential.

Virus Protection. Training to enhance user awareness of the potential harm that can be caused by a computer virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected.

Scope of Policy

This policy applies to all workforce members and policies and procedures for providing appropriate safeguards for PHI implemented by the Practice.

Procedure for Implementing Workforce Security Training

The Privacy Official shall organize and supervise workforce security training that covers the following implementation features:

1. Awareness training for all personnel, including management personnel, in security awareness, to include (but not be limited to):
   - Password maintenance;
   - Incident reporting; and
   - Viruses and other forms of malicious software.
2. Periodic security reminders to employees, agents, and contractors.
3. User education concerning virus protection.
4. User education in importance of monitoring log-in success or failure and how to report discrepancies.
5. User education in password management.

Cross-References

Security Management Process, AP2

Access Control/Personnel Security/Termination Procedures, AP6

Physical Access Controls, PS3

Workstation Policy and Guidelines, PS4

Data Integrity Controls, TS1

Computer Access, Audit, and Authorization Controls, TS2

Data and Entity Authentication, TS3

Workforce Training, PP3.5

Safeguards, PP3.10

Administrative Procedures (AP): Common Sense Protections
AP9

Introduction

Covered entities may make disclosures of PHI that occur incident to other uses and disclosures permitted by the Privacy Rule. However, to avoid violating the Privacy Rule, a Covered Entity must (a) comply with the Minimum Necessary requirement (see PP1.13, Minimum Necessary), and (b) implement reasonable Safeguards to protect PHI against unnecessary access or disclosure. These provisions facilitate accurate, timely, and appropriate transmission of PHI to facilitate treatment, payment, or health care operations, and likely will cover many measures implemented by health providers, health insurers, and others who have compliance responsibilities under the law.

Policy

The Practice will implement common sense measures to provide reasonable Safeguards for PHI disclosed incident to a permitted use or disclosure.

Scope of Policy

This policy applies to all uses and disclosures of PHI, both within the Practice and to an individual or entity outside the Practice, that could result in an unintended disclosure of PHI to a third party. For example, the following is a nonexclusive list of practices that should comply with this policy:

- Use of non-private telephones,
- Public address systems,
- Conversations among health care professionals, and
- Posting of patient charts outside of exam rooms.

Procedure for Identifying Common Sense Protections

The Practice should identify circumstances likely to be encountered by physicians and other Practice staff on a routine basis that may involve risk of indirect and unintentional use or disclosure of PHI by persons, including Practice employees, who do not have any reason to know about the particular PHI. For example, oral communications to colleagues or patients may be overheard, and whiteboards used to identify exam room status may be observed, by other individuals in the same area.

These situations require evaluation to determine whether simple actions or policies can reduce the potential exposure of PHI. In determining which protections to apply, the Practice should take care that the protections do not impede delivery of care. For example, talking in low voices with patients may be a sensible precaution in communications to patients with normal hearing; however, that approach may not be appropriate for a patient with hearing loss.

The protections that the Practice selects should be documented and included in the training provided to Practice personnel, as appropriate.

The following are some examples of potential common sense protections that the Practice may wish to adopt for the identified areas:

Protections for Oral Communications

- Speak quietly
- Limit the amount of information disclosed
- Be aware of the proximity of others—stand out of hearing range
- Request patients to report to a specific location or individual for more information when contacting patients over a public address system

Protections for Visual Displays	■ Restrict access to areas containing visual displays ■ Face visual displays away from hallways or other high-traffic areas ■ Escort all non-Practice personnel in areas containing visual displays
Protections for Clinic Operations Practices	■ Limit information available on sign-in sheets to that necessary to sign in and no more ■ Face charts left outside of exam rooms away from the wall
Structural Protections	■ Isolate or lock file cabinets and record rooms containing PHI ■ Use dividers, cubicles, curtains, or other barriers in areas of multiple patient-staff communications
Patient Communications	■ Limit the content of messages left on answering machines or with family members ■ Respect patient requests for alternative methods of contact and communication ■ Place postcards with PHI in envelopes to prevent unnecessary disclosure
Cross-References	Safeguards Documentation, AP1 Workforce Security Training, AP8 Incidental Disclosures, PP1.7 Minimum Necessary, PP1.13

PRIVACY MANAGEMENT: SAFEGUARDS PP3.10

Physical Security (PS)

Introduction

Physical security involves the safeguards designed to protect the physical computer systems and related equipment from hazards as well as intrusion.

Index of Physical Security Procedures:

Policy/Procedure	Title	Page No.
PS1	Assigned Security Responsibility	361
PS2	Media Controls (paper and electronic)	362
PS3	Physical Access Controls (physical and electronic)	365
PS4	Workstation Policy and Guidelines	368

Physical Security (PS): Assigned Security Responsibility PS1

Introduction

The Practice will need to identify an individual or group of individuals to manage and supervise the execution and use of security measures to protect PHI and to manage and supervise the conduct of personnel as their activities relate to the Safeguards or the protection of PHI.

Policy

It is our policy to designate a single individual or organization to be responsible for the practices, procedures, technology, and other measures used to protect PHI. Unless another individual is designated specifically for this purpose, the Privacy Official shall be responsible for supervising and managing security measures for PHI used within the Practice and PHI received from or disclosed to persons or organizations outside of the Practice.

Scope of Policy

This policy covers responsibility for security of all PHI created, received, used, or maintained by the Practice. Once the responsibility has been allocated, it should be documented in a contract, job description, board resolution, or other appropriate written form.

Procedure for Developing/ Implementing Policy

1. Representatives of the Practice should determine how allocation of responsibility for security can best be accomplished within the Practice's administrative and governance structure. Allocation of responsibility may require action by executive staff (eg, president, CEO, COO) or a governing body (eg, Executive Committee, Board of Directors). In many cases, it will make sense for the Privacy Official to serve as the Security Official.
2. The Privacy Official (together with any other responsible party) develops a work plan with specific objectives for complying with the Safeguard requirements within the required timeframe.
3. The appropriate body or individual within the Practice develops a job description or specifications for the Security Official position that incorporates the benchmarks and goals in the work plan.
4. The work plan and job description should be approved by the appropriate executive or governing body of the Practice.
5. Once the Security Official is designated, the Privacy Official implements the Practice's decision by establishing a chain of authority and reporting responsibility through senior management.

Procedure If the Security Official Is Not the Privacy Official

If the Security Official will be someone other than the Privacy Official, the Practice may use specific steps in selecting an entity or individual to be responsible for Safeguards. The following steps may be added between Steps 1 and 2 noted above:

1. Either the Board or the appropriate executive (eg, Privacy Official) identifies possible individuals (eg, COO, CIO, consultant), or organizations (eg, consultant, Board committee) to be responsible for security measures. In selecting an individual to serve as Security Official, responsible individuals within the Practice may wish to utilize several criteria, which may include any or all of the following:
   - Demonstrated experience in supervision and management of employees and other personnel
   - Knowledge/experience in managing electronic data systems
   - Experience with confidential situations
   - Law enforcement or other security-related experience
   - Status or position that can help provide focus and highlight importance
   - Capacity to accept new responsibilities/possibility of reallocating existing responsibilities
   - Practice's need to spread responsibility across multiple persons
   - Background check or references (if desired, or required by state law for persons dealing with sensitive information)
2. For individuals or entities outside the Practice, the Privacy Official interviews candidates or issues a Request for Proposals (RFP) to competing vendors.
3. The Privacy Official evaluates candidates or vendor submissions and selects a person, group of persons, or an entity to be responsible for Practice security. Where appropriate, the Privacy Official obtains the approval of executive officers or the governing board of the Practice.

Acknowledgment by Security Official

I, _____, hereby acknowledge my appointment as Security Official of _____ [Name of Practice]. I understand my responsibilities include developing and implementing reasonably appropriate Safeguards to protect PHI for the Practice. I have read and agree to the Practice's Privacy Policies and Procedures, including Safeguards, PP3.10.

_____ _____

Signature Date

Physical Security (PS): Media Controls PS2

Introduction

Developing and applying documented policies and procedures that govern the receipt and removal of data storage mechanisms (eg, computer hardware and software, file cabinets) into and out of its facilities can help the Practice to enhance its control over and prevent tampering with or unauthorized access to places where PHI is stored.

Policy

All devices and units used for storing PHI shall be received, maintained, and removed in the manner set forth in the Practice Media Control procedures in coordination with the assigned responsibility for security within the Practice. Practice workforce members who access, backup, store, and dispose of PHI will be responsible for implementing the Media Control procedures. All activities of Practice workforce members that have to do with data storage units and devices must be conducted as required by the Media Control Procedures.

Definitions

See Safeguards in the Glossary.

