Security Policy

Table of Contents

Sparks Family Medicine, LTD/MediTask, LLC/SLMS, LLC
IT Security Policy
Section 100: Introduction
Reviewed: Annually

Approval Date: 08/18/2015 Effective Date: 08/18/2015

101 Purpose
This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at Sparks Family Medicine, LTD, hereinafter, referred to as the Practice. It serves as a central policy document with which all Colleagues must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Practice with policies and guidelines concerning the acceptable use of Practice technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

The policy requirements and restrictions defined in this document shall apply to network infrastructures, databases, external media, encryption, hardcopy reports, films, slides, models, wireless, telecommunication, conversations, and any other methods used to convey knowledge and ideas across all hardware, software, and data transmission mechanisms. This policy must be adhered to by all Practice Colleagues or temporary workers at all locations and by contractors working with the Practice as subcontractors.

103 Scope
This policy document defines common security requirements for all Practice personnel and systems that create, maintain, store, access, process or transmit information. This policy also applies to information resources owned by others, such as contractors of the Practice, entities in the private sector, in cases where Practice has a legal, contractual or fiduciary duty to protect said resources while in Practice custody. In the event of a conflict, the more restrictive measures apply. This policy covers the Practice network system which is comprised of various hardware, software, communication equipment and other devices designed to assist the Practice in the creation, receipt, storage, processing, and transmission of information. This definition includes equipment connected to any Practice domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by the Practice at its office locations or at remote locales.

105 Acronyms/Definitions
Common terms and acronyms that may be used throughout this document:

CEO. The Chief Executive Officer is responsible for the overall privacy and security practices of the company.
CIO. The Chief Information Officer
CMO. The Chief Medical Officer.
CO. The Confidentiality Officer is responsible for annual security training of all staff on confidentiality issues.
CPO. The Chief Privacy Officer is responsible for HIPAA privacy compliance issues.
CST. Confidentiality and Security Team
DoD. Department of Defense
Encryption. The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific 'need to know.'
External Media. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes
FAT or File Allocation Table. The FAT file system is relatively uncomplicated and an ideal format for floppy disks and solid-state memory cards. The most common implementations have a serious drawback in that when files are deleted and new files written to the media, their fragments tend to become scattered over the entire media, making reading and writing a slow process.

Firewall. A dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.
FTP. File Transfer Protocol
HIPAA. Health Insurance Portability and Accountability Act
IT. Information Technology
LAN. Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.
NTFS or New Technology File Systems. NTFS has improved support for metadata and the use of advanced data structures to improve performance, reliability, and disk space utilization plus additional extensions such as security access control lists and file system journaling. The exact specification is a trade secret of Microsoft.
SOW or Statement of Work. An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.
User. Any person authorized to access an information resource.
Privileged Users. System administrators and others specifically identified and authorized by Practice management.
Users with edit/update capabilities. Individuals who are permitted, based on job assignment, to add, delete, or change records in a database**.**
Users with inquiry (read only) capabilities. Individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.
VLAN or Virtual Local Area Network. A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.
VPN or Virtual Private Network. Provides a secure passage through the public Internet.
WAN or Wide Area Network. A computer network that enables communication across a broad area, i.e. regional, national.
Virus. A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

107 Applicable Statutes/Regulations
The following is a list of the various agencies/organizations whose laws, mandates, and regulations were incorporated into the various policy statements included in this document.

National Learning Consortium

Each of the policies defined in this document is applicable to the task being performed – not just to specific departments or job titles.

109 Privacy Officer
The Practice has established a Privacy Officer as required by HIPAA. This Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of the Practice privacy policies in accordance with applicable federal and state laws. The current Privacy Officer for the Practice is:

Brett Sparks, 702-722-2200

111 Confidentiality/Security Team (CST)
The Practice has established a Confidentiality/Security Team made up of key personnel whose responsibility it is to identify areas of concern within the Practice and act as the first line of defense in enhancing the appropriate security posture.

All members identified within this policy are assigned to their positions by the CEO. The term of each member assigned is at the discretion of the CEO, but generally it is expected that the term will be one year. Members for each year will be assigned at the first meeting of the Quality Council in a new calendar year. This committee will consist of the positions within the Practice most responsible for the overall

security policy planning of the organization- the CEO, PO, CMO, ISO, and the CIO (where applicable). The current members of the CST are:

Brett Sparks
Sally Lawrence
Christina Vasquez

If necessary, the CST will meet quarterly to discuss security issues and to review any concerns that arose during the quarter. The CST will identify areas that should be addressed during annual training and review/update security policies as necessary.

The CST will address security issues as they arise and recommend and approve immediate security actions to be undertaken. It is the responsibility of the CST to identify areas of concern within the Practice and act as the first line of defense in enhancing the security posture of the Practice.

The CST is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and recommendations for personnel actions, if appropriate. This log will be reviewed during the quarterly meetings.

The Privacy Officer (PO) or other assigned personnel is responsible for maintaining a log of security enhancements and features that have been implemented to further protect all sensitive information and assets held by the Practice. This log will also be reviewed during the quarterly meetings.

Sparks Family Medicine, LTD/MediTask, LLC/SLMS, LLC
IT Security Policy
Section 200: Employee Responsibilities
Reviewed: Annually

Approval Date: 08/18/2015 Effective Date: 08/18/2015

201 Employee Requirements
The first line of defense in data security is the individual Practice user. Practice users are responsible for the security of all data which may come to them in whatever format. The Practice is responsible for maintaining ongoing training programs to inform all users of these requirements.

Wear Identifying Badge so that it may be easily viewed by others **-** In order to help maintain building security, all Colleagues should prominently display their provided identification badge. Contractors and other people who may be in Practice facilities are provided with visitor badges. Contractors and other people who may be within Practice facilities should be chaperoned when in private areas.

Challenge Unrecognized Personnel **-** It is the responsibility of all Practice personnel to take positive action to provide physical security. If you see an unrecognized person in a restricted Practice office location, you should challenge them as to their right to be there. All visitors to Practice offices must sign in at the front desk. In addition, all visitors, excluding patients, must wear a visitor/contractor badge. All other personnel must be regular Colleagues of the Practice. Any challenged person who does not respond appropriately should be immediately reported to supervisory staff.

Secure Laptop with a Cable Lock **-** When out of the office all laptop computers must be secured. To use a laptop in a public area, laptops must be secured with a cable lock. Cable locks will be provided upon request. All users requesting a cable lock will be instructed on their use and provided a simple user document. Most Practice computers will contain sensitive data either of a medical, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while traveling. The cable locks are not fool proof, but do provide an additional level of security. Many laptop computers are stolen in snatch and run robberies, where the thief runs through an office or hotel room and grabs all of the equipment he/she can quickly remove. The use of a cable lock helps to thwart this type of event.

Unattended Computers **-** Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Practice policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15) minutes of inactivity. Colleagues are not allowed to take any action which would override this setting.

Home Use of Practice Corporate Assets - Only computer hardware and software owned by and installed by the Practice is permitted to be connected to or installed on Practice equipment. Only software that has been approved for corporate use by the Practice may be installed on Practice equipment. Personal computers supplied by the Practice are to be used solely for business purposes. All Colleagues and contractors must read and understand the list of prohibited activities that are outlined below. Modifications or configuration changes are not permitted on computers supplied by the Practice for home use.

Retention of Ownership - All software programs and documentation generated or provided by Colleagues, consultants, or contractors for the benefit of the Practice are the property of the Practice unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Practice Colleagues at their own expense.

203 Prohibited Activities
Personnel are prohibited from the following activities. The list is not inclusive. Other prohibited activities are referenced elsewhere in this document.

1. Crashing an information system. Deliberately crashing an information system is strictly prohibited. Users may not realize that they caused a system crash, but if it is shown that the crash occurred as a result of user action, a repetition of the action by that user may be viewed as a deliberate act.
2. Attempting to break into an information resource or to bypass a security feature. This includes running password-cracking programs or sniffer programs, and attempting to circumvent file or other resource permissions.
3. Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer ("P2P") or other malicious code into an information system.
    - Exception: Authorized information system support personnel, or others authorized by the Practice Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.
4. Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The Practice has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
5. Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Practice computers mus
6. t be approved by the Practice.
7. Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the Practice is strictly prohibited.
8. System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Practice is strictly prohibited.

205 Electronic Communication, e-mail, Internet Usage

As a productivity enhancement tool, The Practice encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Practice owned equipment are considered the property of the Practice – not the property of individual users. Consequently, this policy applies to all Practice Colleagues and contractors, and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, Internet, fax, personal computers, and servers.

Practice provided resources, such as individual computer workstations or laptops, computer systems, networks, e-mail, and Internet software and services are intended for business purposes. However, incidental personal use is permissible as long as:

1) it does not consume more than a trivial amount of ime or resources,
2) it does not interfere with staff productivity,
3) it does not preempt any business activity,
4) it does not violate any of the following:
    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b) Illegal activities – Use of Practice information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
    c) Commercial use – Use of Practice information resources for personal or commercial profit is strictly prohibited.
    d) Political Activities – All political activities are strictly prohibited on Practice premises. The Practice encourages all of its Colleagues to vote and to participate in the election process, but these activities must not be performed using Practice assets or resources.
    e) Harassment – The Practice strives to maintain a workplace free of harassment and that is sensitive to the diversity of its Colleagues. Therefore, the Practice prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in

ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.

f) Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing "junk" mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

Generally, while it is **NOT** the policy of the Practice to monitor the content of any electronic communication, the Practice is responsible for servicing and protecting the Practice's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Several different methods are employed to accomplish these goals. For example, an audit or cost analysis may require reports that monitor phone numbers dialed, length of calls, number of calls to / from a specific handset, the time of day, etc. Other examples where electronic communications may be monitored include, but are not limited to, research and testing to optimize IT resources, troubleshooting technical problems and detecting patterns of abuse or illegal activity.

The Practice reserves the right, at its discretion, to review any Colleagues's files or electronic communications to the extent necessary to ensure all electronic media and services are used in compliance with all applicable laws and regulations as well as Practice policies.

Colleagues should structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

207 Internet Access

Internet access is provided for Practice users and is considered a great resource for the organization. This resource is costly to operate and maintain, and must be allocated primarily to those with business, administrative or contract needs. The Internet access provided by the Practice should not be used for entertainment, listening to music, viewing the sports highlight of the day, games, movies, etc. Do not use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users must understand that individual Internet usage is monitored, and if a Colleague is found to be spending an excessive amount of time or consuming large amounts of bandwidth for personal use, disciplinary action will be taken.

Many Internet sites, such as games, peer-to-peer file sharing applications, chat rooms, and on-line music sharing applications, have already been blocked by the Practice routers and firewalls. This list is constantly monitored and updated as necessary. Any Colleague visiting pornographic sites will be disciplined and may be terminated.

209 Reporting Software Malfunctions

Users should inform the appropriate Practice personnel when the user's software does not appear to be functioning correctly. The malfunction – whether accidental or deliberate - may pose an information security risk. If the user, or the user's manager or supervisor, suspects a computer virus infection, the Practice computer virus policy should be followed, and these steps should be taken immediately:

1. Stop using the computer

2. Do not carry out any commands, including commands to <Save> data.
3. Do not close any of the computer's windows or programs.
4. Do not turn off the computer or peripheral devices.
5. If possible, physically disconnect the computer from networks to which it is attached.
6. Inform the appropriate personnel or Practice ISO as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
7. Write down any changes in hardware, software, or software use that preceded the malfunction.
8. Do not attempt to remove a suspected virus!

The ISO should monitor the resolution of the malfunction or incident, and report to the CST the result of the action with recommendations on action steps to avert future similar occurrences.

211 Report Security Incidents

It is the responsibility of each Practice Colleague or contractor to report perceived security incidents on a continuous basis to the appropriate supervisor or security person. A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users are to formally report all security incidents or violations of the security policy immediately to the Privacy Officer Users should report any perceived security incident to either their immediate supervisor, or to their department head, or to any member of the Practice CST. Members of the CST are specified above in this document.

Reports of security incidents shall be escalated as quickly as possible. Each member of the Practice CST must inform the other members as rapidly as possible. Each incident will be analyzed to determine if changes in the existing security structure are necessary. All reported incidents are logged and the remedial action indicated. It is the responsibility of the CST to provide training on any procedural changes that may be required as a result of the investigation of an incident.

Security breaches shall be promptly investigated. If criminal action is suspected, the Practice Privacy Officer shall contact the appropriate law enforcement and investigative authorities immediately, which may include but is not limited to the police or the FBI.

213 Transfer of Sensitive/Confidential Information

When confidential or sensitive information from one individual is received by another individual while conducting official business, the receiving individual shall maintain the confidentiality or sensitivity of the information in accordance with the conditions imposed by the providing individual. All employees must recognize the sensitive nature of data maintained by the Practice and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Practice policy and will result in personnel action, and may result in legal action.

215 Transferring Software and Files between Home and Work

Personal software shall not be used on Practice computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Practice purchased software on home or on non-Practice computers or equipment.

Practice proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of the Practice without written consent of the respective supervisor or department head. It is crucial to the Practice to protect all data and, in order to do that effectively we must control the systems in which it is contained. In the event that a supervisor or department head receives a request to transfer Practice data to a non-Practice Computer System, the supervisor or department head should notify the Privacy Officer or appropriate personnel of the intentions and the need for such a transfer of data.

The Practice Wide Area Network ("WAN") is maintained with a wide range of security protections in place, which include features such as virus protection, e-mail file type restrictions, firewalls, anti-hacking hardware and software, etc. Since the Practice does not control non-Practice personal computers, the Practice cannot be sure of the methods that may or may not be in place to protect Practice sensitive information, hence the need for this restriction.

217 Internet Considerations

Special precautions are required to block Internet (public) access to Practice information resources not intended for public access, and to protect confidential Practice information when it is to be transmitted over the Internet.

The following security and administration issues shall govern Internet usage. Prior approval of the Practice Privacy Officer or appropriate personnel authorized by the Practice shall be obtained before:

1. An Internet, or other external network connection, is established;
2. Practice information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
3. Users may not install or download any software (applications, screen savers, etc.). If users have a need for additional software, the user is to contact their supervisor;
4. Use shall be consistent with the goals of the Practice. The network can be used to market services related to the Practice, however use of the network for personal profit or gain is prohibited.
5. Confidential or sensitive data - including credit card numbers, telephone calling card numbers, logon passwords, and other parameters that can be used to access goods or services - shall be encrypted before being transmitted through the Internet.
6. The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the Practice Privacy Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

219 Installation of Authentication and Encryption Certificates on the Email System

Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user. Once verified, the certificate is installed on both recipients' workstations, and the two may safely exchange secure e-mail.