Scope of Policy

This policy applies to all storage, maintenance, acquisition, and use of computer hardware, servers, file cabinets, and other data storage devices (including software programs) that are (a) controlled and managed by the Practice, and (b) used for storing PHI. This policy also applies to any situation where storage media must be brought into, removed from, or moved within the Practice, such as internal reorganizations.

Procedure for Developing/ Implementing Media Controls

The following steps should assist the Practice to develop Media Control procedures that reflect its business needs and operations:

1. Provide for access control.

- Security Official identifies and labels media (eg, paper, diskettes), equipment (eg, file cabinets, servers, handheld devices), and locations where PHI used within the Practice currently is kept. Such information may include:
  - ☐ Paper or electronic medical records
  - ☐ Paper or electronic claims and billing records
  - ☐ Paper or electronic patient information

  The media and equipment may be located on or off-site.
  - ☐ Security Official identifies individuals within the Practice and any technical support, off-site facility maintenance or other vendor personnel who need to have access to the media or equipment for business reasons. For each individual, the Security Official must determine the level of access to the media, equipment, or locations required to perform his or her job duties.
  - ☐ The Security Official should classify each individual requiring access according to his or her role within the Practice.
  - ☐ Based on the classification of employees and the levels of access required, the Security Official should determine which individuals require access to each specific type of information storage unit or device.
  - ☐ The Security Official should develop policies to control access to storage equipment by limiting those workforce members with access to each unit or device to those who have reason to do so, and limiting the circumstances under which they may obtain access, and the extent of the access they require. Where necessary and appropriate, these policies should be approved by other Practice representatives prior to distribution to the workforce members.
  - ☐ Access Control Policy may utilize one or more of the following mechanisms to accomplish the limitation of access:
    - Locked rooms, suites, cabinets, and cages with restricted distribution of keys or access codes based on position and need to accessed
    - Use of timers to restrict hours during which material may be accessed
    - Supervised access, where another person must be present to provide access to units or devices
    - Locks, password protections, and other mechanisms for securing laptops and workstations, and preventing unauthorized access to hard drives
    - Prohibiting use of mobile storage media (eg, palm computers, laptops, diskettes) within the Practice unless directly obtained and approved by the Practice
    - Restricting those with authority to download information to mobile devices

2. Maintain accountability by establishing mechanisms to ensure that access and activity related to data storage media, units, equipment, and locations that appear to be authorized by the Practice are in fact authorized. Such mechanisms might include:

- Access logs
- Double-key access
- Biometric or other unique identifier access
- Periodic audits
- Prohibition of home or remote use of Practice equipment or media (location-based access/use)
- Restricted authority for creating duplicate data in any media
- Established approval channels for data storage-related requests

3. Create a regular data backup protocol.

- Security Official identifies types of data routinely created and used by the Practice.
- Security Official identifies data that the Practice must maintain for business reasons or that is required by law or regulation.
- Security Official develops a schedule for creating copies of data that the Practice needs to maintain for business, legal, or regulatory reasons. In creating the schedule, the Security Official may wish to perform a cost-benefit analysis that evaluates the following points:
  - ☐ Multiple sources containing the same or similar data
  - ☐ Ease of reproducing specific sets of data
  - ☐ Cost of reproducing specific sets of data
  - ☐ Possibility of reproducing an existing data set from other sources
  - ☐ Cost of reproducing data versus cost of data backup

4. Provide for secure, organized data storage.

- Security Official identifies media, equipment, and locations used for storing data as in Step 1, and identifies the specific types of data stored on media, equipment, and locations.
- Security Official evaluates physical location and building access and makes an assessment of threats or vulnerabilities.
- Security Official evaluates security measures currently in place to protect media, equipment, and locations involved in data storage from unauthorized access, tampering, or removal.
- Based on identification of risks and exposure related to data storage, Security Official develops records storage plan that may involve relocating storage of specific data sets for more effective organization or to improve the Practice's ability to limit access to appropriate workforce members.
- The security plan also should address vulnerable areas of the Practice's storage methods. The data storage plan should increase the security of data stored by the Practice by using effective methods, which may include one or more of the elements described in Steps 1 and 2 of this procedure.

5. Create a secure disposal regime.

- Security Official evaluates existing disposal mechanisms for PHI and other sensitive data stored by the Practice and makes an assessment of potential vulnerabilities.
- Security Official reviews the Practice's document retention policy to identify appropriate data disposal intervals.

- The Security Official makes determinations about effective ways to address final disposal of paper and electronic records containing sensitive information. A disposal regime may include one or more of the following types of options:
  - ☐ Assigning responsibility for data disposal to a specific, identified individual or organization
  - ☐ Establishing a rotating periodic disposal schedule to dispose of information at regular but not uniform intervals
  - ☐ Requiring supervised access to data storage for data destruction personnel
  - ☐ Destroying rather than recycling data storage equipment

Cross-References

Documentation, AP1

Security Management Process, AP2

Contingency Plans, AP4

Access Control/Personnel Security/Termination, AP6

Physical Access Controls, PS3

Workstation Policy and Guidelines, PS4

Physical Security (PS): Physical Access Controls PS3

Introduction

The Practice should have documented policies and procedures to limit unauthorized physical access to the Practice without unduly restricting authorized access.

Policy

Our policy is to permit only patients, employees, and others with a legitimate business or treatment purpose on Practice premises. Employees and other workforce members must abide by restrictions on access to Practice facilities by unauthorized persons and must keep doors and windows locked and take other steps required to maintain the security of Practice facilities.

Scope of Policy

This policy applies to all individuals on the premises of the Practice and governs the conduct of all individuals who are representatives of the Practice by virtue of an employment or contract relationship with respect to patients and other visitors to the Practice.

Procedure for Developing/ Implementing Physical Access Controls

The Practice should use the procedures described below to develop and implement Physical Access Controls with the following implementation features:

- A Disaster Recovery system
- Provide for emergency mode operation
- Provide for equipment control, into and out of site
- A facility security plan
- Procedures for verifying access authorizations before granting physical access
- A system to organize and review maintenance records
- Need-to-know procedures
- Formal, documented procedures to sign in visitors and provide escorts, if appropriate
- Testing and revision protocols
- All references to the "Security Official" reflect his or her primary responsibility for developing and implementing these policies and procedures but also include other representatives of the Practice whose input may be necessary or desirable in that process

Procedure for Creating a Disaster Recovery System and Providing for Emergency Mode Operation

The majority of the procedures for developing Disaster Recovery and Emergency Mode Operations will be performed in connection with the development of contingency plans under procedure AP4. The Security Official may use the following steps to develop procedures specific to physical access to materials, which should be incorporated into the Practice's overall contingency and emergency operations plans:

- For each type of potential disaster, the Security Official identifies the direct effects on the security of all media, storage, and access to information.
- For each type of disaster, the Security Official develops mechanisms to provide for alternative access, including physical access to critical information for all periods in which the usual and customary source of information is not available.
- In addition to developing alternatives, the Security Official identifies actions needed to (a) prevent damage to data in a disaster; and (b) maintain or minimize the effect upon protections for data resources that restrict physical access. Such tasks should be assigned to specific individuals within the Practice.
- For each record used in the Practice, the Security Official must develop a Data Recovery Plan that contains access controls and other Safeguards to prevent unauthorized use or disclosure of the records being reconstructed.
- The Security Official should investigate Disaster Recovery specialists, issue an RFP for Disaster Recovery plans, and select a vendor for Disaster Recovery services.
- The Security Official evaluates vendor submissions and selects an entity to be responsible for Practice security.
- The Security Official contracts with the vendor for Disaster Recovery services. The contract should include appropriate Business Associate and security provisions.
- The Security Official tests the disaster and emergency operations plan for each critical data source.

Procedure for Developing a Facility Security Plan

- Security Official evaluates physical location and building access and makes an assessment of threats or vulnerabilities. See Media Controls.
- Security Official evaluates security measures currently in place to protect building from unauthorized access, tampering, or removal.
- Based on identification of risks and exposure related to facility access, Security Official develops a facility security plan that may involve one or more of the following elements:
  - ☐ Limits hours or means of access to the facility to appropriate workforce members
  - ☐ Addresses vulnerable areas of the Practice's storage methods or operations

Procedure for Creating Processes to Verify Access Authorizations Before Granting Physical Access

- Security Official evaluates existing circumstances for granting physical access, including purposes, physical environments to which access is granted, and security measures in place.
- Security Official identifies situations under which physical access to facilities may be granted.
- Security Official evaluates and implements access controls that may include use of one or more of the following:
  - ☐ Telephone verification
  - ☐ Advance documentation of credentials
  - ☐ Advance notice and registration requirements for access by non-Practice personnel
  - ☐ Physical escorts (supervised access) for non-Practice personnel and workforce members, where required

Procedure for Developing a System to Organize and Review Maintenance Records

- Security Official reviews existing forms of maintenance documentation developed and maintained by the Practice and/or Practice vendors.
- Security Official reviews or arranges for legal review of contracts with vendors to determine whether Practice has appropriate access to maintenance records.
- In coordination with efforts to control access to storage media under PS2, the Security Official should develop a policy that all maintenance documentation be delivered to his or her office for storage.
- Security Official identifies an appropriate period for review of documentation and an individual to conduct a periodic review of maintenance records.
- Responsibility for the periodic review should be added to the identified individual's job description, which should require that a written report of the results of each review be provided to the Security Official. This step may require action of governing or executive members of the Practice.

Procedure for Instituting Need-To-Know Access

- Security Official develops policy requiring individuals to demonstrate a need for Practice operations purposes to access information or areas where information is stored.
- This policy should be developed and implemented in coordination with Steps 1 and 2 of PS2.

Note

Compliance with this policy's requirements is important for the Practice's obligation to institute appropriate Safeguards to avoid incidental disclosures.

Procedure for Creating Testing and Revision Protocols

- Security Official develops outcome measures for testing, including mastery by individual workforce members.
- Security Official works with Practice personnel to establish a schedule for testing policies and procedures on a regular basis.
- Following testing, participants provide feedback to the Security Official.
- Security Official evaluates the test outcomes and feedback and makes appropriate revisions to the policies and procedures.
- Practice representatives distribute revised written policies to workforce.
- Security Official provides training to workforce members regarding compliance with policies.

Cross-References

Formalized Record Processing, AP5

Access Control/Personnel Security/Termination, AP6

Verification, PP1.12

Documentation, PP3.4

Workforce Security Training, PP3.5

Physical Security (PS): Workstation Policy and Guidelines
PS4

Introduction

Documented instructions and procedures specifying the physical surroundings for an individual computer terminal site based on the information accessed from that site and describing the type and manner of functions authorized to be performed on that terminal will assist the Practice in avoiding unauthorized access or inadvertent disclosure of PHI.

Policy

Individual computer workstations within the Practice where access to PHI is permitted, and computer display screens, shall be positioned to avoid permitting information on the screen to be displayed.

Definitions

See Safeguards in the Glossary.

Scope of Policy

Applies to any and all individuals who have physical or electronic access to the Practice's computer workstations.

Procedure for Developing/ Implementing Workstation Policies and Guidelines

The Practice shall develop policies and guidelines for workstation use to maintain secure workstations using the steps described in the procedures below.

Procedure for Developing a Policy and Guidelines on Workstation Use

- The Security Official reviews each workstation for its usual use and the sensitivity of the information stored on or accessible from the terminal.
- The Security Official evaluates whether each workstation that uses or has access to sensitive information fulfills a necessary business purpose within the Practice, and evaluates any alternatives to workstation access. Such alternatives might include:
  - ☐ Restricting access by date/time of access, or workforce member position or function within the Practice
  - ☐ Limiting amount of sensitive data that a user can access through a particular terminal
- Security Official develops recommended security practices for all workstations to protect against unauthorized access or disclosure of health information. Such practices might include:
  - ☐ Requiring password protected access to all terminals through an initial login process and timed, password protected screensavers
  - ☐ Requiring workforce members to log off before leaving a terminal unattended
  - ☐ Requiring workforce members to close or put away documents or files containing sensitive information within view when leaving the workstation
  - ☐ Requiring workforce members to keep paper records with sensitive information in locked drawers at the workstation
  - ☐ Prohibiting transfer of user IDs and passwords
  - ☐ Prohibiting access to hacker Web sites from Practice terminals.
- Where it is not possible to provide a secure environment for workstations, or where otherwise appropriate, the Security Official develops additional security practices or precautions at specific workstations. Such additional requirements may include:
  - ☐ Disconnecting specific terminals from the Internet
  - ☐ Disconnecting specific terminals from access to sensitive data not required for a Practice business purpose
  - ☐ Restricting the types of activities that can be performed at a specific terminal
  - ☐ Limiting access to the terminal to persons who have a legitimate need for access to accomplish a Practice business purpose

Procedure for Providing Secure Workstation Locations

- For each workstation within the Practice, the Security Official evaluates the physical location and orientation of the terminal, monitor, and peripheral equipment. Criteria used in evaluating workstation locations may include the following:
  - ☐ How much sensitive information is accessed or used with the terminal?
  - ☐ How frequently is sensitive information accessed or used with the terminal?
  - ☐ How easily someone not working at the terminal can see information on the monitor screen?
  - ☐ Are the terminal and peripherals for terminal output located in a locked room?
  - ☐ How many people have access to the workstation's physical environment?
  - ☐ How many authorized users need to use the terminal? For what purposes?
- Based on the evaluation of the location and function of each workstation, the Security Official determines whether any changes in the physical environment of each computer terminal would enhance the security of the terminal or of the data accessed by the terminal. The Security Official should consider the media controls and other access limitations in making a determination to change the physical environment of a workstation.
- If the Security Official believes that changes to enhance workstation security are advisable, he or she must identify and implement reasonable and practical adjustments to enhance security. The assessment of reasonable and practical alternatives may include an analysis of the amount of additional protection the change would provide versus the cost of the change.
- The Security Official may implement reasonable, cost-effective adjustments to the security of workstations, such as the following:
  - ☐ Locking rooms where terminals and peripherals connected to or used with sensitive data are stored
  - ☐ Moving terminals and peripherals to fully enclosed, locked spaces
  - ☐ Erecting dividers or screens to prevent inadvertent exposure of sensitive data on monitors
  - ☐ Restricting the types of information that can be accessed from a specific machine

Cross-References

Access Control/Personnel Security/Termination, AP6

Workforce Security Training, AP8

Physical Access Controls, PS3

PRIVACY MANAGEMENT: SAFEGUARDS PP3.10

Technical Security (TS)

Introduction

Technical security covers (i) the processes to protect information and to control individual access to information; and (ii) the processes put in place to guard against unauthorized access to data in network transmission.

Index of Technical Security Procedures

Policy/Procedure	Title	Page No.
TS1	Data Integrity Controls	371
TS2	Computer Access, Audit, and Authorization Controls	372
TS3	Data and Entity Authentication	375

Technical Security (TS): Data Integrity Controls TS1

Introduction

To maintain the security of sensitive information transmitted or received using communications networks, the Practice should evaluate and develop or acquire mechanisms for implementing technical security protections relating to data integrity, message authentication, access controls or encryption, and network controls.

> Note
>
> A large, networked system is likely to require higher levels of integrity and access controls, more advanced message authentication, and more complex audit, event reporting and authentication features to match the larger institution's network systems. Encryption also may be required.

Policy

The Practice will adopt and maintain technical security mechanisms to protect data against unauthorized access or alteration when transmitted over the communications networks used in normal operations. All Practice workforce members should use the technical security mechanisms implemented by the Practice appropriately consistent with their positions and responsibilities. Misuse or failure to use the technical security mechanisms will be subject to discipline under Practice policies and procedures.

Definitions

See Safeguards in the Glossary.

Scope of Policy

Technical security mechanisms should be implemented in all situations involving transmission or receipt of PHI in an electronic format over a communications network. Appropriate technical security mechanisms will depend on the types of IT employed within the Practice and the purposes for which the technology is used.

Procedure for Developing/ Implementing Technical Security Mechanisms

1. Network inventory and classification

- The Security Official works with the Practice representative in charge of IT to review the Practice's use of any communication networks, the extent of access individual Practice workforce members have to such networks, and the amount of information received, used, or stored by the Practice that is accessible (during transmission or otherwise) to users of that network.
- The Security Official should classify networks as open or limited access based on the number of users that are not otherwise affiliated with the Practice, the set of potential access points, and the restrictions placed on access through those points.

- Access to networks that are not necessary for a legitimate business function of the Practice should be terminated.

2. Development/identification of security mechanisms
   - Once the network(s) and data use patterns are identified, the Security Official should use the process for developing data integrity measures for data transmitted on the network(s) described in Step 1 of TS3.
   - In the network setting, a message authentication code may be a mandatory implementation measure.
3. Data access and integrity controls
   - Where the Security Official has identified use of open networks in pursuit of a legitimate Practice business function, he or she should review available software for encrypting transmissions on any such open networks.
   - Access controls should be in place to prevent unauthorized network users from accessing sensitive information stored by the Practice.
4. Network control features: For all networks (open, private, vendor-supplied [value-added or VAN]), the Security Official should work with the Practice's IT representative to review available products and implement the following controls:
   - Alarm
   - Audit trail
   - Entity authentication
   - Event reporting
5. Monitoring and education: The Security Official also should develop instructions and assign responsibility for monitoring of system outputs and security alerts, as well as the steps to be taken in the event of specific types of alerts.