221 Use of WINZIP Encrypted and Zipped Email

This software allows Practice personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Practice staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

222 De-Identification/Re-Identification of Personal Health Information (PHI)

As directed by HIPAA, all personal identifying information is removed from all data that falls within the definition of PHI before it is stored or exchanged.

De-identification is defined as the removal of any information that may be used to identify an individual or of relatives, employers, or household members. PHI includes:

1. Names
2. Addresses
3. Geographic subdivisions smaller than a state
4. All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)

5. Telephone numbers
6. Facsimile numbers
7. Driver's license numbers
8. Electronic mail addresses
9. Social security numbers
10. Medical record numbers
11. Health plan beneficiary numbers
12. Account numbers, certificate/license numbers
13. Vehicle identifiers and serial numbers
14. Device identifiers and serial numbers
15. Web Universal Resource Locators (URLs)
16. Internet Protocol (IP) address numbers
17. Biometric identifiers
18. Full face photographic images and any comparable images

Re-identification of confidential information: A cross-reference code or other means of record identification is used to re-identify data as long as the code is not derived from or related to information about the individual and cannot be translated to identify the individual. In addition, the code is not disclosed for any other purpose nor is the mechanism for re-identification disclosed.

Sparks Family Medicine, LTD/MediTask, LLC/SLMS, LLC
IT Security Policy
Section 300: Identification and Authentication
Reviewed: Annually

Approval Date: 08/18/2015 Effective Date: 08/18/2015

301 User Logon IDs
Individual users shall have unique logon IDs and passwords. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

19. Each user shall be assigned a unique identifier.
20. Users shall be responsible for the use and misuse of their individual logon ID.

All user login IDs are audited at least twice yearly and all inactive logon IDs are revoked. The Office Manager notifies the Security Officer or appropriate personnel upon the departure of all Colleagues and contractors, at which time login IDs are revoked.

The logon ID is locked or revoked after a maximum of three (3) unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

Users who desire to obtain access to Practice systems or networks must have a completed and signed Network Access Form (Appendix C). This form must be signed by the supervisor or department head of each user requesting access.

303 User Account Passwords
User IDs and passwords are required in order to gain access to all Practice networks and workstations. All passwords are restricted by a corporate-wide password policy to be of a "Strong" nature. This means that all passwords must conform to restrictions and limitations that are designed to make the password difficult to guess. Users are required to select a password in order to obtain access to any electronic information both at the server level and at the workstation level. When passwords are reset, the user will be automatically prompted to manually change that assigned password.

Password Length – Passwords are required to be a minimum of eight characters.

Content Requirements - Passwords must contain a combination of upper and lower case alphabetic characters, numeric characters, and special characters.

Change Frequency – Passwords must be changed immediately when compromised.

Reuse - The previous twelve passwords cannot be reused.

Restrictions on Sharing Passwords - Passwords shall not be shared, written down on paper, or stored within a file or database on a workstation and must be kept confidential.

Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens, and are never printed or included in reports or logs. Passwords are stored in an encrypted format.

305 Confidentiality Agreement
Users of Practice information resources shall sign, as a condition for employment, an appropriate confidentiality agreement. The agreement shall include the following statement, or a paraphrase of it:

I understand that any unauthorized use or disclosure of information residing on the Practice information resource systems may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

Temporary workers and third-party employees not already covered by a confidentiality agreement shall sign such a document prior to accessing Practice information resources.

Confidentiality agreements shall be reviewed when there are changes to contracts or other terms of employment, particularly when contracts are ending or employees are leaving an organization.

307 Access Control

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e. passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e. port protection devices, firewalls, host-based authentication, etc.).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources. Access is granted only by the completion of a Network Access Request Form (Appendix C).

This guideline satisfies the "need to know" requirement of the HIPAA regulation. Users may be added to the information system, network, or EHR **only** upon the signature of the Security Officer or appropriate personnel who is responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

309 Identification and Authentication Requirements

The host security management program shall maintain current user application activity authorizations. Each initial request for a connection or a session is subject to the authorization process previously addressed.

311 User Login Entitlement Reviews

If an employee changes positions at the Practice, employee's new supervisor or department head shall promptly notify the Information Technology ("IT") Department of the change of roles by indicating on the Network Access Request Form (Appendix C) both the roles or access that need to be added and the roles or access that need to be removed so that employee has access to the minimum necessary data to effectively perform their new job functions. The effective date of the position change should also be noted on the Form so that the IT Department can ensure that the employee will have appropriate roles, access, and applications for their new job responsibilities. For a limited training period, it may be necessary for the employee who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new job responsibilities.

No less than annually, the IT Manager shall facilitate entitlement reviews with department heads to ensure that all employees have the appropriate roles, access, and software necessary to perform their job functions effectively while being limited to the minimum necessary data to facilitate HIPAA compliance and protect patient data.

313 Termination of User Logon Account

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the IT Department by indicating "Remove Access" on the employee's Network Access Request Form (Appendix C) and submitting the Form to the IT Department. If employee's termination is voluntary and employee provides notice, employee's supervisor or department head shall promptly notify the IT Department of employee's last scheduled work day so that their user account(s) can be configured to expire. The employee's department head shall be responsible for insuring that all keys, ID badges, and other access devices as well as Practice equipment and property is returned to the Practice prior to the employee leaving the Practice on their final day of employment.

No less than quarterly, the IT Manager or their designee shall provide a list of active user accounts for both network and application access, including access to the clinical electronic health record (“EHR”) and the practice management system (“PMS”), to department heads for review. Department heads shall review the employee access lists within five (5) business days of receipt. If any of the employees on the list are no longer employed by the Practice, the department head will immediately notify the IT Department of the employee’s termination status and submit the updated Network Access Request Form (Appendix C).

Sparks Family Medicine, LTD/MediTask, LLC/SLMS, LLC
IT Security Policy
Section 400: Network Connectivity
Reviewed: Annually

Approval Date: 08/18/2015 Effective Date: 08/18/2015

401 Dial-in Connections
Access to Practice information resources through modems or other dial-in devices / software, if available, shall be subject to authorization and authentication by an access control system. **Direct inward dialing without passing through the access control system is prohibited.** Dial-up numbers shall be unlisted.

Systems that allow public access to host computers, including mission-critical servers, warrants additional security at the operating system and application levels. Such systems shall have the capability to monitor activity levels to ensure that public usage does not unacceptably degrade system responsiveness.

Dial-up access privileges are granted only upon the request of a department head with the submission of the Network Access Form and the approval of the Privacy Officer or appropriate personnel.

403 Dial-out Connects
Practice provides a link to an Internet Service Provider**.** If a user has a specific need to link with an outside computer or network through a direct link, approval must be obtained from the Privacy Officer or appropriate personnel. The appropriate personnel will ensure adequate security measures are in place.

405 Telecommunication Equipment
Certain direct link connections may require a dedicated or leased phone line. These facilities are authorized only by the Privacy Officer or appropriate personnel and ordered by the appropriate personnel. Telecommunication equipment and services include but are not limited to the following:

1. Phone lines
2. Fax lines
3. Calling cards
4. Phone head sets
5. Software type phones installed on workstations
6. Conference calling contracts
7. Cell phones
8. Blackberry type devices
9. Call routing software
10. Call reporting software
11. Phone system administration equipment
12. T1/Network lines
13. Long distance lines
14. 800 lines
15. Local phone lines
16. PRI circuits
17. Telephone equipment

407 Permanent Connections
The security of Practice systems can be jeopardized from third party locations if security practices and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of

Practice systems. The Privacy Officer or appropriate personnel should be involved in the process, design and approval.

409 Emphasis on Security in Third Party Contracts

Access to Practice computer systems or corporate networks should not be granted until a review of the following concerns have been made, and appropriate restrictions or covenants included in a statement of work ("SOW") with the party requesting access.

1. Applicable sections of the Practice Information Security Policy have been reviewed and considered.
2. Policies and standards established in the Practice information security program have been enforced.
3. A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
4. The right to audit contractual responsibilities should be included in the agreement or SOW.
5. Arrangements for reporting and investigating security incidents must be included in the agreement in order to meet the covenants of the HIPAA Business Associate Agreement.
6. A description of each service to be made available.
7. Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
8. A detailed list of users that have access to Practice computer systems must be maintained and auditable.
9. If required under the contract, permission should be sought to screen authorized users.
10. Dates and times when the service is to be available should be agreed upon in advance.
11. Procedures regarding protection of information resources should be agreed upon in advance and a method of audit and enforcement implemented and approved by both parties.
12. The right to monitor and revoke user activity should be included in each agreement.
13. Language on restrictions on copying and disclosing information should be included in all agreements.
14. Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
15. Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
16. If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
17. A formal method to grant and authorized users who will access to the data collected under the agreement should be formally established before any users are granted access.
18. Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
19. Because annual confidentiality training is required under the HIPAA regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.
20. A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

411 Firewalls

Authority from the Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to a Practice router or firewall.

Sparks Family Medicine, LTD/MediTask, LLC/SLMS, LLC
IT Security Policy
Section 500: Malicious Code and Encryption
Reviewed: Annually

Approval Date: 08/18/2015 Effective Date: 08/18/2015

501 Antivirus Software Installation
Antivirus software is installed on all Practice personal computers and servers. Virus update patterns are updated daily on the Practice servers and workstations. Virus update engines and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

Configuration **-** The antivirus software currently implemented by the Practice is McAfee VirusScan Enterprise[18]. Updates are received directly from McAfee[19] which is scheduled daily at 5:00 PM[20].

Remote Deployment Configuration **-** Through an automated procedure, updates and virus patches may be pushed out to the individual workstations and servers on an as needed basis.

Monitoring/Reporting – A record of virus patterns for all workstations and servers on the Practice network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Privacy Officer or appropriate personnel.

503 New Software Distribution
Only software created by Practice application staff, if applicable, or software approved by the Privacy Officer or appropriate personnel will be used on internal computers and networks. A list of approved software is maintained in Appendix C. All new software will be tested by appropriate personnel in order to ensure compatibility with currently installed software and network configuration. In addition, appropriate personnel must scan all software for viruses before installation. This includes shrink-wrapped software procured directly from commercial sources as well as shareware and freeware obtained from electronic bulletin boards, the Internet, or on disks (magnetic or CD-ROM and custom-developed software).

Although shareware and freeware can often be useful sources of work-related programs, the use and/or acquisition of such software must be approved by the Privacy Officer or appropriate personnel. Because the software is often provided in an open distribution environment, special precautions must be taken before it is installed on Practice computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage Practice hardware, software, or data, and that the software does not contain viruses, either originating with the software designer or acquired in the process of distribution.

All data and program files that have been electronically transmitted to a Practice computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Practice personnel for instructions for scanning files for viruses.

Every diskette, CD-ROM, DVD and USB device is a potential source for a computer virus. Therefore, every diskette, CD-ROM, DVD and USB device must be scanned for virus infection prior to copying information to a Practice computer or network.

Computers shall never be “booted” from a diskette, CD-ROM, DVD or USB device received from an outside source. Users shall always remove any diskette, CD-ROM, DVD or USB device from the computer when not in use. This is to ensure that the diskette, CD-ROM, DVD or USB device is not in the computer when the machine is powered on. A diskette, CD-ROM, DVD or USB device infected with a boot virus may infect a computer in that manner, even if the diskette, CD_ROM, DVD or USB device is not “bootable”.

505 Retention of Ownership
All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Practice are the property of the Practice unless covered by a contractual agreement. Employees developing programs or documentation must sign a statement acknowledging Practice ownership at the time of employment. Nothing contained herein applies to software purchased by Practice employees at their own expense.

507 Encryption
Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text*;* encrypted data is referred to as cipher text**.**

509 Encryption Key
An encryption key specifies the particular transformation of plain text into cipher text, or vice versa during decryption.

If justified by risk analysis, sensitive data and files shall be encrypted before being transmitted through networks. When encrypted data are transferred between agencies, the agencies shall devise a mutually agreeable procedure for secure key management. In the case of conflict, the Practice shall establish the criteria in conjunction with the Privacy Officer or appropriate personnel. The Practice employs several methods of secure data transmission.

511 Installation of Authentication and Encryption Certificates on the Email System
Any user desiring to transfer secure e-mail with a specific identified external user may request to exchange public keys with the external user by contacting the Privacy Officer or appropriate personnel. Once verified, the certificate is installed on each recipient workstation, and the two may safely exchange secure e-mail.

513 Use of Winzip Encrypted and Zipped E-mail
This software allows Practice personnel to exchange e-mail with remote users who have the appropriate encryption software on their system. The two users exchange private keys that will be used to both encrypt and decrypt each transmission. Any Practice staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

515 File Transfer Protocol (FTP)
Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any FTP transfers should be directed to the Privacy Officer or appropriate personnel.

517 Secure Socket Layer (SSL) Web Interface
Any EHR hosted (ASP) system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Colleague Network Access Form and have appropriate approval from the supervisor or department head as well as the Privacy Officer or appropriate personnel before any access is granted.

Sparks Family Medicine, LTD/MediTask, LLC/SLMS, LLC
IT Security Policy
Section 600: Building Security and Telecommuting
Reviewed: Annually

Approval Date: 08/18/2015 Effective Date: 08/18/2015

601 Building Security
It is the policy of the Practice to provide building access in a secure manner. Each site, if applicable, is somewhat unique in terms of building ownership, lease contracts, entranceway access, fire escape requirements, and server room control. However, the Practice strives to continuously upgrade and expand its security and to enhance protection of its assets and medical information that has been entrusted to it. The following list identifies measures that are in effect at the Practice. All other facilities, if applicable, have similar security appropriate for that location.

Sparks Family Medicine, 10155 W. Twain Ave, Suite 110, Las Vegas, NV 89147

1. Entrance to the building during non-working hours is controlled by keyed entry and an alarm system monitored by Johnson Alarms Security. Key access points are equipped with motion detection sensors. Any attempted entrance without an approved code or activation of an active motion detector will result in immediate notification to Johnson Alarms Security.
2. Only Practice employees are given the security code for entrance. Disclosure of the security code to non-employees is strictly prohibited.
3. The security code is unique to each employee. Security codes are changed upon termination of employees.
4. The door to the reception area is locked at all times and requires appropriate credentials or escort past the reception or waiting area door(s).
5. The reception area is staffed at all times during the working hours of 8:00 AM to 5:00 PM.
6. Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk, wear a visitor badge (excluding patients), and be accompanied by a Practice staff member. In some situations, non-Practice personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times.
7. Fire Protection: Use of local building codes are observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

603 Telecommuting
With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. The Practice considers telecommuting to be an acceptable work arrangement in certain circumstances. This policy is applicable to all employees and contractors who work either permanently or only occasionally outside of the Practice office environment. It applies to users who work from their home full time, to employees on temporary travel, to users who work from a remote office location, and to any user who connects to the Practice network and/or hosted EHR, if applicable, from a remote location.

While telecommuting can be an advantage for users and for the organization in general, it presents new risks in the areas of confidentiality and security of data. Workers linked to the Practice's network become an extension of the wide area network and present additional environments that must be protected against the danger of spreading Trojans, viruses, or other malware. This arrangement also exposes the corporate as well as patient data to risks not present in the traditional work environment.

605 Telecommuting General Requirements
Telecommuting workers are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable to other employees/contractors.

1. **Need to Know:** Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
2. **Password Use:** The use of a strong password, changed at least every 90 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.
3. **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.
4. **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

607 Telecommuting Required Equipment

Employees approved for telecommuting must understand that the Practice will not provide all equipment necessary to ensure proper protection of information to which the employee has access; however, the following lists define the equipment and environment required:

Practice Provided:

None

Employee Provided:

Broadband connection and fees,
Paper shredder,
Secure office environment isolated from visitors and family,
A lockable file cabinet or safe to secure documents when away from the home office.

609 Telecommuting Hardware Security Protections

Virus Protection**:** Home users must never stop the update process for Virus Protection. Virus Protection software is installed on all Practice personal computers and is set to update the virus pattern on a daily basis. This update is critical to the security of all data, and must be allowed to complete.

VPN and Firewall Use**:** Established procedures must be rigidly followed when accessing Practice information of any type. The Practice requires the use of VPN software and a firewall device. Disabling a virus scanner or firewall is reason for termination.

Security Locks: Use security cable locks for laptops at all times, even if at home or at the office. Cable locks have been demonstrated as effective in thwarting robberies.

Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected by HIPAA or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 15 minutes of inactivity.

611 Telecommuting Data Security Protection

Data Backup**:** Backup procedures have been established that encrypt the data being moved to an external media. Use only that procedure – do not create one on your own. If there is not a backup procedure established, or if you have external media that is not encrypted, contact the appropriate Practice personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to the Practice**:** Transferring of data to the Practice requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Do not circumvent established procedures, nor create your own method, when transferring data to the Practice.

External System Access: If you require access to an external system, contact your supervisor or department head. Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Do not send any individual-identifiable information (PHI or PII) via e-mail unless it is encrypted. If you need assistance with this, contact the Privacy Officer or appropriate personnel to ensure an approved encryption mechanism is used for transmission through e-mail.

Non-Practice Networks: Extreme care must be taken when connecting Practice equipment to a home or hotel network. Although the Practice actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the Practice has no ability to monitor or control the security procedures on non-Practice networks.

Protect Data in Your Possession: View or access only the information that you have a need to see to complete your work assignment. Regularly review the data you have stored to ensure that the amount of patient level data is kept at a minimum and that old data is eliminated as soon as possible. Store electronic data only in encrypted work spaces. If your laptop has not been set up with an encrypted work space, contact the Privacy Officer or appropriate personnel for assistance.

Hard Copy Reports or Work Papers: Never leave paper records around your work area. Lock all paper records in a file cabinet at night or when you leave your work area.

Data Entry When in a Public Location: Do not perform work tasks which require the use of sensitive corporate or patient level information when you are in a public area, i.e. airports, airplanes, hotel lobbies. Computer screens can easily be viewed from beside or behind you.

Sending Data Outside the Practice**:** All external transfer of data must be associated with an official contract, non-discloser agreement, or appropriate Business Associate Agreement. Do not give or transfer any patient level information to anyone outside the Practice without the written approval of your supervisor.

613 Disposal of Paper and/or External Media

Shredding: All paper which contains sensitive information that is no longer needed must be shredded before being disposed. Do not place in a trash container without first shredding. All employees working from home, or other non-Practice work environment, MUST have direct access to a shredder.

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with HIPAA compliant procedures.

1. Do not throw any media containing sensitive, protected information in the trash.
2. Return all external media to your supervisor
3. External media must be wiped clean of all data. The Privacy Officer or appropriate personnel has very definitive procedures for doing this – so all external media must be sent to them.
4. The final step in this process is to forward the media for disposal by a certified destruction agency.

Sparks Family Medicine, LTD/MediTask, LLC/SLMS, LLC
IT Security Policy
Section 700: Specific Protocols and Devices
Reviewed: Annually

Approval Date: 08/18/2015 Effective Date: 08/18/2015

701 Wireless Usage Standards and Policy
Due to an emergence of wireless access points in hotels, airports, and in homes, it has become imperative that a Wireless Usage policy be developed and adopted to ensure the security and functionality of such connections for Practice employees. This policy outlines the processes and procedures for acquiring wireless access privileges, utilizing wireless access, and ensuring the security of Practice laptops and mobile devices.

Approval Procedure **-** In order to be granted the ability to utilize the wireless network interface on your Practice laptop or mobile device you will be required to gain the approval of your immediate supervisor or department head and the Privacy Officer or appropriate personnel of the Practice. The Colleague Network Access Form is used to make such a request. Once this form is completed and approved you will be contacted by appropriate Practice personnel to setup your laptop and schedule training.

Software Requirements **-** The following is a list of minimum software requirements for any Practice laptop that is granted the privilege to use wireless access:

1. Windows XP with Service Pack 3 (Firewall enabled)
2. Antivirus software
3. Full Disk Encryption
4. Appropriate VPN Client, if applicable
5. Internet Explorer 6.0 SP2 or Greater

If your laptop does not have all of these software components, please notify your supervisor or department head so these components can be installed.

Training Requirements **-** Once you have gained approval for wireless access on your Practice computer, you will be required to attend a usage and security training session to be provided by the Privacy Officer or appropriate personnel. This training session will cover the basics of connecting to wireless networks, securing your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks. This training will be conducted within a reasonable period of time once wireless access approval has been granted, and in most cases will include several individuals at once.

702 Use of Transportable Media
Transportable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB key devices.

The purpose of this policy is to guide employees/contractors of the Practice in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Practice networks. Every workstation or server that has been used by either Practice employees or contractors is presumed to have sensitive information stored on its hard drive. Therefore procedures must be carefully followed when copying data to or from transportable media to protect sensitive Practice data. Since transportable media, by their very design are easily lost, care and protection of these devices must be addressed. Since it is very likely that transportable media will be provided to a Practice employee by an external source for the exchange of information, it is necessary that all employees have guidance in the appropriate use of media from other companies.

The use of transportable media in various formats is NOT common practice within the Practice, but all users must be aware that sensitive data could potentially be lost or compromised when moved outside of

Practice networks. Transportable media received from an external source could potentially pose a threat to Practice networks. ***Sensitive data*** includes all human resource data, financial data, Practice proprietary information, and personal health information ("PHI") protected by the Health Insurance Portability and Accountability Act ("HIPAA").

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

- No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted format.
- All USB keys used to store Practice data or sensitive data must be an encrypted USB key issued by the Privacy Officer or appropriate personnel. The use of a personal USB key is strictly prohibited.
- Users must never connect their transportable media to a workstation that is not issued by the Practice.
- Non-Practice workstations and laptops may not have the same security protection standards required by the Practice, and accordingly virus patterns could potentially be transferred from the non-Practice device to the media and then back to the Practice workstation.

  Example: Do not copy a work spreadsheet to your USB key and take it home to work on your home PC.
- Data may be exchanged between Practice workstations/networks and workstations used within the Practice. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

  Examples of necessary data exchange include:
  Data provided to auditors via USB key during the course of the audit.
- It is permissible to connect transferable media from other businesses or individuals into Practice workstations or servers as long as the source of the media in on the Practice Approved Vendor list (Appendix D).
- Before initial use and before any ***sensitive data*** may be transferred to transportable media, the media must be sent to the Privacy Officer or appropriate personnel to ensure appropriate and approved encryption is used. Copy ***sensitive data*** only to the encrypted space on the media. Non-sensitive data may be transferred to the non-encrypted space on the media.
- Report all loss of transportable media to your supervisor or department head. It is important that the CST team is notified either directly from the employee or contractor or by the supervisor or department head immediately.
- When an employee leaves the Practice, all transportable media in their possession must be returned to the Privacy Officer or appropriate personnel for data erasure that conforms to US Department of Defense standards for data elimination.

The Practice utilizes an approved method of encrypted data to ensure that all data is converted to a format that cannot be decrypted. The Privacy Officer or appropriate personnel can quickly establish an encrypted partition on your transportable media.

When no longer in productive use, all Practice laptops, workstation, or servers must be wiped of data in a manner which conforms to HIPAA regulations. All transportable media must be wiped according to the same standards. Thus all transportable media must be returned to the Privacy Officer or appropriate personnel for data erasure when no longer in use.

Sparks Family Medicine, LTD/MediTask, LLC/SLMS, LLC
IT Security Policy
Section 800: Medical Information and External Media/Hardware
Reviewed: Annually

Approval Date: 08/18/2015 Effective Date: 08/18/2015

801 Retention/Destruction of Medical Information
Many state and federal laws regulate the retention and destruction of medical information. The Practice actively conforms to these laws and follows the strictest regulation if/when a conflict occurs.

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information practice, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, and a complaint record are maintained for a period of at least 6 years.

Record Destruction - All hardcopy medical records that require destruction are shredded.

803 Disposal of External Media
It must be assumed that any external media in the possession of an employee is likely to contain either protected health information ("PHI") or other sensitive information. Accordingly, external media (CD-ROMs, DVDs, diskettes, USB drives) should be disposed of in a method that ensures that there will be no loss of data and that the confidentiality and security of that data will not be compromised.

The following steps must be adhered to:

1. It is the responsibility of each employee to identify media which should be shredded and to utilize this policy in its destruction.
2. External media should never be thrown in the trash.
3. When no longer needed all forms of external media are to be sent to the Privacy Officer or appropriate personnel for proper disposal.
4. The media will be secured until appropriate destruction methods are used based on NIST 800-88 guidelines.

805 Requirements Regarding Equipment
All equipment to be disposed of will be wiped of all data, and all settings and configurations will be reset to factory defaults. No other settings, configurations, software installation or options will be made. Asset tags and any other identifying logos or markings will be removed.

807 Disposition of Excess Equipment
As the older Practice computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

1. Older machines are regularly utilized for spare parts.
2. Older machines are used on an emergency replacement basis.
3. Older machines are used for testing new software.
4. Older machines are used as backups for other production equipment.
5. Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
6. Older machines are used to provide a second machine for personnel who often work from home.

Sparks Family Medicine, LTD/MediTask, LLC/SLMS, LLC
IT Security Policy
Section 900: Additional Policies
Reviewed: Annually

Approval Date: 08/18/2015 Effective Date: 08/18/2015

901 Statement of Change Policy
To ensure that Practice is tracking changes to networks, systems, and workstations including software releases and software vulnerability patching in information systems that contain electronic protected health information ("ePHI"). Change tracking allows the Information Technology ("IT") Department to efficiently troubleshoot issues that arise due to an update, new implementation, reconfiguration, or other change to the system.

Procedure
1. The IT staff or other designated Practice employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.
    a. When changes are tracked within a system, i.e. Windows updates in the Add or Remove Programs component or electronic health record (EHR) updates performed and logged by the vendor, they do not need to be logged on the change management tracking log; however, the employee implementing the change will ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

903 Statement of Audit Controls Policy
To ensure that Practice implements hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain electronic protected health information ("ePHI"). Audit Controls are technical mechanisms that track and record computer activities. An audit trail determines if a security violation occurred by providing a chronological series of logged computer events that relate to an operating system, an application, or user activities.

The Practice is committed to routinely auditing users' activities in order to continually assess potential risks and vulnerabilities to ePHI in its possession. As such, the Practice will continually assess potential risks and vulnerabilities to ePHI in its possession and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

Procedure
1. See policy entitled Information System Activity Review for the administrative safeguards for auditing system activities.
2. The Information Technology Services shall enable event auditing on all computers that process, transmit, and/or store ePHI for purposes of generating audit logs. Each audit log shall include, at a minimum: user ID, login time and date, and scope of patient data being accessed for each attempted access. Audit trails shall be stored on a separate computer system to minimize the impact of such auditing on business operations and to minimize access to audit trails.
3. The Practice shall utilize appropriate network-based and host-based intrusion detection systems. The Information Technology Services shall be responsible for installing, maintaining, and updating such systems.

905 Statement of Information System Activity Review Policy
To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and

access reports. Practice shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

Procedure

1. See policy entitled Audit Controls for a description of the technical mechanisms that track and record activities on Practice's information systems that contain or use ePHI.
2. The Information Technology Services shall be responsible for conducting reviews of Practice's information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
3. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.
4. Such reviews shall be conducted annually. Audits also shall be conducted if Practice has reason to suspect wrongdoing. In conducting these reviews, the Information Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:
    a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.

    b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
    c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.
    d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

All significant findings shall be recorded using the report format referred to in Section 2 of this policy and procedure.

1. The Information Technology Services shall forward all completed reports, as well as recommended actions to be taken in response to findings, to the Security Officer for review. The Security Officer shall be responsible for maintaining such reports. The Security Officer shall consider such reports and recommendations in determining whether to make changes to Practice's administrative, physical, and technical safeguards. In the event a security incident is detected through such auditing, such matter shall be addressed pursuant to the policy entitled Employee Responsibilities (Report Security Incidents).

907 Statement of Data Integrity Policy

Practice shall implement and maintain appropriate electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.

The purpose of this policy is to protect Practice's ePHI from improper alteration or destruction.

Procedure

To the fullest extent possible, Practice shall utilize applications with built-in intelligence that automatically checks for human errors.Practice shall acquire appropriate network-based and host-based intrusion detection systems. The Security Officer shall be responsible for installing, maintaining, and updating such systems. To prevent transmission errors as data passes from one computer to another, Practice will use encryption, as determined to be appropriate, to preserve the integrity of data. Practice will check for possible duplication of data in its computer systems to prevent poor data integration between different computer systems.