Cross-References

Documentation, AP1

Formalized Record Processing, AP4

Access Control/Personnel Security/Termination, AP5

Workforce Security Training, AP8

Physical Access Controls, PS3

Data and Entity Authentication, TS3

Verification, PP1.12

Internal Sanctions, PP3.6

Technical Security (TS): Computer Access, Audit, and Authorization Controls TS2

Introduction

Policies and procedures that protect information and control individual access to information, including access controls, audit controls, authorization controls, data authentication, and entity authentication can be very effective components of the Practice's appropriate Safeguards.

Policy

The Practice will implement technological mechanisms to minimize unauthorized access to or alteration of sensitive information that is used, stored, or received in electronic form. All Practice workforce members will be required to comply with the access and usage policies and procedures implemented by the Practice. Failure to meet the standards of behavior established by the policies and procedures will result in disciplinary action.

Definitions

See Safeguards in the Glossary.

Scope of Policy

Access controls must be applied to all situations in which the Practice stores PHI in an electronic format. Appropriate access controls will depend on the types of IT employed within the Practice and the purpose(s) for which each technology is used. A large, networked system is likely to require more sophisticated access controls, in line with the increased number of users.

Procedure for Developing/ Implementing Computer Controls

1. Emergency Access: As part of the Practice's efforts to create Disaster Recovery and emergency operations procedures and using the same steps described in PS3, the Security Official should work with other Practice representatives to develop ways of accessing information the Practice needs to operate in the event of and during a disaster or emergency. At least two individuals should be designated to have the capability and responsibility to provide emergency access for the Practice.

2. Access and Authorization Controls

- Security Official reviews how the Practice's business operates to determine the types of information that members of the Practice's workforce need to have to do their jobs.
- Security Official evaluates the Practice's information access needs and determines the best way to make sure that workforce members have access only to the information they need to meet their responsibilities. In performing this evaluation, the Security Official should make his or her efforts consistent with the Practice's procedures to implement the Minimum Necessary, PP1.13, standard for disclosures within the Practice. The Security Official should make information available to workforce members based on one or more of the following criteria:
  - Context: The circumstances in which a workforce member seeks to access information controls whether he or she can obtain access. For example, a physician may obtain more medical information about a patient from a workstation in a procedure suite than in the reception area.
  - Role: Access is granted based on the function the workforce member performs for the Practice. Access would be available to all individuals who serve the same function. For example, physicians would be able to access patients' medical records, but receptionists would not have such access. This type of access restriction may be particularly important for the Minimum Necessary standard.
  - User: Access is provided based on a workforce member's specific identity (eg, a user identification, password).

    For example, Dr A would have access to information about all of Dr A's patients but none of Dr B's patients.

  These mechanisms may be used individually or in different combinations. In a small practice, user-based access (user identification and password) may be all that is necessary. Combining two or more of these mechanism likely may be more expensive, but could also provide more security or improve the Practice's ability to serve patients.

  For example, where Dr B is ill or away from the office and Dr A is covering for her, a system that combined user and context-based access could enhance patient care by permitting Dr A to access Dr B's patients' records when Dr B's absence is entered into the system. Adding a role-based access mechanism such as requiring an administrator to enter Dr B's absence into the system could provide additional security for Dr B's patients' records.

- Where changes to current operations would be necessary, the Security Official consults IT specialists to determine how to implement the controls and whether additional software, hardware, customization, or physical location of resources may be required. In most cases, the Practice will need to rely on vendors to make security enhancements to the systems each vendor supplies.
- The Security Official should be aware of the security features of similar products on the market to determine whether security issues can be more effectively addressed by changing products. A practice is not required to make a change in software or other vendor-supplied material simply because it is available. Rather, the Practice should weigh the risks presented by the existing software and the potential benefits and consequences of making a change to determine the correct course of action. This information should be included in the Security Official's decision about how to implement access controls.
- The Security Official develops policies governing behavior around workstations and other points of access to the information.

3. Encryption

- The Security Official reviews when and how the Practice transmits or receives PHI in electronic form and evaluates any risk that the information may be intercepted or diverted by unauthorized individuals. An effective evaluation must include identification of the following items:
  - ☐ Use of open networks (eg, the Internet), where individuals who are not the intended recipients can gain access to information;
  - ☐ Points (eg, modems, routers) where information leaves an internal system for another computer or system outside the Practice;
  - ☐ The type of internal network (eg, wireless) and any measures in place to protect others from the network.
- In light of the risks revealed by the evaluation, the Security Official determines whether the Practice should require that some or all transmissions of PHI be encrypted. Encryption would be required for transmission of information over open networks and may be required for certain wireless transmissions, as well.

  For example, the Practice may wish to require encrypted transmissions from handheld computers (eg, Palm, Handspring, Compaq) to the Practice's network, or take steps to increase protection of a wireless network.

4. Implement audit controls

- The Security Official and the representative in charge of computer systems and software for the Practice should review current system configurations and mechanisms for tracking access to and use of networks, workstations, and information. The review should identify whether existing audit methods provide enough information for the Practice to identify suspect access activity, assess how well its security measures are working, and identify potential weaknesses in the design or operation of the system.
- The Security Official and computer systems representative should develop a plan that addresses weaknesses in auditing capabilities and adopt appropriate new steps that strike a reasonable balance between effectiveness and additional burdens and costs regarding memory, data storage, and enforcement requirements.
- In consultation with the computer systems representative, the Security Official should establish periodic reviews of the data generated by the audit system.

- Audit results should be reviewed regularly to identify violations of Practice policy. Individuals responsible for violations revealed by audits should be sanctioned as provided for in Internal Sanctions, P3.6.

Cross-References

Documentation, AP1

Formalized Record Processing, AP4

Information Access Control, AP5

Workforce Security Training, AP8

Physical Access Controls, PS3

Verification, PP1.12

Internal Sanctions, PP3.6

Technical Security (TS): Data and Entity Authentication
TS3

Introduction

The Practice must take reasonable measures to verify that the data it reads and maintains has not been altered in an unauthorized manner, and verify the identity and authority of individuals and entities who create and receive the data.

Policy

The Practice will take reasonable steps to implement mechanisms on its systems to establish and verify the identities of users and other individuals who have access to the system. The Practice will also take reasonable steps to prevent unauthorized access or changes to the content of data received or maintained on the system.

Definitions

See Safeguards in the Glossary.

Scope of Policy

Authentication requirements apply to all systems that receive, process, or maintain data in electronic form.

Procedure for Developing/ Implementing Data and Entity Authentication

1. Provide for Data Authentication

- Security Official reviews system configuration to determine the ways that the Practice creates and stores electronic records containing PHI. The Security Official also reviews how and when the Practice transmits PHI electronically to an outside entity, or receives PHI electronically from a third party.
- Based on the data use survey, the Security Official determines the Practice's needs for a means of confirming that data has not been accessed or changed in an unauthorized way. To make this determination, the Security Official might consider the following factors:
  - ☐ The volume of information to be authenticated;
  - ☐ The speed required for transmission, access, and authentication; and
  - ☐ The number of third parties who need to touch or access the information.

In light of these factors, the Security Official reviews the available software products on the market to meet the needs of the Practice. Such products should use at least one of the following authentication technologies:

- ☐ The use of a check sum;
- ☐ Double keying;
- ☐ A message authentication code; or
- ☐ Digital signature.

Where necessary, the Security Official may coordinate efforts with trading partners to ensure compatibility of systems for all who require access.

2. Provide for Entity Authentication

- In establishing the Access and Authorization controls described in Steps 2 and 3 in TS2, the Security Official must provide for a mechanism to assign each individual who has access to any of the Practice's computers and electronic data storage systems with a unique user identifier that represents that person within the system. The Security Official must also issue a policy requiring individuals to logoff of terminals or the system at appropriate times specified by the policy (eg, when an employee is leaving their workstation unattended or has finished using their computer for the day). As a backup to these policies, the Security Official must provide for the system to log a user off automatically after an appropriate period of inactivity.
- In addition to the unique identifier and policy regarding automatic logout, the Security Official must provide for a secondary authentication procedure that includes at least one of the following implementation features:
  - ☐ Biometric identification;
  - ☐ Password;
  - ☐ Personal identification number;
  - ☐ Telephone callback procedure; or
  - ☐ A token.