To prevent programming or software bugs, Practice will test its information systems for accuracy and functionality before it starts to use them. Practice will update its systems when IT vendors release fixes to address known bugs or problems.

1. Practice will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.
2. To prevent exposing magnetic media to a strong magnetic field, workforce members shall keep magnetic media away from strong magnetic fields and heat. For example, computers should not be left in automobiles during the summer months.

909 Statement of Contingency Plan Policy

To establish and implement policies and procedures for responding to an emergency or other occurrence (e.g., fire, vandalism, system failure, natural disaster) that damages systems that contain ePHI.

Practice is committed to maintaining formal practices for responding to an emergency or other occurrence that damages systems containing ePHI. Practice shall continually assess potential risks and vulnerabilities to protect health information in its possession, and develop, implement, and maintain appropriate administrative, physical, and technical security measures in accordance with the HIPAA Security Rule.

Procedure

1. Data Backup Plan
    a. Practice, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies of ePHI.
    b. At the conclusion of each day, Monday through Friday, an incremental backup of all servers containing ePHI shall be backed up to tape. On Saturday, a full backup of all servers containing ePHI shall be backed up to tape. The backup tapes are taken each week off site by the IS Manager or his/her designee to ensure safeguard of Practice's data. One month of backup data will be maintained at all times in a remote location. Backup media that is no longer in service will be disposed of in accordance with the Disposal of External Media/Hardware policy.
    c. The Security Officer shall monitor storage and removal of backups and ensure all applicable access controls are enforced.
    d. The Security Officer shall test backup procedures on an annual basis to ensure that exact copies of ePHI can be retrieved and made available. Such testing shall be documented by the Security Officer. To the extent such testing indicates need for improvement in backup procedures, the Security Officer shall identify and implement such improvements in a timely manner.

2. Disaster Recovery and Emergency Mode Operations Plan
    a. The Security Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:
        i. Restoring or recovering any loss of ePHI and/or systems necessary to make ePHI available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and
        ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at the off-site locations at which backups are stored or other secure off-site location.
    b. The disaster recovery and emergency mode operation plan shall include the following:
        i. Current copies of the information systems inventory and network configuration developed and updated as part of Practice’s risk analysis.
        ii. Current copy of the written backup procedures developed and updated pursuant to this policy.
        iii. An inventory of hard copy forms and documents needed to record clinical, registration, and financial interactions with patients.

iv. Identification of an emergency response team. Members of such team shall be responsible for the following:
    1. Determining the impact of a disaster and/or system unavailability on Practice's operations.
    2. In the event of a disaster, securing the site and providing ongoing physical security.
    3. Retrieving lost data.
    4. Identifying and implementing appropriate "work-arounds" during such time information systems are unavailable.
    5. Taking such steps necessary to restore operations.
v. Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of Practice's risk analysis
vi. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:
    1. Members of the immediate response team,
    2. Facilities at which backup data is stored,
    3. Information systems vendors, and
    4. All current workforce members.

c. The disaster recovery team shall meet on at least an annual basis to:
    i. Review the effectiveness of the plan in responding to any disaster or emergency experienced by Practice;
    ii. In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and
    iii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security Officer shall be responsible for convening and maintaining minutes of such meetings. The Security Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

911 Statement of Security Awareness and Training Policy
To establish a security awareness and training program for all members of Practice's workforce, including management.

All workforce members shall receive appropriate training concerning Practice's security policies and procedures. Such training shall be provided prior to the effective date of the HIPAA Security Rule and on an ongoing basis to all new employees. Such training shall be repeated annually for all employees.

Procedure

a. Security Training Program
    i. The Security Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such initial training addressing the requirements of the HIPAA Security Rule including the updates to HIPAA regulations found in the Health Information Technology for Economic and Clinical Health (HITECH) Act. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. The Security Officer shall be responsible for maintaining appropriate documentation of all training activities.
    ii. The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of ePHI, e.g., addition of new hardware or software, and increased threats.
b. Security Reminders
    i. The Security Officer shall generate and distribute to all workforce members routine security reminders on a regular basis. Periodic reminders shall address password

security, malicious software, incident identification and response, and access control. The Security Officer may provide such reminders through formal training, e-mail messages, discussions during staff meetings, screen savers, log-in banners, newsletter/intranet articles, posters, promotional items such as coffee mugs, mouse pads, sticky notes, etc. The Security Officer shall be responsible for maintaining appropriate documentation of all periodic security reminders.

ii. The Security Officer shall generate and distribute special notices to all workforce members providing urgent updates, such as new threats, hazards, vulnerabilities, and/or countermeasures.

c. Protection from Malicious Software
   i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:
      a) Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,
      b) The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,
      c) Instructions to never download files from unknown or suspicious sources,
      d) Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,
      e) The importance of backing up critical data on a regular basis and storing the data in a safe place,
      f) Damage caused by viruses and worms, and
      g) What to do if a virus or worm is detected.

d. Password Management
   i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:
      a) Passwords must be changed every 90 days.
      b) A user cannot reuse the last 12 passwords.
      c) Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters.
      d) Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.
      e) A password must be promptly changed if it is suspected of being disclosed, or known to have been disclosed.
      f) Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to “fix” a computer or handle an emergency situation) or individuals, including family members.
      g) Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.
      h) Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.
      i) Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.

913 Statement of Security Management Process Policy

To ensure Practice conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ePHI held by Practice.

Practice shall conduct an accurate and thorough risk analysis to serve as the basis for Practice’s HIPAA Security Rule compliance efforts. Practice shall re-assess the security risks to its ePHI and evaluate the effectiveness of its security measures and safeguards as necessary in light of changes to business practices and technological advancements.

Procedure

a. The Security Officer shall be responsible for coordinating Practice's risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.
b. The risk analysis shall proceed in the following manner:
    i. Document Practice's current information systems.
        a) Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendor, licenses, maintenance schedule, and function. Update/develop network diagram illustrating how organization's information system network is configured.
        b) Update/develop facility layout showing location of all information systems equipment, power sources, telephone jacks, and other telecommunications equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.
        c) For each application identified, identify each licensee (*i.e.,* authorized user) by job title and describe the manner in which authorization is granted.
        d) For each application identified:
            i) Describe the data associated with that application.
            ii) Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.
            iii) Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.
            iv) Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.
            v) Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.
            vi) For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.
        e) Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of ePHI created, received, maintained, or transmitted by Practice. Consider the following:
            i) Natural threats, e.g., earthquakes, storm damage.
            ii) Environmental threats, e.g., fire and smoke damage, power outage, utility problems.
            iii) Human threats
                a. Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls
                b. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment
                c. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail
                d. External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction
            iv) Identify and document vulnerabilities in Practice's information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to ePHI, modification of ePHI, denial of service, or repudiation (*i.e.,* the inability to identify the source and hold some

person accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities.

f) Determine and document probability and criticality of identified risks.
   i) Assign probability level, i.e., likelihood of a security incident involving identified risk.
      a. "Very Likely" (3) is defined as having a probable chance of occurrence.
      b. "Likely" (2) is defined as having a significant chance of occurrence.
      c. "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.
   ii) Assign criticality level.
      a. "High" (3) is defined as having a catastrophic impact on the medical practice including a significant number of medical records which may have been lost or compromised.
      b. "Medium" (2) is defined as having a significant impact including a moderate number of medical records within the practice which may have been lost or compromised.
      c. "Low" (1) is defined as a modest or insignificant impact including the loss or compromise of some medical records.
   iii) Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.

g) Identify and document appropriate security measures and safeguards to address key vulnerabilities. To accomplish this task, review the vulnerabilities you have identified in relation to the standards and implementation specifications. Focus on those vulnerabilities with high risk scores, as well as specific security measures and safeguards required by the Security Rule.

h) Develop and document an implementation strategy for critical security measures and safeguards.
   i) Determine timeline for implementation.
   ii) Determine costs of such measures and safeguards and secure funding.
   iii) Assign responsibility for implementing specific measures and safeguards to appropriate person(s).
   iv) Make necessary adjustments based on implementation experiences.
   v) Document actual completion dates.

i. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.

c. The Security Officer shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security Officer shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the HIPAA Security Regulations; new federal, state, or local laws or regulations affecting the security of ePHI; changes in technology, environmental processes, or business processes that may affect HIPAA Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations shall include the following:

i. Inspections, reviews, interviews, and analysis to assess adequacy of administrative and physical safeguards. Such evaluation shall include interviews to assess employee compliance; after-hours walk-through inspections to assess physical security, password protection (i.e., not posted), and workstation sessions terminated (i.e., employees logged out); review of latest security policies and procedures for correctness and completeness; and inspection and analysis of training, incident, and media logs for compliance.

ii. Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, Practice shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement

915 Emergency Operations Procedures (EHR outage) Purpose
To provide procedures for managing and documenting patient encounters when Electronic Health Record (EHR) and Practice Management (PM) systems are unavailable due to planned or unexpected outages.

Definitions
Electronic Health Record (EHR) – Electronic records of patient encounters in a healthcare delivery setting. An electronic health record typically consists of information including: patient demographics, progress notes, medication history, vital signs and laboratory results.

Practice Management (PM) – A practice Management System is usually a computer based system used to manage the day-to-day operations of a healthcare practice. Tasks typically performed by a PM system include: scheduling appointments, maintaining patient and insurance information, billing functions and generating various reports.

Procedures

Notification:

The Information Systems or Technology Manager shall notify Practice management as soon as practicable in the event of:

1. planned downtime of EHR systems,
2. unexpected outage of EHR systems, and
3. resumption of EHR services following an outage such that normal operations may resume.

Scheduling:

If the EHR system is not operational or otherwise unavailable, the schedule printed the previous day is retrieved. The center manager is tasked with maintaining a copy of this schedule or assigning this duty as appropriate.

If phones are operational, patient appointments may not be made. The operator should ask for pertinent contact information and record a message using the paper telephone encounter form.

Patient Encounters:

1. Telephone encounters should be entered onto the paper telephone encounter form and transferred to a nurse for triage. Out folders should be used as temporary charts.
2. Paper daybills should be used to record patient encounter for billing/tracking purposes. Check-in staff should verify patient's name, date of birth, telephone number, home address, and insurance information as available on the paper; schedule and record all changes on the daybill.
3. If the patient is a walk-in or new patient and demographic information is not available, paper registration forms should be filled out by check-in staff and placed in a temporary chart.
4. If co-pay information was available on the schedule, or if the patient has a co-pay amount listed on their insurance card, the check-in person should collect as appropriate.
5. Overhead pages through the telephone system will be used to notify nursing staff when a patient is ready to be taken back.
6. Paper progress note templates should be used to record usual nurse intake.
7. Out folder is placed on exam room door as before, using the flag system to notify provider that the patient is ready.
8. Provider records notes on paper progress notes.
9. Provider orders are recorded on paper progress notes, while recording the appropriate charges for orders on the paper daybill.
10. The out folder is placed on the door and the flag system is used if nurse intervention is needed.
11. When the provider/nurse is finished with the patient, the provider will complete the encounter form (diagnosis, charges, and desired return appointment date/time) and have the patient go to check-out.

12. Encounter forms and progress notes should be kept for loading into the EHR for when the EHR operational and normal operations resume.

System Restoration:

Patient encounters occurring during system downtime should be entered into the system via the following procedures:

7. The chief complaint should be appended with "- downtime progress note attached."
    4. Paper progress notes should be attached to electronic progress notes by scanning directly onto the progress note.
    5. Billing/insurance information should be updated as necessary as the diagnosis and charges from the encounter form are entered.
    6. Immunizations should be entered into the electronic progress notes.
    7. Scheduling telephone calls should be returned. A telephone encounter does not need to be entered into the EHR.
    8. Telephone encounters for all other issues should be entered into the system and routed as appropriate.

Additional Functions:

The Practice manager is responsible for maintaining an adequate stock of paper forms in anticipation of system downtime.

Faxes will be evaluated by a nurse for urgency of review by provider.

Items requiring review by a provider will be placed in an out folder on the provider's desk.

All other phone/fax information will be scanned into the patient's record when the EHR system is operational and normal operations have resumed.

917 Emergency Access "Break the Glass" Policy Summary

The Practice has formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency. The Practice has a formal, documented emergency access procedure enabling Practice workforce members to access the minimum EPHI necessary to effectively and efficiently treat patients in the event of a major medical emergency.

Purpose

This policy reflects Practice commitment to have emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency.

Definitions

Medical emergency means medically necessary care which is immediately needed to preserve life, prevent serious impairment to bodily functions, organs, or parts, or prevent placing the physical or mental health of the patient in serious jeopardy.

Electronic protected health information (EPHI) means individually identifiable health information that is:

9. Transmitted by electronic media
10. Maintained in electronic media

Electronic media means:

1. Electronic storage media including memory devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; or

2. Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the internet, extranet (using internet technology to link a business with information accessible only to collaborating parties), leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage

media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media, because the information being exchanged did not exist in electronic form before the transmission.

Information system means an interconnected set of information resources under the same direct management control that shares common functionality. A system normally includes hardware, software, information, data, applications, communications, and people.

Workforce member means employees, volunteers, 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. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Policy
1. The Practice has formal, documented emergency access procedure enabling authorized workforce members to obtain required EPHI during a medical emergency. The procedure includes:

1. Identifying and defining which the Practice workforce members authorized to access EPHI during an emergency.
2. Identifying and defining manual and automated methods to be used by authorized Practice workforce members to access EPHI during a medical emergency.
3. Identify and define appropriate logging and auditing that must occur when authorized Practice workforce members access EPHI during an emergency.

2. The Practice has a formal, documented emergency access procedure enabling Practice workforce members to access the minimum EPHI necessary to treat patients in the event of a medical emergency. Such access must be authorized by appropriate Practice management or designated personnel.

3. Regular training and awareness on the emergency access procedure is provided to all Practice workforce members.

4. All appropriate Practice workforce members have access to a current copy of the procedure and an appropriate number of current copies of the procedure should be kept off-site.

Scope/Applicability

This policy is applicable to all divisions and workforce members that use or disclose electronic protected health information for any purposes. This policy's scope includes all electronic protected health information, as described in definitions below.

HIPAA Security
Regulatory Category: Technical Safeguards
Regulatory Type: REQUIRED Implementation Specification for Access Control Standard
Regulatory Reference: 45 CFR 164.312(a)(2)(ii)
Rule Language:

"Establish (and implement as needed) procedures for obtaining necessary electronic protected health information (EPHI) during a medical emergency."

Scenario
"Break the Glass" refers to the practice of enabling a licensed practitioner to view a patient's medical record, or a portion thereof, under emergency circumstances, when that practitioner does not have the necessary system access privileges.

Policy Authority/Enforcement
The Practice Security Officer is responsible for monitoring and enforcement of this policy.

Procedures

Mechanism to Provide Emergency Access to EPHI

1. This process will bypass formal access procedures and is limited to medical emergencies.
2. The CEO, CIO, Medical Director, or department head[31] may make requests for emergency access in writing.
3. The request should contain:
    a. The individual being granted the emergency access,
    b. Job title
    c. Reason for emergency access
    d. Date and time granted access
    e. The name of the individual granting access.
4. The Security Officer[31], or designated person, records information about emergency users and the emergency access rights assigned to them.
5. The system administrator and Security Officer[31] have created 2 administrator accounts solely for the purpose of emergency access. These accounts should be obviously named, such as breakglass01 and breakglass02 to allow for easy tracking of actions. These accounts and passwords are stored <these accounts need to be located where it would be obvious if they have been used or are missing, as though they were in a fire alarm box which required the glass to be broken to pull the alarm. A location such as in a sealed envelope taped to the side of a monitor in a very conspicuous place such as the nurses' station. Or, they can be locked in an area and require two employees, such as a manager and building security to access. There are a few EHR vendors who have "break glass" access available in their software, but that is not a common ability at this time.> [31]
6. The emergency access will be tracked and documented based on capabilities of the EHR. The tracking documentation will be reviewed by the Security Officer to determine that emergency access was appropriate.
7. At the conclusion of the event that precipitated the granting of emergency access, the Security Officer ensures the breakglass accounts are disabled, and new ones created in anticipation of the next emergency.
8. Any inappropriate use of emergency access will be treated as a security incident, and may subject an employee to disciplinary action, up to and including termination.
9. Documentation concerning emergency access will be retained and maintained for at least six years from the date of creation.

Note:
When using a specific user account that provides full access to all EPHI (an administrator account) consider the following:

1. Creating an extremely complicated password (but one an employee will be able to enter while under the stress of an emergency situation).
    11. Securing the password.
    12. Periodically changing the password.

Enforcement
Please refer to *IS-2.0 Sanction Policy* for details regarding disciplinary action against employees, contractors, or any individuals who violate this policy.

919 Sanction Policy
It is the policy of the Practice that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Practice will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.
The Practice will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Practice's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Purpose

To ensure that there are appropriate sanctions that will be applied to workforce members who violate the requirements of HIPAA, Practice's security policies, Directives, and/or any other state or federal regulatory requirements.

Definitions
Workforce member means employees, volunteers, 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. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.
Sensitive information, includes, but not limited to, the following:

13. Protected Health Information (PHI) – Individually identifiable health information that is in any form or media, whether electronic, paper, or oral.
14. Electronic Protected Health Information (ePHI) – PHI that is in electronic format.
15. Personnel files – Any information related to the hiring and/or employment of any individual who is or was employed by the Practice.
16. Payroll data – Any information related to the compensation of an individual during that individuals' employment with the Practice.
17. Financial/accounting records – Any records related to the accounting practices or financial statements of the Practice.
18. Other information that is confidential – Any other information that is sensitive in nature or considered to be confidential.

Availability refers to data or information is accessible and useable upon demand by an authorized person.
Confidentiality refers to data or information is not made available or disclosed to unauthorized persons or processes.
Integrity refers to data or information that have not been altered or destroyed in an unauthorized manner.

Violations
Listed below are the types of violations that require sanctions to be applied. They are stated at levels 1, 2, and 3 depending on the seriousness of the violation.

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name & password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the Information Security Officer, Privacy Officer, Chief Information Officer, and/or authorized designee.
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code

Level	Description of Violation
	(user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

Recommended Disciplinary Actions
In the event that a workforce member violates the Practice's privacy and security policies and/or violates the Health Insurance Portability and Accountability Act of 1996 (HIPAA) or related state laws governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on the Practice's privacy and security policies • Retraining on the proper use of internal or required forms
2	• Letter of Reprimand*; or suspension • Retraining on privacy/security awareness • Retraining on the Practice's privacy and security policies • Retraining on the proper use of internal or required forms
• 3	• Termination of employment or contract • Civil penalties as provided under HIPAA or other applicable Federal/State/Local law • Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

•

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. If formal discipline is deemed necessary, the Practice shall consult with Human Resources prior to taking action. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

*A Letter of Reprimand must be reviewed by Human Resources before given to the employee.

Exceptions
Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with the Practice.

References
U.S. Department of Health and Human Services
Health Information Privacy. Retrieved April 24, 2009, from
http://www.hhs.gov/ocr/privacy/index.html

Related Policies
Information Security Policy

Acknowledgment
I, the undersigned employee or contractor, hereby acknowledges receipt of a copy of the Sanction Policy for Practice Name[1].

Dated this _____ day of _____, 20____.

_____
Signature of Employee/Contractor

921 Employee Background Checks Policy

The Practice will conduct employment reference checks, investigative consumer reports, and/or background investigations on all candidates for employment prior to making a final offer of employment, and may use a third party to conduct these background checks. The Practice will obtain written consent from applicants and employees prior to ordering reports from third-party providers, and will provide a description of applicant and employee rights and all other documentation as required by law to each applicant or candidate in accordance with FCRA and applicable state and federal statutes. All background checks are subject to these notice and consent requirements.

An investigative consumer report compiles information on a candidate's general reputation, personal characteristics, or mode of living. This information may be gathered online including social networking sites, through public or educational records, or through interviews with employers, friends, neighbors, associates, or anyone else who may have information about the employee or potential employee. In the pre-employment process, investigative consumer reports typically include such things as criminal records checks, education verification checks, and employment verification checks.

The type of information that will be collected by the Practice in background checks may include, but is not limited to, some or all of the following:

1. Private and government agency reports related to any history of criminal, dishonest, or violent behavior, and other reports that relate to suitability for employment
2. Education (including degrees awarded and GPA)
3. Employment history, abilities, and reasons for termination of employment
4. Professional licensing board reports
5. Address history
6. Credit reports
7. Social security number scans
8. Civil court filings
9. Motor vehicle and driving records
10. Professional or personal references

This information may also be sought out at other times during employment, such as during reassignment or promotional periods, and following safety infractions or other incidents.

The Practice will conduct background checks in compliance with the federal Fair Credit Reporting Act

(FCRA), the Americans with Disabilities Act (ADA), and all other applicable local, state, and federal laws and regulations. Applicants and employees may request and receive a copy of requested "investigative consumer reports."

A reported criminal offense conviction will not necessarily disqualify a candidate from employment. The nature and seriousness of the offense, the date of the offense, the surrounding circumstances, rehabilitation, the relevance of the offense to the specific position(s), and whether hiring, transferring or promoting the applicant would pose an unreasonable risk to the business may be considered before a final decision is reached. The Practice will follow FCRA requirements, other applicable statutes, and Practice procedures for providing information and reports, making decisions, and responding to applicants and employees regarding potentially adverse actions to an investigative report.

The Practice reserves the right to withdraw any offer of employment or consideration for employment, or discharge an employee, upon finding falsification, misrepresentation, or omission of fact on an employment application, resume, or other attachments, as well as in verbal statements, regardless of when it is discovered.

Background check reports shall be maintained in separate, confidential files and retained in accordance with the Practice's document retention procedures.

923 e-Discovery Policy

It is the policy of this organization to produce and disclose relevant information and records in compliance with applicable laws, court procedures, and agreements made during the litigation process.

Purpose

The purpose of this policy is to outline the steps in the production and disclosure process for health information and records related to e-discovery for pending litigation.

Scope

This policy addresses e-discovery production and disclosure procedures related to the Federal Rules of Civil Procedures. Health information and records include both paper and electronic data related to relevant patient medical records and enterprise sources.

Procedure

Accurate Patient Identification

Responsible	Action
HIM	For litigation involving an individual's medical records, verify the patient's identity in the master patient index, including demographic information and identifiers including the medical record number. *[Note: When conducting searches, it is critical to accurately identify the correct patient and relevant information.]*
HIM	Note multiple medical record numbers, identifiers, aliases, etc., that will be used during the search process to find relevant information.

Subpoena Receipt and Response

Responsible	Action
Litigation Response Team	Upon receipt, subpoenas should be reviewed to determine that all elements are contained, the parties and the purpose are clearly identified, and the scope of information requested is clear. • Validate the served subpoenas before official acceptance. The validation process includes at a minimum:

Responsible	Action
Litigation Response Team, continued	• Verification of appropriate service of the subpoena and that the organization is under legal obligation to comply with it, and • Verification that the seal and clerk of the court signature are present and valid Review of the venue and jurisdiction of the court for the case and verification that the court is located within legal distance/mileage requirements.
HIM	Notify the Litigation Response Team that subpoena has been received and determine if a legal hold is in place. If not, the Litigation Response Team should determine whether a legal hold should be applied.
HIM	If the subpoena requests "any and all records," HIM and/or Legal Services should work with the judge and/or plaintiff's attorney to clarify the scope and type of information being requested. *[Note: The e-discovery process will identify vast volumes of data which can overwhelm a case; the parties should identify information that is necessary and relevant rather than providing all information.]*
Litigation Response Team/Legal Services	Provide direction to HIM in the processing of the subpoena, including the specific information to produce, agreed upon file formats and forms of production, whether an objection will be filed, timeframe to produce and disclose, and whether on-site testing/sampling will be conducted by the requesting party.
Litigation Response Team/Legal Services	If an outside firm is retained, such as outside counsel or discovery/litigation consultants, perform an analysis to determine if the contracted firm will have access to PHI and will need to sign a Business Associate Agreement with this organization. Execute Business Associate Agreement as appropriate.

Search and Retrieve Process

Responsible	Action
Litigation Response Team	Identify the potential sources of information which may hold potentially relevant information, such as: 11. Legal Health Record/EHR System (including source information systems such as nursing, ED, lab, radiology, etc.) 12. Local area servers for the office 13. Personal shares or personal folders on servers 14. Dedicated servers for the organization 15. Laptop and/or department computers 16. Home computers, PDAs, SmartPhones 17. E-mail, including archived e-mail and sent e-mail 18. E-mail trash bin, desktop recycle bin
Litigation Response Team, continued	19. Text/instant message archives 20. Removable storage media (e.g., disks, tapes, CDs, DVDs, memory sticks and thumb drives) 21. Department/office files such as financial records 22. Personal desk files 23. Files of administrative personnel in department/office 24. Files located in department/office staff home 25. Web site archives

Responsible	Action
HIM, Data Owners	Based on direction from the litigation response team on the potential locations of relevant information and the information agreed upon in the discovery plan and/or subpoena, establish search parameters (patient identifiers, search terms, key words, etc.) and conduct the search process. Maintain a record of the systems searched, search methodology, search parameters (terms), and search results.
IT	Provide assistance to HIM and Data Owners in the search and retrieval process for various systems and data sources.
HIM, Data Owners	Screen or filter the search results, eliminating inappropriate information (e.g., wrong patient, outside the timeframe, not relevant to the proceeding, etc.).
Legal Services	Review the content of the data/data sets found to determine relevancy to the proceeding and identify information that is considered privileged.
Legal Services, HIM, Data Owners	Determine the final list of relevant data/data sets, location, and search methodology.

Production of Records/Data

Responsible	Action
HIM, Data Owners, IT	Determine the format the information will be disclosed, such as: paper, ASCII, PDF, TIF, screen shot, mirror copy of data file, or review of material on-line. The format will vary depending on data, source, and agreement made in the Discovery Plan/Form 35.
HIM, Data Owners, IT	Produce the information in the agreed-upon format as outlined in the discovery plan/Form 35.
Legal Services, HIM, Data Owners, IT	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different patient) as appropriate.
Legal Services	Conduct final review of information before disclosing to requesting party.
Legal Services	Retain a duplicate of information disclosed to requesting party.

Charges for Copying and Disclosure

Responsible	Action
HIM, Data Owners, IT	For the information searched and disclosed, calculate the costs for search, retrieval, and disclosure methods using the organization's established formula and governmental formulas for reproduction charges.
HIM	Invoice requesting parties for allowable charges related to the reproduction of health information and records.
Legal Services	Determine whether other expenses may be charged in accordance with the discovery plan or negotiation with litigants and/or judge.

Testing and Sampling

Responsible	Action

Responsible	Action
Legal Services	A party to the legal proceeding may request to test and sample the search and retrieve methodology. Testing and sampling should be discussed and agreed upon during the pretrial conference and part of the discovery plan, including whether an external party will test and sample the search and retrieve methodologies. The costs and charges should also be determined and negotiated.
HIM, Data Owners	Retain information on all searches; including methodology, key words, and systems used in case the methodology has to be recreated for testing purposes and to determine if the sample was statistically valid.
Litigation Response Team, HIM	Assign a monitor for the outside party during their testing protocols.

Attorney/Third Party Request to Review Electronic Data

Responsible	Action
Litigation Response Team	Determine the procedures for allowing an attorney or third party to review the electronic records and search results on-line. This includes where the review will occur, system access controls, monitoring during the review session, and the charges, if any.
Legal Services, IT, HIM, Data Owners	Mask, redact, or retract non-relevant, privileged, or confidential information (such as on a different patient) as appropriate.
HIM, Data Owners	Verify the outside party is allowed access to the record and systems by reviewing all supporting documentation (e.g., signed consent, credentials from retained firm, etc.).
HIM, Data Owners	Prepare for access by identifying the types of information that party is allowed to access. If an authorization has been signed by a patient or legal representative, allow access to legal medical records and/or other information as outlined in the authorization. If other types of information will be reviewed, access is allowed based on the subpoena, court order, state/federal statutes, or agreed-upon discovery plan.

Responding to Interrogatories, Deposition, Court Procedures

Responsible	Action
Legal Services	Legal Services manages the process for completion of the interrogatories and will coordinate processes related to depositions and testifying in court.
HIM (official record custodian)	HIM may provide information for an interrogatory, be deposed, or testify in court. HIM is the official custodian of the record and can testify whether the records were kept in the normal course of business and the authenticity of the records. In addition, HIM also addresses the good faith operations related to records management, retention/destruction, and the search and retrieval process/parameters.
IT (official system custodian)	IT may provide information for an interrogatory, be deposed, or testify in court. IT is the official custodian of the information system and may testify about the technical infrastructure, system architecture, security practices, source applications, and the good faith operations from a technical infrastructure perspective.