Cross-References

Documentation, AP1

Formalized Record Processing, AP4

Information Access Control, AP5

Workforce Security Training, AP8

Access Controls, PS3

Computer Access, Audit, and Authorization Controls, TS2

Verification, PP1.12

F3.10B

Sample Questionnaire for Safeguards Vendors

(vendors of equipment, software, other products, or services involved in the storage, maintenance, and transmission of PHI)

Inquiry	Notes
■ Identify the features of your product/service that provide protection for health information.	
■ Do you own or lease the server space on which you store data?	
■ What physical protections (eg, locked cages, security personnel, access logs) are provided for your servers/other data storage units?	
■ Does the way your product/service interfaces with our other data storage or processing products (eg, software, hardware) create any potential security threats for our system?	
■ How will using your product/service increase our system's vulnerability to unauthorized access or tampering by outside parties?	
■ How will using your product/service decrease our system's vulnerability to unauthorized access or tampering by outside parties?	
■ What protections will your product/service provide or permit us to implement to protect against unauthorized access or tampering by inside parties?	
■ How much control over the transmission of information does your product/service provide? Specifically, does your product or service record or transmit information relating to user activities automatically, or otherwise without the specific direction of the user?	
■ What, if any, precautions should we consider taking to prevent unauthorized access to or tampering with data as a result of using your product/service?	
■ What training do you provide for your personnel regarding information security? How frequently?	
■ What personnel will have access to data transmitted or stored by the Practice as a result of our use of your product/service? For what purpose(s)?	
■ How will your product/service permit us to identify individuals using or accessing data?	
■ How will your product/service permit us to track activity on our system?	

Inquiry	Notes
■ How will your product/service permit us to track activity on our system?	
■ How will your product/service permit us to identify who has created, accessed, modified, transmitted, or received data?	
■ How will your product/service help us protect data against unauthorized modification when being stored or transmitted?	
■ How will your product/service alert us to an unusual event, condition, or occurrence?	
■ How much knowledge and what type of training is required to utilize (the security features of) your product/service?	
■ What type of access do you require to our systems to implement your product/service? What personnel will have access and for what purpose(s)?	

Safeguards Glossary

Term	Definition
Access Controls	Mechanisms for protecting sensitive communications transmissions over open or private networks so that they cannot easily be intercepted and interpreted by parties other than the intended recipient.
Accountability	The property that ensures that the actions of an entity can be traced uniquely to that entity.
Alarm	Any device that can sense an abnormal condition within the system and provide, either locally or remotely, a signal indicating the presence of the abnormality. The signal may range from a contact closure to a time-phased automatic shutdown and restart cycle.
Audit Controls	Mechanisms employed to record and examine system activity.
Audit Trail	Information regarding activity on the network, which provides the basis for a security audit.
Authorization Control	The mechanism for obtaining consent for the use and disclosure of health information.
Automatic Logoff	A security procedure that causes an electronic session to terminate after a predetermined time of inactivity, such as 15 minutes.
Biometric Identification	An identification system that identifies a human from a measurement of a physical feature or repeatable action of the individual (eg, hand geometry, retinal scan, iris scan, fingerprint patterns, facial characteristics, DNA sequence characteristics, voice prints, and hand-written signature).
Certification	This is the technical evaluation performed as part of, and in support of, the accreditation process that establishes the extent to which a particular computer system or network design and implementation meet a pre-specified set of security requirements. This evaluation may be performed internally or by an external accrediting agency.
Chain of Trust Partner Agreement	A contract between two business partners to exchange data electronically and protect that data.
Context-Based Access	An access control procedure based on the context of a transaction (as opposed to being based on attributes of the initiator or target).
Data Authentication	The corroboration that data has not been altered or destroyed in an unauthorized manner.
Data Backup	A retrievable, exact copy of information.
Data Storage	The retention of health care information pertaining to an individual in any format.
Disaster Recovery	The process enabling an entity to restore any loss of data in the event of fire, vandalism, natural disaster, or system failure.
Disposal	Final disposition of data and/or hardware on which electronic data is stored.
Documentation	Written security plans, rules, procedures, and instructions concerning all components of the Practice's security.
Emergency Access	Documented instructions for obtaining necessary information during a crisis.
Emergency Mode Operation	Access Controls in place that enable an entity to continue to operate in the event of fire, vandalism, natural disaster, or system failure.
Encryption	The process of making sensitive data unintelligible for transmission over unsecured lines with minimal risk of disclosure to individuals who lack the key to unscramble the original message.
Entity	An individual user or other person or entity accessing data.
Entity Authentication	A mechanism to protect data transmissions on communications networks by irrefutably identifying authorized users, programs, and process, and denying access to unauthorized users, programs, and process.

Term	Definition
Equipment Control	Documented security procedures for bringing hardware and software into and out of a facility and for maintaining a record of that equipment. This includes, but is not limited to, the marking, handling, and Disposal of hardware and storage media.
Event Reporting	A network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, such as the completion of a request for information.
Facility Security Plan	A plan to safeguard the premises and building (exterior and interior) from unauthorized physical access and to safeguard the equipment therein from unauthorized physical access, tampering, and theft.
Formal Mechanism for Processing Records	Documentation policies and procedures for the routine, and nonroutine, receipt, manipulation, storage, dissemination, transmission, and/or Disposal of health information.
Incident Procedures	Formal, documented instructions for reporting security breaches, including all of the steps below.
Information Access Control	Formal, documented policies and procedures for granting different levels of access to health care information, including all of the procedural steps listed below.
Integrity Controls	A security mechanism employed to ensure the validity of the information being electronically transmitted or stored.
Internal Audit	In-house review of the records of system activity (such as logins, file accesses, and security incidents) maintained by an organization.
Inventory	Formal, documented identification of hardware and software assets.
Maintenance Records	Documentation of repairs and modifications to the physical components of a facility, such as hardware, software, walls, doors, and locks.
Media Controls	Formal, documented policies and procedures that govern the receipt and removal of hardware/software (such as diskettes and tapes) into and out of a facility, including all of the features below.
Message Authentication	A mechanism, such as a Message Authentication code, designed to ensure that a message received matches the message sent (eg, transmitted over a network).
Need-to-Know Procedures	A security principle stating that a user should have access only to the data he or she needs to perform a particular function.
Password Management	Rules to be followed in creating and changing passwords and the need to keep them confidential.
Personal Identification Number	A number or code assigned to an individual and used to provide verification of identity.
Personnel Security	All personnel who have access to any sensitive information have the required authorities as well as all appropriate clearances, including implementation of the procedural steps below.
Physical Access Control (Limited Access)	Formal, documented policies and procedures to be followed to limit physical access to an entity while ensuring that properly authorized access is allowed. Includes all of the implementation features below.
Policy and Guidelines on Workstation Use	Documented instructions/procedures delineating the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific computer terminal site or type of site, dependent upon the sensitivity of the information accessed from that site.
Regular Security Testing	The process used to determine that the security features of a system are implemented as designed and that they are adequate for a proposed applications environment. Includes hands-on functional testing, penetration testing, and verification.

Term	Definition
Report Procedures	Documented formal mechanism employed to document security incidents.
Response Procedures	Documented formal rules or instructions for actions to be taken as a result of the receipt of a security incident report.
Risk Analysis	A process whereby cost-effective security/control measures may be selected by balancing the costs of various security/control measures against the losses that would be expected if these measures were not in place.
Risk Management	Process of assessing risk, taking steps to reduce risk to an acceptable level, and maintaining that level of risk.
Role-Based Access Control	An alternative to traditional access control models (eg, discretionary or non-discretionary access control policies) that permits the specification and enforcement of enterprise-specific security policies in a way that maps more naturally to an organization's structure and business activities. Rather than attempting to map an organization's Security Policy to a relatively low-level set of technical controls (typically, access control lists), Role-Based Access means that each user is assigned one or more predefined roles, each of which has been assigned the various privileges needed to perform that role.
Sanction Policies and Procedures	Statements regarding disciplinary actions that are communicated to all employees, agents, and contractors.
Secure Workstation Location	Physical Safeguards to eliminate or minimize the possibility of unauthorized access to information; for example, locating a terminal used to access sensitive information in a locked room and restricting access to that room, not placing a terminal used to access patient information in any area of a doctor's office where the screen contents can be viewed from the reception area.
Security Management Process	Creation, administration, and oversight of policies to ensure the prevention, detection, containment, and correction of security breaches involving Risk Analysis and Risk Management.
Security Policy	Statement(s) of information values, protection responsibilities, and organization commitment for a system.
Telephone Callback	A method of authenticating the identity of the receiver and sender of information through a series of "questions" and "answers" sent back and forth establishing the identity of each. For example, when the communicating systems exchange a series of identification codes as part of the initiation of a session to exchange information, or when a host computer disconnects the initial session before the authentication is complete, and the host calls the user back to establish a session at a predetermined telephone number.
Termination Procedures	Formal, documented instructions, which include appropriate security measures for the ending of an employee's employment or an internal/external user's access.
Testing and Revision Protocols	The restriction of program testing and revision to formally authorized personnel.
Token	A physical item that is used to provide identity. Typically an electronic device that can be inserted in a door or a computer system to obtain access.
Unique User Identifier	A combination name/number assigned and maintained in security procedures for identifying and tracking individual user identity.
User-Based Access Control	A security mechanism used to grant users of a system access based upon the identity of the user.
Verifying Access Authorizations	Formal, documented policies and instructions for validating the access privileges of an entity before granting those privileges.