Responsible	Action
Data Owners	Data owners may provide information for an interrogatory, be deposed, or testify in court. The data owners may testify about the specific issues related to their department/business process area.
Primary/Direct Custodian	Primary/direct custodians may provide information for an interrogatory, be deposed, or testify in court. The primary/direct custodians are those person(s) who work with the data directly or have direct involvement/knowledge of the events the litigation. For example, a staff nurse who has made an entry into the medical record and is knowledgeable about the events of a case in litigation.
Business Associates/Third Parties	Business Associates/Third Parties may provide information for an interrogatory, be deposed, or testify in court. These include contractors and others who serve a variety of functions associated with a party's information but who themselves are not parties to the litigation. Examples include Internet service providers, application service providers such as a claims clearinghouse, and other providers who provide services ranging from off-site data storage to complete outsourcing of the IT Department.

925 e-Disovery Policy: Retention
It is the policy of this organization to maintain and retain enterprise health information and records in compliance with applicable governmental and regulatory requirements. This organization will adhere to retention schedules and destruction procedures in compliance with regulatory, business, and legal requirements.

Purpose
The purpose of this policy is to achieve a complete and accurate accounting of all relevant records within the organization; to establish the conditions and time periods for which paper based and electronic health information and records will be stored, retained, and destroyed after they are no longer active for patient care or business purposes; and to ensure appropriate availability of inactive records.

Scope
This policy applies to all enterprise health information and records whether the information is paper based or electronic. It applies to any health record, regardless of whether it is maintained by the Health Information Management Department or by the clinical or ancillary department that created it.

Definitions
Data Owners: Each department or unit that maintains patient health records, either in electronic or paper form, is required to designate a records management coordinator who will ensure that records in his or her area are preserved, maintained, and retained in compliance with records management policies and retention schedules established by the Health Information Management Department *[or other designated authority]*.

Property Rights: All enterprise health information and records generated and received are the property of the organization. No employee, by virtue of his or her position, has any personal or property right to such records even though he or she may have developed or compiled them.

Workforce Responsibility: All employees and agents are responsible for ensuring that enterprise health information and records are created, used, maintained, preserved, and destroyed in accordance with this policy.

Destruction of Enterprise Health Information and Records: At the end of the designated retention period for each type of health information and record, it will be destroyed in accordance with the procedures in this policy unless a legal hold/preservation order exists or is anticipated.

Unauthorized Destruction: The unauthorized destruction, removal, alteration, or use of health information and records is prohibited. Persons who destroy, remove, alter or use health information and records in an unauthorized manner will be disciplined in accordance with the organization's Sanction Policy.

Procedure

Responsible	Action
Data Owner/Departments	Data owners/departments will designate records coordinator for their areas and report that designation to the Records Committee and Litigation Response Team.
Record Committee	*[Note: This may be an existing committee, such as the Medical Record Committee, that has membership representing Legal, Compliance, IS/IT, Information Security, HIM, Clinical, and others as appropriate]* The record committee's role is to authorize any changes to the Retention, Storage, and Destruction policies and procedures; review and approve retention schedules and revisions to current retention schedules; address compliance audit findings; and review and approve control forms relating to business records.
HIM	HIM will convene the Record Committee as needed *[or at regular intervals]* and maintain responsibility for the following: 26. Review, maintain, publish, and distribute retention schedules and records management policies. 27. Audit compliance with records management (both electronic and paper) policies and retention schedules and report findings to Record Committee. 28. Serve as point of contact for Records Coordinators. 29. Provide training for Records Coordinators. Training will be provided on an individual basis to Records Coordinators and any individual or department that needs assistance. 30. Oversee operation of designated offsite record storage center(s) for archival storage of paper health information and records or serve as contract administrator for such services. 31. Contract for destruction of paper and electronic records and certification thereof.
IT/HIM/Data Owners	IT/HIM/Data Owners will ensure that electronic storage of enterprise health information and records is carried out in conjunction with archiving and retention policies.
Records Coordinators	Records coordinators are responsible for implementing and maintaining records management programs for their designated areas. They will organize and manage online records management control forms relating to enterprise records and information in their areas of responsibility to accomplish the following: 32. Transfer records to storage 33. Identify, control, and maintain records in storage 34. Retrieve and/or return records from/to storage 35. Document the destruction of records and the deletion of records from the records inventory 36. Monitor the records management process Record coordinators will obtain (if not already trained) and maintain records management skills.

Responsible	Action
Legal Services	Legal Services serves as subject matter expert and provides counsel regarding records designations and legal and statutory requirements for records retention and pending legal matters. It ensures that access to or ownership of records is appropriately protected in all divestitures of property or lines of business or facility closures.

Guidelines for Retention of Records/Information and Schedules:

Record Retention	Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention period has expired, the record is approved for destruction by the record owner, and a Certificate of Destruction is executed.
Non-record Retention	Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated. For example, when the non-record information, such as an employee's personal notes, is transferred to a record, such as an incident report, the notes are no longer useful and should be discarded. Preliminary working papers and superseded drafts should be discarded, particularly after subsequent versions are finalized. Instances where an author or recipient of a document is unsure whether a document is a record as covered or described in this policy should be referred to the Compliance Officer for determination of its status and retention period.
E-mail Communication Retention	Depending on content, e-mail messages between clinicians and between patients and clinicians and documents transmitted by e-mail may be considered records and are subject to this policy. If an e-mail message would be considered a record based on its content, the retention period for that e-mail message would be the same for similar content in any other format. The originator/sender of the e-mail message (or the recipient of a message if the sender is outside Organization) is the person responsible for retaining the message if that message is considered a record. Users must save e-mail messages in a manner consistent with departmental procedures for retaining other information of similar content. Users should be aware of *Messaging Policies* that establish disposal schedules for e-mail and manage their e-mail accordingly.

Development of Records Retention Schedules	Retention Schedule Determined by Law: All records will be maintained and retained in accordance with Federal and state laws and regulations. *[Note: minimum retention schedules are attached to this policy]*. Electronic records must follow the same retention schedule as physical records, acknowledging the format and consolidated nature of records within an application or database. Changes to Retention Schedule: Proposed changes to the record retention schedules will be submitted to the Records Committee for initial review. The Records Committee, in consultation with the Legal Services Department, will research the legal, fiscal, administrative, and historical value of the records to determine the appropriate length of time the records will be maintained and provide an identifying code. The proposed revisions will be submitted to the Records Committee for review and approval. The approved changes will be published and communicated to the designated Records Coordinators. Retention of Related Computer Programs: Retention of records implies the inherent ability to retrieve and view a record within a reasonable time. Retained electronic data must have retained with it the programs required to view the data. Where not economically feasible to pay for maintenance costs on retired or obsolete hardware or software only for the purpose of reading archived or retained data, then data may be converted to a more supportable format, as long as it can be demonstrated that the integrity of the information is not degraded by the conversion. Data Owners should work closely with IT personnel in order to comply with this section. Retention of Records in Large Applications: Retention of data for large-scale applications, typically those that reside in the data center and are accessed by a larger audience, shall be the responsibility of the IT department. Retention of Records on Individual Workstations: Primary responsibility for retention of data created at the desktop level—typically with e-mail, Microsoft "Office" applications such as Word, Excel, PowerPoint, Access, or other specialized but locally run and saved computer applications—shall be with the user/author. The user/author will ensure that the documents are properly named and saved to be recognizable by the user in the future, and physically saved to a "shared drive." By saving a copy in this manner, IT will create an archive version of the saved document for a specified number of years after the user deletes the copy from the shared drive. Records with retention periods in excess of this period will require an alternative means of retention. Users are responsible for the security of any confidential information and/or protected health information created or maintained on their workstations.

Storage and Destruction Guidelines

Active/Inactive Records	Records are to be reviewed periodically by the Data Owner to determine if they are in the active, inactive, or destruction stage. Records that are no longer active will be stored in the designated off-site storage facility. Active stage is that period when reference is frequent and immediate access is important. Records should be retained in the office or close to the users. Data Owners, through their Records Coordinator, are responsible for maintaining the records in an orderly, secure, and auditable manner throughout this phase of the record life-cycle.
Active/Inactive Records, continued	Inactive stage is that period when records are retained for occasional reference and for legal reasons. Inactive records for which scheduled retention periods have not expired or records scheduled for permanent retention will be cataloged and moved to the designated off-site storage facility. Destruction stage is that period after records have served their full purpose, their mandated retention period, and finally are no longer needed.

Storage of Inactive Records	All inactive records identified for storage will be delivered with the appropriate Records Management Forms to the designated off-site storage facility where the records will be protected, stored, and will remain accessible and cataloged for easy retrieval. Except for emergencies, the designated off-site storage facility will provide access to records during normal business hours.
Records Destruction	General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules. Permanent Records: Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the record may be destroyed in accordance with the Records Retention Schedules but in no case shall records used in evidence to litigation be destroyed earlier than a specified number of years from the date of the settlement of litigation. Destruction of Records Containing Confidential Information: Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable. The approved methods to destroy records include: *[Note: specify based on local, state, and federal rule; these could potentially include recycling, shredding, burning, pulping, pulverizing, and magnetizing.]*[31] A Certificate of Destruction form must be approved and signed by the appropriate management staff prior to the destruction of records. The Certificate of Destruction shall be retained by the off-site storage facility manager. Destruction of Non-Records Containing Confidential Information: Destruction Non-Records containing personal health information or other forms of confidential corporate, employee, member, or patient information of any kind shall be rendered unrecognizable for both source and content by means of shredding, pulping, etc., regardless of media. This material shall be deposited in on-site, locked shred collection bins or boxed, sealed, and marked for destruction. Disposal of Electronic Storage Media: Electronic storage media must be assumed to contain confidential or other sensitive information and must not leave the possession of the organization until confirmation that the media is unreadable or until the media is physically destroyed.
Records Destruction, continued	Disposal of Electronic Media: Electronic storage media, such as CD-ROMS, DVDs, tapes, tape reels, USB thumb drives, disk drives or floppy disks containing confidential or sensitive information may only be disposed of by approved destruction methods. These methods include: *[Note: specify based on local, state, and federal rules; these could potentially include: burning, shredding, or some other approach which renders the media unusable; degaussing, which uses electro-magnetic fields to erase data; or, preferred for magnetic media when media will not be physically destroyed, "zeroization" programs (a process of writing repeated sequences of ones and zeros over the information)]*[31]. CD-ROMs, DVDs, magneto-optical cartridges and other storage media that do not use traditional magnetic recording approaches must be physically destroyed. Disposal of IT Assets: Department managers must coordinate with the IT Department on disposing surplus property that is no longer needed for business activities according to the Disposal of IT Assets Policy. Disposal of information system equipment, including the irreversible removal of information and software, must occur in accordance with approved procedures and will be coordinated by IT personnel.

927 Breach Notification Purpose and Procedures
To outline the process for notifying affected individuals of a breach of protected information under the Privacy Act, unsecured protected health information (PHI) for the purposes of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), Health Information Technology for Economic and Clinical Health Act (HITECH), and/or state breach notification purposes.

Scope
This applies to all employees, volunteers, and other individuals working under contractual agreements with the Practice.

Definitions
State Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of Personal Information that compromises the security, confidentiality, or integrity of the Personal Information.

Personal Information – Personal Information has many definitions including definitions by statute which may vary from state to state. Most generally, Personal Information is a combination of data elements which could uniquely identify an individual. Please review applicable state data breach statutes to determine what definition of Personal Information is applicable for purposes of the document.

HIPAA Breach – Unauthorized acquisition, access, use, or disclosure of unsecured PHI.

Personally Identifiable Information (PII) – Information in any form that consists of a combination of an individual's name and one or more of the following: Social Security Number, driver's license or state ID, account numbers, credit card numbers, debit card numbers, personal code, security code, password, personal ID number, photograph, fingerprint, or other information which could be used to identify an individual.

Individually Identifiable Health Information (IIHI) – PII which includes information related to the past, present or future condition, treatment, payment or provision of health care to the identified individual.

Privacy Act Breach – Unauthorized acquisition or reasonable belief of unauthorized acquisition of personal information protected by the Privacy Act. This information includes, but is not limited to Social Security Number, government issued ID numbers, financial account numbers or other information posing a risk of identity theft.

Private Information – Information protected by the Privacy Act, Personally Identifiable Information, Personal Information and Protected Health Information collectively.

Protected Health Information (PHI) – Individually identifiable health information except for education records covered by FERPA and employment records.

Procedure
Reporting a Possible Breach

1. Any employee who becomes aware of a possible breach of privacy involving Private Information in the custody or control of the Practice will immediately inform their supervisor/manager, and the Privacy Officer.
2. Notification should occur immediately upon discovery of a possible breach or before the end of your shift if other duties interfere, however, in no case should notification occur later than twenty-four (24) hours after discovery.
    a. The supervisor/manager will verify the circumstances of the possible breach and inform the Privacy Officer and the division Administrator/Director within twenty-four (24) hours of the initial report.
3. You may call the Privacy Officer directly at _____-_____[32].
    a. Provide the Privacy Officer with as much detail as possible.
    b. Be responsive to requests for additional information from the Privacy Officer.
    c. Be aware that the Privacy Officer has an obligation to follow up on any reasonable belief that Private Information has been compromised.

4. The Privacy Officer, in conjunction with the Practice's Legal Counsel, will decide whether or not to notify the President/CEO as appropriate by taking into consideration the seriousness and scope of the breach.

Containing the Breach

1. The Privacy Officer will take the following steps to limit the scope and effect of the breach.
    a. Work with department(s) to immediately contain the breach. Examples include, but are not limited to:
        i. Stopping the unauthorized practice
        ii. Recovering the records, if possible
        iii. Shutting down the system that was breached
        iv. Mitigating the breach, if possible
        v. Correcting weaknesses in security practices
        vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity

Investigating and Evaluating the Risks Associated with the Breach

1. To determine what other steps are immediately necessary, the Privacy Officer in collaboration with the Practice's Legal Counsel and affected department(s) and administration, will investigate the circumstances of the breach.
    a. A team will review the results of the investigation to determine root cause(es), evaluate risks, and develop a resolution plan.
        i. The Privacy Breach Assessment tool will help aid the investigation.
    b. The Privacy Officer, in collaboration with the Practice's Legal Counsel, will consider several factors in determining whether to notify individuals affected by the breach including, but not limited to:
        i. Contractual obligations
        ii. Legal obligations – the Practice's Legal Counsel should complete a separate legal assessment of the potential breach and provide the results of the assessment to the Privacy Officer and the rest of the breach response team
        iii. Risk of identity theft or fraud because of the type of information lost such as social security number, banking information, identification numbers
        iv. Risk of physical harm if the loss puts an individual at risk of stalking or harassment
        v. Risk of hurt, humiliation, or damage to reputation when the information includes medical or disciplinary records
        vi. Number of individuals affected

Notification

1. The Privacy Officer will work with the department(s) involved, the Practice's Legal Counsel and appropriate leadership to decide the best approach for notification and to determine what may be required by law.
2. If required by law, notification of individuals affected by the breach will occur as soon as possible following the breach.
    a. Affected individuals must be notified without reasonable delay, but in no case later than sixty (60) calendar days after discovery, unless instructed otherwise by law enforcement or other applicable state or local laws.
        i. Notices must be in plain language and include basic information, including:
            1. What happened
            2. Types of PHI involved
            3. Steps individuals should take
            4. Steps covered entity is taking
            5. Contact Information
        ii. Notices should be sent by first-class mail or if individual agrees electronic mail. If insufficient or out-of-date contact information is available, then a substitute notice is required as specified below.

    b. If law enforcement authorities have been contacted, those authorities will assist in determining whether notification may be delayed in order not to impede a criminal investigation.
3. The required elements of notification vary depending on the type of breach and which law is implicated. As a result, the Practice's Privacy Officer and Legal Counsel should work closely to draft any notification that is distributed.
4. Indirect notification such as website information, posted notices, media will generally occur only where direct notification could cause further harm, or contact information is lacking.
    a. If a breach affects five-hundred (500) or more individuals, or contact information is insufficient, the Practice will notify a prominent media outlet that is appropriate for the size of the location with affected individuals, and notice will be provided in the form of a press release.
5. Using multiple methods of notification in certain cases may be the most effective approach.

Business associates must notify the Practice if they incur or discover a breach of unsecured PHI.

1. Notices must be provided without reasonable delay and in no case later than sixty (60) days after discovery of the breach.
2. Business associates must cooperate with the Practice in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If the Practice's Legal Counsel determines that HIPAA notification is not required; this notice is also not required.

1. Information regarding breaches involving five-hundred (500) or more individuals, regardless of location, must be submitted to HHS at the same time that notices to individuals are issued.
2. If a breach involves fewer than five-hundred (500) individuals, the Practice will be required to keep track of all breaches and to notify HHS within sixty (60) days after the end of the calendar year.

Prevention

1. Once immediate steps are taken to mitigate the risks associated with the breach, the Privacy Officer will investigate the cause of the breach.
    a. If necessary, this will include a security audit of physical, organizational, and technological measures.
    b. This may also include a review of any mitigating steps taken.
2. The Privacy Officer will assist the responsible department to put into effect adequate safeguards against further breaches.
3. Procedures will be reviewed and updated to reflect the lessons learned from the investigation and regularly thereafter.
4. The resulting plan will also include audit recommendations, if appropriate.

Compliance and Enforcement
All managers and supervisors are responsible for enforcing these procedures. Employees who violate these procedures are subject to discipline up to and including termination in accordance with the Practice's Sanction Policy.

929 Approved Software
The following list has been approved for use by the Practice. All software must be installed and maintained by the appropriate Practice personnel.

Software	Version	Approved by	Date	Description/Comments

Software	Version	Approved by	Date	Description/Comments

931 Approved Vendors

Vendor	Primary Contact	Main Number	Product / Service	Description/Comments

933 Credit Card Security Policies

Introduction
This document explains Sparks Family Medicine's credit card security requirements as required by the Payment Card Industry Data Security Standard (PCI DSS) Program. Sparks Family Medicine management is committed to these security policies to protect information utilized by Sparks Family Medicine in attaining its business goals. All employees are required to adhere to the policies described within this document.

Scope of Compliance
The PCI requirements apply to all systems that store, process, or transmit cardholder data. Currently, Sparks Family Medicine's cardholder environment consists only of limited payment applications (typically point-of-sale systems) connected to the internet, but does not include storage of cardholder data on any computer system.
Due to the limited nature of the in-scope environment, this document is intended to meet the PCI requirements as defined in Self-Assessment Questionnaire (SAQ) C, ver. 2.0, October, 2010. Should Sparks Family Medicine implement additional acceptance channels, begin storing, processing, or transmitting cardholder data in electronic format, or otherwise become ineligible to validate compliance under SAQ C, it will be the responsibility of Sparks Family Medicine to determine the appropriate compliance criteria and implement additional policies and controls as needed.

Requirement 1: Build and Maintain a Secure Network

Firewall Configuration

Firewalls must restrict connections between untrusted networks and any system in the cardholder data environment. An "untrusted network" is any network that is external to the networks belonging to the entity under review, and/or which is out of the entity's ability to control or manage. (PCI Requirement 1.2)

Inbound and outbound traffic must be restricted to that which is necessary for the cardholder data environment. All other inbound and outbound traffic must be specifically denied. (PCI Requirement 1.2.1)

All open ports and services must be documented. Documentation should include the port or service, source and destination, and a business justification for opening said port or service. (PCI Requirement 1.2.1)

Perimeter firewalls must be installed between any wireless networks and the cardholder data environment. These firewalls must be configured to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. (PCI Requirement 1.2.3)

Firewall configuration must prohibit direct public access between the Internet and any system component in the cardholder data environment as follows:

- Direct connections are prohibited for inbound and outbound traffic between the Internet and the cardholder data environment (PCI Requirement 1.3.3)
- Outbound traffic from the cardholder data environment to the Internet must be explicitly authorized (PCI Requirement 1.3.5)
- Firewalls must implement stateful inspection, also known as dynamic packet filtering (PCI Requirement 1.3.6)

Any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are to access the organization's network must have a local (personal) software firewall installed and active. This firewall must be configured to specific standards, and not alterable by mobile and/or employee-owned computer users. (PCI Requirement 1.4)

Requirement 2: Do not use Vendor-Supplied Defaults for System Passwords and Other Security Parameters

Vendor Defaults

Vendor-supplied defaults must always be changed before installing a system on the network. Examples of vendor-defaults include passwords, SNMP community strings, and elimination of unnecessary accounts. (PCI Requirement 2.1)

Default settings for wireless systems must be changed before implementation. Wireless environment defaults include, but are not limited to:

- default encryption keys
- passwords
- SNMP community strings
- default passwords/passphrases on access points
- other security-related wireless vendor defaults as applicable

Firmware on wireless devices must be updated to support strong encryption for authentication and transmission of data over wireless networks. (PCI Requirement 2.1.1)

Unneeded Services and Protocols

Only necessary services, protocols, daemons, etc., as needed for the function of the system may be enabled. All services and protocols not directly needed to perform the device's specified function must be disabled. (PCI Requirement 2.2.2)

Non-Console Administrative Access

Credentials for non-console administrative access must be encrypted using technologies such as SSH, VPN, or SSL/TLS. Encryption technologies must include the following: (PCI Requirement 2.3)

Must use strong cryptography, and the encryption method must be invoked before the administrator's password is requested.

System services and parameter files must be configured to prevent the use of telnet and other insecure remote login commands.

Must include administrator access to web-based management interfaces

Requirement 3: Protect Stored Cardholder Data

Prohibited Data

Processes must be in place to securely delete sensitive authentication data post-authorization so that the data is unrecoverable. (PCI Requirement 3.2)

Payment systems must adhere to the following requirements regarding non-storage of sensitive authentication data after authorization (even if encrypted):

The full contents of any track data from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere) are not stored under any circumstance. (PCI Requirement 3.2.1)

The card verification code or value (three-digit or four-digit number printed on the front or back of a payment card) is not stored under any circumstance. (PCI Requirement 3.2.2)

The personal identification number (PIN) or the encrypted PIN block are not stored under any circumstance. (PCI Requirement 3.2.3)

Displaying PAN

Sparks Family Medicine will mask the display of PANs (primary account numbers), and limit viewing of PANs to only those employees and other parties with a legitimate need. A properly masked number will show only the first six and the last four digits of the PAN. (PCI requirement 3.3)

Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

Transmission of Cardholder Data

Cardholder data sent across open, public networks must be protected through the use of strong cryptography or security protocols (e.g., IPSEC, SSLTLS). Only trusted keys and/or certificates can be accepted. For SSL/TLS implementations HTTPS must appear as part of the URL, and cardholder data may only be entered when HTTPS appears in the URL. (PCI Requirement 4.1)

Industry best practices (for example, IEEE 802.11i) must be used to implement strong encryption for authentication and transmission for wireless networks transmitting cardholder data or connected to the cardholder data environment. (PCI Requirement 4.1.1)

Sending unencrypted PANs by end-user messaging technologies is prohibited. Examples of end-user technologies include email, instant messaging and chat. (PCI requirement 4.2)

Requirement 5: use and Regularly Update Anti-Virus Software or Programs

Anti-Virus

All systems, particularly personal computers and servers commonly affected by viruses, must have installed an anti-virus program which is capable of detecting, removing, and protecting against all know types of malicious software. (PCI Requirement 5.1, 5.1.1)

All anti-virus programs must be kept current through automatic updates, be actively running, be configured to run periodic scans, and capable of generating audit logs. Anti-virus logs must be retained in accordance with PCI requirement 10.7. (PCI Requirement 5.2)

Requirement 6: Develop and Maintain Secure Systems and Applications

Security Patches

All critical security patches must be installed with one month of release. This includes relevant patches for operating systems and all installed applications. (PCI Requirement 6.1)

Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

Limit Access to Cardholder Data

Access to Sparks Family Medicine's cardholder system components and data is limited to only those individuals whose jobs require such access. (PCI Requirement 7.1)

Access limitations must include the following:

Access rights for privileged user IDs must be restricted to the least privileges necessary to perform job responsibilities. (PCI Requirement 7.1.1)

Privileges must be assigned to individuals based on job classification and function (also called "role-based access control). (PCI Requirement 7.1.2)

Requirement 8: Assign a Unique ID to Each Person with Computer Access

Remote Access

Two-factor authentication must be incorporated for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (PCI Requirement 8.3)

Vendor Accounts

All accounts used by vendors for remote maintenance shall be enabled only during the time period needed. Vendor remote access accounts must be monitored when in use. (PCI Requirement 8.5.6)

Requirement 9: Restrict Physical Access to Cardholder Data

Physically Secure all Media Containing Cardholder Data

Hard copy materials containing confidential or sensitive information (e.g., paper receipts, paper reports, faxes, etc.) are subject to the following storage guidelines:

All media must be physically secured. (PCI requirement 9.6)

Strict control must be maintained over the internal or external distribution of any kind of media containing cardholder data. These controls shall include:

- Media must be classified so the sensitivity of the data can be determined. (PCI Requirement 9.7.1)
- Media must be sent by a secure carrier or other delivery method that can be accurately tracked. (PCI Requirement 9.7.2)

Logs must be maintained to track all media that is moved from a secured area, and management approval must be obtained prior to moving the media. (PCI Requirement 9.8)

Strict control must be maintained over the storage and accessibility of media containing cardholder data. (PCI Requirement 9.9)

Destruction of Data

All media containing cardholder data must be destroyed when no longer needed for business or legal reasons. (PCI requirement 9.10)

Hardcopy media must be destroyed by shredding, incineration or pulping so that cardholder data cannot be reconstructed. Container storing information waiting to be destroyed must be secured to prevent access to the contents. (PCI requirement 9.10.1)

Requirement 10: Regularly Test Security Systems and Processes

Testing for Unauthorized Wireless Access Points

At least quarterly, Sparks Family Medicine will perform testing to ensure there are no unauthorized wireless access points present in the cardholder environment. (PCI Requirement 11.1)

This testing must detect and identify any unauthorized wireless access points, including at least the following:

- WLAN cards inserted into system components
- Portable wireless devices connected to system components (for example, by USB, etc.)
- Wireless devices attached to a network port or network device

If automated monitoring is utilized (for example, wireless IDS/IPS, NAC, etc.) it must be configured to generate alerts.
Detection of unauthorized wireless devices must be included in the Incident Response Plan (see PCI Requirement 12.9).

Vulnerability Scanning

At least quarterly, and after any significant changes in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades), Sparks Family Medicine will perform vulnerability scanning on all in-scope systems. (PCI Requirement 11.2)

Internal vulnerability scans must be repeated until passing results are obtained, or until all “high” vulnerabilities as defined in PCI Requirement 6.2 are resolved. (PCI Requirement 11.2.1, 11.2.3)

Quarterly vulnerability scan results must satisfy the ASV Program guide requirements (for example, no vulnerabilities rated higher than a 4.0 by the CVSS and no automatic failures. External vulnerability scans must be performed by an Approved Scanning Vendor (ASV), approved by the Payment Card Industry Security Standards Council (PCI SSC). (PCI Requirement 11.2.2, 11.2.3)

Requirement 11: Maintain a Policy that Addresses Information Security for Employees and Contractors

Security Policy

Sparks Family Medicine shall establish, publish, maintain, and disseminate a security policy that addresses how the company will protect cardholder data. (PCI Requirement 12.1)

This policy must be reviewed at least annually, and must be updated as needed to reflect changes to business objectives or the risk environment. (PCI requirement 12.1.3)

Critical Technologies

Sparks Family Medicine shall establish usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email, and internet usage. (PCI requirement 12.3)

These policies must include the following:

- Explicit approval by authorized parties to use the technologies (PCI Requirement 12.3.1)
- Authentication for use of the technology (PCI Requirement 12.3.2)
- A list of all such devices and personnel with access (PCI Requirement 12.3.3)
- Acceptable uses of the technologies (PCI Requirement 12.3.5)
- Acceptable network locations for the technologies (PCI Requirement 12.3.6)
- Automatic disconnect of sessions for remote-access technologies after a specific period of inactivity (PCI Requirement 12.3.8)

Activation of remote-access technologies for vendors and business partners only when needed by vendors and business partners, with immediate de-activation after use (PCI Requirement 12.3.9)

Security Responsibilities

Sparks Family Medicine's policies and procedures must clearly define information security responsibilities for all personnel. (PCI Requirement 12.4)

Incident Response Policy

The Privacy Officer shall establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI requirement 12.5.3)

Incident Identification

Employees must be aware of their responsibilities in detecting security incidents to facilitate the incident response plan and procedures. All employees have the responsibility to assist in the incident response procedures within their particular areas of responsibility. Some examples of security incidents that an employee might recognize in their day to day activities include, but are not limited to,

- Theft, damage, or unauthorized access (e.g., papers missing from their desk, broken locks, missing log files, alert from a security guard, video evidence of a break-in or unscheduled/unauthorized physical entry)
- Fraud – Inaccurate information within databases, logs, files or paper records

Reporting an Incident

The Privacy Officer should be notified immediately of any suspected or real security incidents involving cardholder data:

Contact the Privacy Officer to report any suspected or actual incidents. The Internal Audit's phone number should be well known to all employees and should page someone during non-business hours.