Term	Definition
Virus Checking	The act of running a computer program that identifies and disables (A) another "virus" computer program, typically hidden, that attaches itself to other programs and has the ability to replicate; (B) a code fragment (not an independent program) that reproduces by attaching to another program; or (C) a code embedded within a program that causes a copy of itself to be inserted in one or more other programs.
Virus Protection	Training to enhance user awareness of the potential harm that can be caused by a computer virus, how to prevent the introduction of a virus to a computer system, and what to do if a virus is detected.
Workforce Security Training	Education in which all employees, agents, and contractors must participate concerning the vulnerabilities of health information in an entity's possession and ways to ensure the protection of that information. This training should include, based on job responsibilities, customized education programs that focus on issues regarding use of health information and responsibilities regarding confidentiality and security.

chapter 4

Workforce Training Tips

TRAINING TIPS

Introduction

This chapter provides pointers about conducting training and how your Practice can use this book itself as a training tool.

Remember, even though there are packaged privacy training tools available commercially to help train your Practice's workforce on HIPAA, the Privacy Rule requires that you train your workforce on your Practice's *own* policies and procedures. The Workforce Training Policy and Procedure (PP3.5) provides you with the policies, procedures, and documentation steps required to comply with the Privacy Rule. This chapter gives you some suggestions about how you can more efficiently and effectively meet these training requirements.

Use the Policies and Procedures Documents as Training Materials

It is critical to your compliance effort that your Practice workforce is familiar with and understands your policies and procedures that affect their jobs. We suggest that you use the policies and procedures themselves as training tools. This will save significant time in developing materials for training. In addition, the more your staff reads and reviews these documents, the more likely they will understand what they are required to do.

Here are some tips for using the policies and procedures contained in this book for training:

- Make acetates of each page of a policy and procedure for a training session. Review each page on an overhead projector.
- If your polices and procedures are electronically stored, you can use a computer overhead projector to project the pages of the policies and procedures.
- Show examples of forms that have been completed to help the staff understand how the forms are to be used.

Include a Discussion Component in Training Sessions

Include a discussion session at the end of each training session. Give staff an opportunity to ask questions or comment about how the policy or procedure will be applied in real-life scenarios. Allowing questions and comments will help the trainer to evaluate the staff's understanding of the training content.

Don't Do Too Much, Too Fast

If time allows, try to space out the training over multiple sessions. This will help staff absorb the information in more manageable portions and prevent staff from becoming overwhelmed and discouraged. Consider training on the Phase I Policies and Procedures before training on Phase II.

Keep the Tone Positive

The individuals conducting training should be positive about the implementation of the Privacy Rule requirements. Consider involving staff members in the development and conduct of training sessions to increase buy-in.

Training at Multiple Sites

When a practice operates at multiple physical sites, training can be difficult to coordinate. Consider using teleconferencing or video conferencing to conduct training at multiple sites to avoid travel time and multiple training sessions.

Document Ideas and Issues that are Raised at Training Sessions

Often, questions or comments about a policy or procedure will be raised by staff during training sessions that will raise previously unidentified issues or concerns that must be addressed. Document these concerns so that the Privacy Official can address them at a later time. Because the HIPAA Privacy Rule is new, many questions about how to apply the requirements will arise as the polices and procedures are being implemented.

Encourage Staff to Refer to the Policies and Procedures

Emphasize to the staff that the polices and procedures documents are tools for their use. Make sure everyone knows where copies are located within the Practice. Consider whether smaller subsets of policies and procedures can be maintained by individuals near their work areas if they will be used frequently.

Encourage Staff to Use the Privacy Official as a Resource

There will undoubtedly be questions that arise that are not directly answered by the policies and procedures. Encourage staff to contact the Practice's Privacy Official when they have questions or concerns.

Use Privacy Bulletins

Maintaining privacy awareness is an ongoing task. The Privacy Official may distribute periodic Privacy Bulletins to Practice staff addressing various aspects of privacy compliance. Below are some examples of a what a Privacy Bulletin might contain:

- General reminders about a particular policy or procedure to refresh understanding.
- Examples or clarifications of how specific policies and procedures are to be applied to particular facts.
- Summary of any complaints that have been received with references to applicable policies and procedures.
- Summary privacy topics or events covered in news and periodicals to demonstrate current attitudes toward patient privacy.

appendix B

Crosswalk of Policies and Procedures to Privacy Rule Provisions

Note: Definitions of key terms are defined in the Privacy Rule at §§160.103, 160.202, and 164.501.

Number	Policy/Procedure	Rule Provisions (All citations are to 45 C.F.R. Parts 160 or 164)
	PHI Permissions	
PP1.0	General Policy	
	Permissions	
PP1.1	Required Disclosures	§164.502(a)(2)
PP1.2	Disclosures to the Patient	§164.502(a)(1)(i)
PP1.3	Our Treatment, Payment, Operations	§164.506(c)
PP1.4	Others' Treatment, Payment, Operations	§164.506(c)
PP1.5	Operations of Organized Health Care Arrangement	§164.506(c)
PP1.6	Family, Friends, and Disaster Relief Organizations	§164.510
PP1.7	Incidental Disclosures	§§164.502(b), 164.514(d), 164.530(c)
PP1.8	Public Purpose	§164.512
PP1.9	Authorization	§164.508
PP1.10	De-Identification	§§164.502(d), 164.514(a)-(c)
PP1.11	Limited Data Set	§164.514(3)
	Special Requirements	
PP1.12	Verification	§164.514(h)
PP1.13	Minimum Necessary	§§154.502(b), 154.514(d)
PP1.14	Business Associates	§§164.502(e), 164.504(e), 164.532(d)-(e)
PP1.15	Personal Representatives	§164.502(g)
PP1.16	Marketing	§164.508(a)
PP1.17	Psychotherapy Notes	§164.508(a)
PP1.18	Consistent with Notice of Privacy Practices	§164.502(i)
PP1.19	Consistent with Other Documents	§§164.508, 164.522(a), 164.522(b), 164.526
PP1.20	Consent (State or Other Law)	§160.203

Number	Policy/Procedure	Rule Provisions (All citations are to 45 C.F.R. Parts 160 or 164)
	Patient Rights	
PP2.0	General Policy	§§164.522-164.528, 164.530(d)
PP2.1	Access	§164.524
PP2.2	Amendment	§164.525
PP2.3	Accounting	§164.528
PP2.4	Alternative Communications	§164.522(b)
PP2.5	Further Restrictions	§164.522(a)
PP2.6	Complaints	§164.530(d)
	Privacy Management	
PP3.0	General Policy	§164.530
PP3.1	Privacy Official/Privacy Contact	§164.530(a)
PP3.2	Notice of Privacy Practices—Development and Distribution	§§164.520, 164.530(i)(4)
PP3.3	Policies and Procedures	§164.530(i)
PP3.4	Documentation	§164.530(j)
PP3.5	Workforce Training	§164.530(b)
PP3.6	Internal Sanctions	§164.530(e)
PP3.7	Mitigation	§164.530(f)
PP3.8	No Retaliation	§164.530(g)
PP3.9	No Waiver	§164.530(h)
PP3.10	Safeguards	§154.530(c)

appendix C

Glossary of Selected HIPAA Definitions

This is a glossary of selected HIPAA Definitions from the Privacy Rule. Terms marked by an asterisk (*) are terms as defined by the authors of this book and are not defined terms in the Privacy Rule.

A

Act. Refers to the Social Security Act.

* **Access Request.** See PP2.1.

* **Amendment Request.** See PP2.2.

* **Authorization.** See PP1.9.