No one should communicate with anyone outside of their supervisor(s) or the Privacy Officer about any details or generalities surrounding any suspected or actual incident. All communications with law enforcement or the public will be coordinated by the Privacy Officer.

Document any information you know while waiting for the Privacy Officer to respond to the incident. If known, this must include date, time, and the nature of the incident. Any information you can provide will aid in responding in an appropriate manner.

Incident Response

Responses can include or proceed through the following stages: identification, severity classification, containment, eradication, recovery and root cause analysis resulting in improvement of security controls.

Contain, Eradicate, Recover and perform Root Cause Analysis

1. Notify applicable card associations.

Visa

Provide the compromised Visa accounts to Visa Fraud Control Group within ten (10) business days. For assistance, contact 1-(650)-432-2978. Account numbers must be securely sent to Visa as instructed by the Visa Fraud Control Group. It is critical that all potentially compromised accounts are provided. Visa will distribute the compromised Visa account numbers to issuers and ensure the confidentiality of entity and non-public information. See Visa's "What to do if compromised" documentation for additional activities that must be performed. That documentation can be found at

http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_what_to_do_if_compromised.pdf

MasterCard

Contact your merchant bank for specific details on what to do following a compromise. Details on the merchant bank (aka. the acquirer) can be found in the Merchant Manual at http://www.mastercard.com/us/wce/PDF/12999_MERC-Entire_Manual.pdf. Your merchant bank will assist when you call MasterCard at 1-(636)-722-4100.

Discover Card

Contact your relationship manager or call the support line at 1-(800)-347-3083 for further guidance.

2. Alert all necessary parties. Be sure to notify:
   a. Merchant bank
   b. Local FBI Office
   c. U.S. Secret Service (if Visa payment data is compromised)
   d. Local authorities (if appropriate)
3. Perform an analysis of legal requirements for reporting compromises in every state where clients were affected. The following source of information must be used: http://www.ncsl.org/programs/lis/cip/priv/breach.htm
4. Collect and protect information associated with the intrusion. In the event that forensic investigation is required the Privacy Officer will work with legal and management to identify appropriate forensic specialists.
5. Eliminate the intruder's means of access and any related vulnerabilities.
6. Research potential risks related to or damage caused by intrusion method used.

Root Cause Analysis and Lessons Learned

Not more than one week following the incident, the Privacy Officer and all affected parties will meet to review the results of any investigation to determine the root cause of the compromise and evaluate the effectiveness of the *Incident Response Plan*. Review other security controls to determine their appropriateness for the current risks. Any identified areas in which the plan, policy or security control can be made more effective or efficient, must be updated accordingly.

Security Awareness

Sparks Family Medicine shall establish and maintain a formal security awareness program to make all personnel aware of the importance of cardholder data security. (PCI Requirement 12.6)

Service Providers

Sparks Family Medicine shall implement and maintain policies and procedures to manage service providers. (PCI requirement 12.8)

This process must include the following:

- ❑ Maintain a list of service providers (PCI requirement 12.8.1)
- ❑ Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of the cardholder data the service providers possess (PCI requirement 12.8.2)

- ❑ Implement a process to perform proper due diligence prior to engaging a service provider (PCI requirement 12.8.3)
    - ❑ Monitor service providers' PCI DSS compliance status (PCI requirement 12.8.4)

Appendix E – Incident Response Tools

Tool	Attached Form/Worksheet	Description
Security Incident Report	Security_Incident-Report-Confidential.doc	Security incident report utilized by the reporting employee or witness to an incident or potential incident.
Security Incident Investigation	Security_Incident-Investigation-Confident	Security incident investigation report that that allows for further investigation of a potential incident upon receipt of the initial security incident report.
Security Incident Log	Security_Incident-Log-Confidential.xls	Security incident log to ensure incidents are tracked for further analysis and follow-up.
Security Breach Assessment Tool	Security_Incident-Breach Assessment-Cor	Privacy breach assessment tool which can assist in determining the severity of a breach.

933 Incident Response Tools
Security Incident Report: Security incident report utilized by the reporting employee or witness to an incident or potential incident (follows).

Security Incident Investigation: Security incident investigation report that that allows for further investigation of a potential incident upon receipt of the initial security incident report (follows).

Security Incident Log: Security incident log to ensure incidents are tracked for further analysis and follow-up (follows).

Security Breach Assessment Tool: Privacy breach assessment tool which can assist in determining the severity of a breach, (follows).

SECURITY INCIDENT REPORT
Sparks Family Medicine, Ltd Location

Directions: The reporting Colleague or witness needs to complete Section 1 and Section 2. The Colleague or witness can consult with the IT Department to complete Section 2. All persons who contribute information to the report should be recorded in the "Report Augmented By" field. When completed, the form should be **submitted to the Security Officer** with a copy to be retained by the reporting Colleague or witness and, if applicable, provided to the Office Manager. The completed form should be submitted **within 24 hours of discovery of the incident or event**. Please print clearly or type.

Section 1: Incident Reporter			
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			
(If Available) Alternate Phone Number:			
Report Submitted To – **Indicate name and title**:			
Section 2: Incident Details			
Date and Time of Discovery of Incident:		Estimated Date and Time Incident Started:	
Description of Incident – **Be Specific**:			
PHI Compromise Suspected?	☐ Yes ☐ No		
Location of Incident:			
Current Status of Incident:			
Source or Cause of Incident:			
Employees, Contractors or Others with Incident Knowledge – **List all known potential witnesses**:			
Operating System, version, and patch level:			
Antivirus Software Installed, Enabled and Updated?	☐ Yes ☐ No Comments:		
Description of Affected Resources:			
Mitigating Factors:			
Estimated Technical Impact of Incident:			
Response Actions Performed:			
Other Organizations Contacted:			
Report Augmented By:			
Additional Comments:			

I understand that by submitting this Incident Report in good faith, I cannot be subject to retaliation. I attest that the information contained in this Incident Report is true and accurate to the best of my knowledge on the date indicated below. If I obtain any additional information regarding this incident, I agree to provide said supplementary information to the person specified above in "Report Submitted To" and/or the designated Incident Handler. I agree to cooperate fully with all investigators of this incident until the incident is closed.

_____ _____
Incident Reporter's Signature Date

SECURITY INCIDENT REPORT INSTRUCTIONS

- **Report Number** should be left blank; this will be completed by the Incident Handler.
- **Time** should be recorded in the 24 hour format and include the time zone of the primary location of the incident. Unless otherwise noted, the time zone will default to your primary office location.
- **Description of the Incident** may include how it was detected, what occurred, who detected it, etc.
- **PHI Compromise Suspected** should be "Yes" if there is any concern by any person contributing to this report that personal health information (PHI) was compromised. "No" should only be indicated if all persons contributing to the report are certain that PHI was not compromised.
- **Location of Incident** may be a campus, building, department, or room. Please be as specific as possible.
- **Current Status of the Incident** may be an ongoing attack, one time occurrence, resolved issue, etc.
- **Source or Cause of Incident** (if known) may include the computer's location, host name, and/or IP address; user account; etc.
- **Contact Information** should include name, title, organization, phone number and email (as known).
- **Operating System** may include Windows XP, Vista, or 7; Windows Server 2003 or 2008; Mac; Linux; Unix; etc.
- **Affected Resources** may include a network device, a workstation, an application, or specific data and may be described as hardware location, IP address, and host name; a system name, location, and function; a user account; etc.
- **Technical Impact** may include data deleted or compromised, system crashed, application unavailable, nonfunctional workstation, etc.
- **Response Action Performed** may include shutting off the computer, disconnecting the computer from the network, beginning malicious software removal, disabling an affected user account, etc.; documentation should include the action taken and identify who took the action.
- **Organizations Contacted** may include software vendor(s), hardware vendor(s), contracted IT support and others; recorded information should include organization, contact's name, date and time of initial contact, and contact method (phone, email, etc.). Any response from the contacted organizations should be noted in the Additional Comments field.
- **Report Augmented By** should list the contact information of everyone except the initial reporter who provided data for the report.

This Report is based on the guidelines found in Appendix 3 of NIST SP 800-61 Rev. 1: *Computer Security Incident Handling Guide*. A list of all NIST 800 publications can be found at http://csrc.nist.gov/publications/PubsSPs.html.

SECURITY INCIDENT INVESTIGATION REPORT
Sparks Family Medicine, Ltd Location

Directions: Upon receipt of a Security Incident Report, an investigation into the incident shall be initiated. The Security Incident Investigation Report should be completed as thoroughly as possible by the Incident Handler and Investigators. Since investigations vary, some sections may not be applicable to every investigation. Please print clearly or type.

Section 1: Incident Handler			
Date Report Received:		Date Report Processing Began:	
Name:		Report Number:	
Title:		Department:	
Email Address:			
Phone Number and, If Applicable, Extension:			

Section 2: Incident Update	
Current Status of Incident Response:	
Summary of Incident:	

Section 3: Investigators				
Name	**Title**	**Organization**	**Phone**	**Email**

Section 4: Log of Actions Taken			
Date	**Incident Handler/ Investigator**	**Action**	**Results**

Section 5: Evidence Found		
Date	**Incident Handler/ Investigator**	**Evidence**

Section 6: Parties Involved in Incident				
Name	**Title**	**Organization**	**Phone**	**Email**

Section 7: Incident Handler and Investigator Comments		
Date	**Incident Handler/ Investigator**	**Comments**

Section 8: Findings		
Type of Incident:	☐ Unauthorized Access	☐ Inappropriate Usage
☐ Malicious Code	☐ Denial of Service	☐ Multiple Component
Cause of Incident:		
Cost of Incident:		
Business Impact of Incident:		

PHI Compromised? ☐ Yes ☐ No

If yes, Estimated Number of Compromised PHI Accounts: _____ - or -

(If known) Actual Number of Compromised PHI Accounts: _____.

PHI Breach Impact: ☐ High (≥ 500 PHI Accounts) ☐ Medium (< 500 PHI Accounts) ☐ Unknown

Data Encrypted? ☐ Yes ☐ No If yes, description of encryption:_____.

Important Note: If PHI accounts may have been compromised and data was not encrypted, please follow breach evaluation procedures and, if necessary, breach notification procedures.

Was the breach evaluation processes initiated? ☐ Yes ☐ No

If yes, date of breach evaluation initiation: _____.

Section 9: Recommended Corrective Actions		
Recommended By	**Date**	**Recommended Corrective Action**

Section 10: Actions Taken		
Performed By	**Date**	**Action Taken**

Section 11: Notifications Made			
Organization	**Point of Contact**	**Date of Notification**	**Summary of Information Provided**

I attest that the information contained in this Investigation Report is true and accurate to the best of my knowledge and the knowledge of all contributors. I further attest that all parties who participated in the investigation, all findings of the investigation, and all recommended corrective actions as well as all actions taken by any parties to this investigation are clearly documented. This Investigation Report has been provided to the HIPAA Committee for review in both its final form and, as appropriate, throughout the term of the investigation. Effective on the date indicated below, this incident investigation is considered closed.

_____ _____

Incident Handler's Signature Date

SECURITY INCIDENT INVESTIGATION REPORT INSTRUCTIONS

- **Date Report Received** is the date that the Security Officer or Risk Manager first viewed the Incident Report.
- **Date Report Processing Began** is the date that the assigned Incident Handler began reviewing and investigating the Incident Report.
- **Report Number** should be assigned by the Security Officer. This Report Number should be noted on both the Security Incident Investigation Report and the Security Incident Report. If more than one Security Incident Report was filed for the same security incident/event, all of the applicable Report Numbers should be listed on the Security Incident Investigation Report.
- **Current Status of Incident** may be an ongoing attack, one time occurrence, resolved issue, etc.
- **Summary of Incident** is the summary of all information known about the security incident/event at the beginning of the investigation process.
- **Parties Involved in Incident** should include all persons who were interviewed and all persons who were found to be involved in the incident/event.
- **Cause of Incident** may include misconfigured application, unpatched host, compromised user account, inappropriate user permissions, etc.
- **Cost of Incident** should include both the cost of the investigation including the time spent investigating and the cost of any actions necessary to mitigate the security breach including initial and ongoing costs.
- **Business Impact of Incident** could either be a description of the incident's effect (i.e. the accounting department was unable to perform tasks for two days) or an impact category based on the cost (i.e. a "major" incident has a cost of over $100,000) as defined in the practice's Security Incident Policy.
- **PHI Breach Impact** is based on either the estimated number of compromised PHI records or, if known, the actual number of compromised PHI records.
- **Description of Encryption** should include the encryption type (i.e. DES, 3DES, AES, etc.); the encryption level (i.e. 128-bit, 192-bit, 256-bit); compliance with the FIPS 140-2 standard; whether data was encrypted at rest, in transit, or both; and any other pertinent information.
- **Recommended Corrective Actions** includes ALL recommended corrective actions even if they were not acted upon. This will create a clear record of all corrective actions considered.
- **Actions Taken** should include, of course, only the recommended corrective actions that were acted upon.
- **Notifications Made** may include the CEO, the Board of Directors/Trustees, legal counsel, law enforcement, and employees. However, any breach notification as required in HIPAA regulations, including the American Recovery and Reinvestment Act's (ARRA) Health Information Technology for Economic and Clinical Health (HITECH) Act, should be documented within the breach evaluation and notification procedure.

This Report is based on the guidelines found in Appendix 3 of NIST SP 800-61 Rev. 1: *Computer Security Incident Handling Guide*. A list of all NIST 800 publications can be found at http://csrc.nist.gov/publications/PubsSPs.html.

Security Incident Report Log
Sparks Family Medicine Location

Maintained by: _____, Security Officer

Report Number	Date of Incident Report	Incident Reporter	Reported To	Incident Handler	Brief Report Description	Date Report Was Closed