B

Business associate. Except as provided in paragraph 2 of this definition, business associate refers to, with respect to a covered entity, a person who:

1. On behalf of such covered entity or of an organized health care arrangement (as defined in §164.501 of this subchapter) in which the covered entity participates, but other than in the capacity of a member of the workforce of such covered entity or arrangement, performs, or assist in the performance of:
   (i) A function or activity involving the use or disclosure of individually identifiable health information, including claims processing or administration, data analysis, processing or administration, utilization review, quality assurance, billing, benefit management, practice management, and repricing; or
   (ii) Any other function or activity regulated by this subchapter; or
   (iii) Provides, other than in the capacity of a member of the workforce of such covered entity, legal actuarial, accounting, consulting, data aggregation (as defined in §164.501 of this subchapter), management, administrative, accreditation, or financial services to or for such covered entity, or to or for an organized health care arrangement in which the covered entity participates, where the provision of the service involves the disclosure of individually identifiable health information from such covered entity or arrangement, or from another business associate of such covered entity or arrangement, to the person.
2. A covered entity participating in an organized health care arrangement that performs a function or activity as described by paragraph (1)(i) of this definition for or on behalf of such organized health care arrangement, or that provides a service as described in paragraph (1)(ii) of this definition to or for such organized health care arrangement, does not, simply through the performance of such function or activity or the provision of such service, become a business associate of other covered entities participating in such organized health care arrangement.
3. A covered entity may be a business associate of another covered entity.

C

Compliance date. Refers to the date by which a covered entity must comply with a standard, implementation specification, requirement, or modification adopted under this subchapter.

Covered entity. Refers to:

1. A health plan.
2. A health care clearinghouse.
3. A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

Covered functions. Refers to those functions of a covered entity the performance of which makes the entity a health plan, health care provider, or health care clearinghouse.

D

Data aggregation. Refers to, with respect to protected health information created or received by a business associate in its capacity as the business associate of a covered entity, the combining of such protected health information by the business associate with the protected health information received by the business associate in its capacity as business associate of another covered entity, to permit data analyses that relate to the health care operations of the respective covered entities.

Designated record set. Refers to:

1. A group of records maintained by or for a covered entity that is:
   (i) The medical records and billing records about individuals maintained by or for a covered health care provider;
   (ii) The enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or
   (iii) Used, in whole or in part, by or for the covered entity to make decisions about individuals.
2. For purposes of this paragraph, the term record means any item, collection, or grouping of information that includes protected health information and is maintained, collected, used, or disseminated by or for a covered entity.

Direct treatment relationship. Refers to a treatment relationship between an individual and a health care provider that is not an indirect treatment relationship.

Disclosure. Refers to the release, transfer, provision of access to, or divulging in any other manner of information outside the entity holding the information.

* **Disclosure Accounting Request.** See PP2.3.

G

Group health plan. (*See also* health plan) Refers to an employee welfare benefit plan (as defined in section 3(1) of the Employee Retirement Income and Security Act of 1974 (ERISA), 29 U.S.C. 1002(1)), including insured and self-insured plans, to the extent that the plan provides medical care (as defined in section 2791(a)(2) of the Public Health Service Act (PHS Act), 42 U.S.C. 300gg-91(a)(2)), including items and services paid for as medical care, to employees or their dependents directly or through insurance, reimbursement, or otherwise, that:

1. Has 50 or more participants (as defined in section 3(7) of ERISA, 29 U.S.C. 1002(7)); or
2. Is administered by an entity other than the employer that established and maintains the plan.

H

HCFA. Refers to the Health Care Financing Administration within the Department of Health and Human Services.

Health care. Refers to the care, services, or supplies related to the health of an individual. Includes, but is not limited to, the following:

1. Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and
2. Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care clearinghouse. Refers to a public or private entity, including a billing service, repricing company, community health management information system, or community health information system, and "value-added" networks and switches, that does either of the following functions:

1. Processes or facilitates the processing of health information received from another entity in a nonstandard format or containing nonstandard data content into standard data elements or a standard transaction.
2. Receives a standard transaction from another entity and processes or facilitates the processing of health information into nonstandard format or nonstandard data content for the receiving entity.

Health care operations. Refers to any of the following activities of the covered entity to the extent that the activities are related to covered functions, and any of the following activities of an organized health care arrangement in which the covered entity participates:

1. Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
2. Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;
3. Underwriting, premium rating, and other activities relating to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of §164.514(g) are met, if applicable.
4. Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;
5. Business planning and development, such as conducting cost-management and planning-related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and
6. Business management and general administrative activities of the entity, including, but not limited to:
   (i) Management activities relating to implementation of and compliance with the requirements of this subchapter;
   (ii) Customer service, including the provision of data analyses for policy holders, plan sponsor, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer;
   (iii) Resolution of internal grievances;
   (iv) Due diligence in connection with the sale or transfer of assets to a potential successor in interest, if the potential successor in interest is a covered entity, or, following completion of the sale or transfer, will become a covered entity; and
   (v) Consistent with the applicable requirements of §164.514, creating de-identified health information, fundraising for the benefit of the covered entity, and marketing for which an individual authorization is not required as described in §164.514(e)(2).

Health care provider. Refers to a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information. Refers to any information, whether oral or recorded in any form or medium, that:

1. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Health insurance issuer. As defined in section 2971(b)(2) of the PHS Act, 42 U.S.C. 300gg-91(b)(2) and used in the definition of health plan in this section, refers to an insurance company, insurance service, or insurance organization (including an HMO) that is licensed to engage in the business of insurance in a state and is subject to state law that regulates insurance. Such term does not include a group health plan.

Health maintenance organization (HMO). As defined in section 2791(b)(3) of the PHS Act, 42 U.S.C. 300gg-91(b)(3) and used in the definition of health plan in this section, refers to a federally qualified HMO, an organization recognized as an HMO under state law, or a similar organization regulated for solvency under state law in the same manner and to the same extent as such an HMO.

Health oversight agency. Refers to an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such public agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is authorized by law to oversee the health care system (whether public or private) or government programs in which health information is necessary to determine eligibility or compliance, or to enforce civil rights laws for which health information is relevant.

Health plan. Refers to an individual or group plan that provides, or pays the cost of, medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).

1. Includes the following, singly or in combination:
   (i) A group health plan, as defined in this section.
   (ii) A health insurance issuer, as defined in this section.
   (iii) An HMO, as defined in this section.
   (iv) Part A or Part B of the Medicare program under title XVIII of the Act.
   (v) The Medicaid program under title XIX of the Act, 42 U.S.C. 1396, et seq.
   (vi) An issuer of a Medicare supplemental policy (as defined in section 1882(g)(1) of the Act, 42 U.S.C. 1395ss(g)(1)).
   (vii) An issuer of a long-term care policy, excluding a nursing home fixed-indemnity policy.
   (viii) An employee welfare benefit plan or any other arrangement that is established or maintained for the purpose of offering or providing health benefits to the employees of two or more employers.
   (ix) The health care program for active military personnel under title 10 of the United States Code.
   (x) The veterans health care program under 38 U.S.C. chapter 17.
   (xi) The Civilian Health and Medical Program of the Uniformed Services (CHAMPUS) (as defined in 10 U.S.C. 1072(4)).
   (xii) The Indian Health Service program under the Indian Health Care Improvement Act, 25 U.S.C. 1601, et seq.
   (xiii) The Federal Employees Health Benefits Program under 5 U.S.C. 8902, et seq.
   (xiv) An approved state child health plan under title XXI of the Act, providing benefits for the child health assistance that meet the requirements of section 2103 of the Act, 42 U.S.C. 1397, et seq.
   (xv) The Medicare Choice program under Part C of title XVIII of the Act, 42 U.S.C. 1395w-21 through 1395w-28.
   (xvi) A high-risk pool that is a mechanism established under state law to provide health insurance coverage or comparable coverage to eligible individuals.
   (xvii) Any other individual or group plan, or combination or individual or group plans, that provides or pays for the cost of medical care (as defined in section 2791(a)(2) of the PHS Act, 42 U.S.C. 300gg-91(a)(2)).
2. Excludes:
   (i) Any policy, plan, or program to the extent that it provides, or pays for the cost of, excepted benefits that are listed in section 2791(c)(1) of the PHS Act, 42 U.S.C. 300gg-91(c)(1); and

(ii) A government-funded program (other than one listed in paragraph (1)(i)–(xvi) of this definition):

(A) Whose principal purpose is other than providing, or paying the cost of, health care; or

(B) Whose principal activity is:

(1) The direct provision of health care to persons; or

(2) The making of grants to fund the direct provision of health care to persons.

I

Implementation specification. Refers to specific requirements or instructions for implementing a standard.

* **Incidental Disclosure.** See PP1.7.

Indirect treatment relationship. Refers to a relationship between an individual and a health care provider in which:

1. The health care provider delivers health care to the individual based on the orders of another health care provider; and
2. The health care provider typically provides services or products, or reports the diagnosis or results associated with the health care, directly to another health care provider, who provides the services or products or reports to the individual.

Individual. Refers to the person who is the subject of protected health information.

Individually identifiable health information. Refers to the information that is a subset of health information, including demographic information collected from an individual; and

1. Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and
2. Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

(i) That identifies the individual; or

(ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Inmate. Refers to a person incarcerated in or otherwise confined to a correctional institution.

L

Law enforcement official. Refers to an officer or employee of any agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, who is empowered by law to:

1. Investigate or conduct an official inquiry into a potential violation of law; or
2. Prosecute or otherwise conduct a criminal, civil, or administrative proceeding arising from an alleged violation of law.

M

Marketing. Refers to making a communication about a product or service, a purpose of which is to encourage recipients of the communication to purchase or use the product or service.

1. Does not include communications that meet the requirement of paragraph 2 of this definition and that are made by a covered entity:

(i) For the purpose of describing the entities participating in a health care provider network or health plan network, or for the purpose of describing if and the extent to which a product or service (or payment for such product or service) is provided by a covered entity or included in a plan of benefits; or

(ii) That are tailored to the circumstances of a particular individual and the communications are:

(A) Made by a health care provider to an individual as part of the treatment of the individual, and for the purpose of furthering the treatment of that individual; or

(B) Made by a health care provider or health plan to an individual in the course of managing the treatment of that individual, or for the purpose of directing or recommending to that individual alternative treatments, therapies, health care providers, or settings of care.

2. A communication described in paragraph (1) of this definition is not included in marketing if:
   (i) The communication is made orally; or
   (ii) The communication is in writing and the covered entity does not receive direct or indirect remuneration from a third party for making the communication.

* **Minimum Necessary.** See PP1.13.

* **Mitigation.** See PP3.7.

O

Organized health care arrangement. Refers to:

1. A clinically integrated care setting in which individuals typically receive health care from more than one health care provider;
2. An organized system of health care in which more than one covered entity participates, and in which the participating covered entities:
   (i) Hold themselves out to the public as participating in a joint arrangement; and
   (ii) Participate in joint activities that include at least one of the following:
      (A) Utilization review, in which health care decisions by participating covered entities are reviewed by other participating covered entities or by a third party on their behalf;
      (B) Quality assessment and improvement activities, in which treatment provided by participating covered entities is assessed by other participating covered entities or by a third party on their behalf; or
      (C) Payment activities, if the financial risk for delivering health care is shared, in part or in whole, by participating covered entities through the joint arrangements and if protected health information created or received by a covered entity is reviewed by other participating covered entities or by a third party on their behalf for the purpose of administering the sharing of financial risk.
3. A group health plan and a health insurance issuer or HMO with respect to such group health plan, but only with respect to protected health information created or received by such health insurance issuer or HMO that relates to individuals who are or who have been participants or beneficiaries in such group health plan;
4. A group health plan and one or more other group health plans each of which are maintained by the same plan sponsor; or
5. The group health plans described in paragraph (4) of this definition and health insurance issuers or HMOs with respect to such group health plans, but only with respect to protected health information created or received by such health insurance issuers or HMOs that relates to individuals who are or have been participants or beneficiaries in any of such group health plans.

P

Payment. Refers to:

1. The activities undertaken by:
   (i) A health plan to obtain premiums or to determine or fulfill its responsibility for coverage and provision of benefits under the health plan; or
   (ii) A covered health care provider or health plan to obtain or provide reimbursement for the provision of health care; and
2. The activities in paragraph (1) of this definition relate to the individual to whom health care is provided and include, but are not limited to:
   (i) Determinations of eligibility or coverage (including coordination of benefits or the determination of cost sharing amounts), and adjudication or subrogation of health benefit claims;
   (ii) Risk adjusting amounts due based on enrollee health status and demographic characteristics;

(iii) Billing, claims management, collection activities, obtaining payment under a contract for reinsurance (including stop-loss insurance and excess of loss insurance), and related health care data processing;

(iv) Review of health care services with respect to medical necessity, coverage under a health plan, appropriateness of care, or justification of charges;

(v) Utilization review activities, including pre-certification and pre-authorization of services, concurrent and retrospective review of services; and

(vi) Disclosure to consumer reporting agencies of any of the following protected health information relating to reimbursement:

(A) Name and address;

(B) Date of birth;

(C) Social security number;

(D) Payment history;

(E) Account number; and

(F) Name and address of health care provider and/or health plan.

* **Permissions.** This is the term the authors use in this book to refer to the various categories of permitted uses and disclosures of Protected Health Information under the Privacy Rule.

* **Personal representative.** See PP1.15.

Plan sponsor. Defined at section 3(16)(B) of ERISA, 29 U.S.C. 1002(16)(B).

Protected health information. Refers to individually identifiable health information:

1. Except as provided in paragraph (2) of this definition, that is:
   (i) Transmitted by electronic media;
   (ii) Maintained in any medium described in the definition of electronic media at §162.103 of this subchapter; or
   (iii) Transmitted or maintained in any other form or medium.
2. Excludes individually identifiable health information in:
   (i) Education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. 1232g; and
   (ii) Records described at 20 U.S.C. 1232g(a)(4)(B)(iv).

Psychotherapy notes. Refers to notes recorded (in any medium) by a health care provider who is a mental health professional documenting or analyzing the contents of a conversation during a private counseling session or a group, joint, or family counseling session and that are separated from the rest of the individual's medical record. Excludes medication prescription and monitoring, counseling session start and stop times, the modalities and frequencies of treatment furnished, results of clinical tests, and any summary of the following items: diagnosis, functional status, the treatment plan, symptoms, prognosis, and progress to date.

Public health authority. Refers to an agency or authority of the United States, a state, a territory, a political subdivision of a state or territory, or an Indian tribe, or a person or entity acting under a grant of authority from or contract with such agency, including the employees or agents of such public agency or its contractors or persons or entities to whom it has granted authority, that is responsible for public health matters as a part of its official mandate.

Q

Qualified Protective Order. Refers to an order of a court or administrative tribunal or a stipulation by the parties to the litigation or administrative proceeding that:

- Prohibits the parties from using or disclosing the PHI for any purposes other than the litigation or proceeding for which the PHI was requested; and
- Requires either the destruction of or the return to the Practice of the PHI, including all copies made, at the end of the litigation or proceeding.

R

Relates to the privacy of individually identifiable health information. Refers to, with respect to a state law, that the state law has the specific purpose of protecting the privacy of health information or affects the privacy of health information in a direct, clear, and substantial way.

Required by law. Refers to a mandate contained in law that compels a covered entity to make a use or disclosure of protected health information and that is enforceable in a court of law. Includes, but is not limited to, court orders and court-ordered warrants; subpoenas or summons issued by a court, grand jury, a governmental or tribal inspector general, or an administrative body authorized to require the production of information; a civil or an authorized investigative demand; Medicare conditions of participation with respect to health care providers participating in the program; and statutes or regulations that require the production of information, including statutes or regulations that require such information if payment is sought under a government program providing public benefits.

Research. Refers to a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

S

Secretary. Refers to the Secretary of Health and Human Services or any other officer or employee of HHS to whom the authority involved has been delegated.

Small health plan. Refers to a health plan with annual receipts of $5 million or less.

* **Special Requirements.** This is the term the authors use in this book to refer to various Privacy Rule restrictions that can apply to a use or disclosure that is otherwise permitted under the Privacy Rule. These restrictions are in addition to the requirements of an applicable Permission.

Standard. Refers to a rule, condition, or requirement:

1. Describing the following information for products, systems, services, or practices:
   (i) Classification of components.
   (ii) Specification of materials, performance, or operations; or
   (iii) Delineation of procedures; or
2. With respect to the privacy of individually identifiable health information.

Standard setting organization (SSO). Refers to an organization accredited by the American National Standards Institute that develops and maintains standards for information transactions or data elements, or any other standard that is necessary for, or will facilitate the implementation of, this part.

State law. Refers to a constitution, statute, regulation, rule, common law, or other state action having the force and effect of law.

T

Trading partner agreement. Refers to an agreement related to the exchange of information in electronic transactions, whether the agreement is distinct or part of a larger agreement, between each party to the agreement. (For example, a trading partner agreement may specify, among other things, the duties and responsibilities of each party to the agreement in conducting a standard transaction.)

Transaction. Refers to the transmission of information between two parties to carry out financial or administrative activities related to health care. It includes the following types of information transmission:

1. Health care claims or equivalent encounter information.
2. Health care payment and remittance advice.
3. Coordination of benefits.
4. Health care claim status.
5. Enrollment and disenrollment in a health plan.
6. Eligibility for a health plan.
7. Health plan premium payments.
8. Referral certification and authorization.
9. First report of injury.
10. Health claims attachments.
11. Other transactions that the Secretary may prescribe by regulation.

Treatment. Refers to the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.

U

Use. Refers to, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

V

* **Verification.** See PP1.12.

W

Workforce. Refers to employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.