AppwoRx IT Policy And Procedures

Version 1.5 ● Updated 22 October 2015

Contents

Introduction

Purpose

This document defines the technical controls and security configurations users, Information Technology (IT) administrators and product developers are required to implement in order to ensure the integrity and availability of the data environment at Appworx, hereinafter, referred to as the Company. It serves as a central policy document with which all employees and contractors must be familiar, and defines actions and prohibitions that all users must follow. The policy provides IT managers within the Company with policies and guidelines concerning the acceptable use of Company 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 Company employees or temporary workers at all locations and by contractors working with the Company as subcontractors.

Scope

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

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 Companys 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 –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes

FAT – 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 – 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 - 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 Company 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 – 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 – Virtual Private Network – Provides a secure passage through the public Internet.

WAN – 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.

Privacy Officer

The Company 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 Company privacy policies in accordance with applicable federal and state laws. The current Privacy Officer for the Company is:
Christopher Cabell – Tel: 561.237.5500

Confidentiality/Security Team (CST)

The Company has established a Confidentiality / Security Team made up of key personnel whose responsibility it is to identify areas of concern within the Company 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 Company 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:

CEO – Christopher Cabell
CTO – George Cain
CMO – Dr. Ariel Soffer

The CST will meet quarterly to discuss security issues and to review 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 Company and act as the first line of defense in enhancing the security posture of the Company.

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 Company. This log will also be reviewed during the quarterly meetings.

Employee Responsibilities

Employee Requirements

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

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. Company policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15)11 minutes of inactivity. Employees are not allowed to take any action which would override this setting.

Home Use of Company Corporate Assets - Only computer hardware and software owned by and installed by the Company is permitted to be connected to or installed on Company equipment. Only software that has been approved for corporate use by the Company may be installed on Company equipment. Personal computers supplied by the Company are to be used solely for business purposes. All employees 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 Company for home use.

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

Prohibited Activities

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

- 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.
- 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.
- 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 Company 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.
- 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 Company 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.

- Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Company computers must be approved by the Company.
- Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the Company is strictly prohibited.
- System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Company is strictly prohibited.

Electronic Communication, E-mail, Internet Usage

As a productivity enhancement tool, The Company encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Company owned equipment are considered the property of the Company – not the property of individual users. Consequently, this policy applies to all Company employees 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.

1. Company 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:
2. it does not consume more than a trivial amount of employee time or resources,
3. it does not interfere with staff productivity,
4. it does not preempt any business activity,
5. 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 Company 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 Company information resources for personal or commercial profit is strictly prohibited.
   d) Political Activities – All political activities are strictly prohibited on Company premises. The Company encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Company assets or resources.
   e) Harassment – The Company strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Company 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 Company to monitor the content of any electronic communication, the Company is responsible for servicing and protecting the Company'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 Company reserves the right, at its discretion, to review any employee'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 Company policies.

Employees 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.

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.

Internet Access and Usage

Internet access is provided for Company 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 Company 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 an employee 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 Company routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

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

The following security and administration issues shall govern Internet usage.

Prior approval of the Company Privacy Officer or appropriate personnel authorized by the Company shall be obtained before:

- An Internet, or other external network connection, is established;
- Company information (including notices, memoranda, documentation and software) is made available on any Internet-accessible computer (e.g. web or ftp server) or device;
- 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;
- Use shall be consistent with the goals of the Company. The network can be used to market services related to the Company, however use of the network for personal profit or gain is prohibited.
- 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.
- The encryption software used, and the specific encryption keys (e.g. passwords, pass phrases), shall be escrowed with the Company 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.

Software Malfunctions

Users should inform the appropriate Company 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 Company computer virus policy should be followed, and these steps should be taken immediately:

- Stop using the computer
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- If possible, physically disconnect the computer from networks to which it is attached.
- Inform the appropriate personnel or Company 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.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- 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.

Anti-virus Software

Antivirus software is installed on all Company personal computers and servers. Virus update patterns are updated daily on the Company 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 Company is McAfee VirusScan Enterprise18. Updates are received directly from McAfee19 which is scheduled daily at 5:00 PM20.

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 Company 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.

New Software

Only software created by Company 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 Company computers and networks. These precautions include determining that the software does not, because of faulty design, “misbehave” and interfere with or damage Company 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 Company computer or network from another location must be scanned for viruses immediately after being received. Contact the appropriate Company 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 Company 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".

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

Security Incidents

It is the responsibility of each Company employee 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 Company 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 Company 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 Company 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.

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 Company and hold all data in the strictest confidence. Any purposeful release of data to which an employee may have access is a violation of Company policy and will result in personnel action, and may result in legal action.
Personal software shall not be used on Company computers or networks. If a need for specific software exists, submit a request to your supervisor or department head. Users shall not use Company purchased software on home or on non-Company computers or equipment.

Company 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 Company without written consent of the respective supervisor or department head. It is crucial to the Company 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 Company data to a non-Company 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 Company 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 Company does not control non-Company personal computers, the Company cannot be sure of the methods that may or may not be in place to protect Company sensitive information, hence the need for this restriction.

Transfer of Encrypted Data

WinZip encryption and zipping software allows Company 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 Company staff member who desires to utilize this technology may request this software from the Privacy Officer or appropriate personnel.

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:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers

- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- 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.

Disposal of Paper and/or 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.

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

- Do not throw any media containing sensitive, protected information in the trash.
- Return all external media to your supervisor
- 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.
- The final step in this process is to forward the media for disposal by a certified destruction agency.

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 Company in the proper use of transportable media when a legitimate business requirement exists to transfer data to and from Company networks. Every workstation or server that has been used by either Company 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 Company 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 Company 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 common Company within the Company. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Company networks. Transportable media received from an external source could potentially pose a threat to Company networks. Sensitive data includes all human resource data, financial data, Company 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 Company 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 Company. Non-Company workstations and laptops may not have the same security protection standards required by the Company, and accordingly virus patterns could potentially be transferred from the non-Company device to the media and then back to the Company 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 Company workstations/networks and workstations used within the Company. 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 Company workstations or servers as long as the source of the media in on the Company 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 Company, 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 Company 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 Company 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.

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:

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

Equipment Disposal

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.

As the older Company computers and equipment are replaced with new systems, the older machines are held in inventory for a wide assortment of uses:

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

Identification and Authentication

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:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.
- All user login IDs are audited at least twice yearly13 and all inactive logon IDs are revoked. The Company Human Resources Department notifies the Security Officer or appropriate personnel upon the departure of all employees 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 Company 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.

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 Company equipment and property is returned to the Company prior to the employee leaving the Company 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 Company 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 Company, 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).

Passwords

User IDs and passwords are required in order to gain access to all Company 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 six 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 every 120 days. Compromised passwords shall be changed immediately.

Reuse - The previous twelve17 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.

Confidentiality Agreement

Users of Company information resources shall sign, as a condition for employment, an appropriate confidentiality agreement (Appendix D). 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 Company 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 Company 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.

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 form can only be initiated by the appropriate department head, and must be signed by the department head and the Security Officer or appropriate personnel.

This guideline satisfies the "need to know" requirement of the HIPAA regulation, since the supervisor or department head is the person who most closely recognizes an employee's need to access data. 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.

Online banner screens, if used, shall contain statements to the effect that unauthorized use of the system is prohibited and that violators will be subject to criminal prosecution.

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.

If an employee changes positions at the Company, 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.

Violations

It is the policy of the Company that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Company will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.
The Company will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Company'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).

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 (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.

In the event that a workforce member violates the Company'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 Company'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 Company'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 Company 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.

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 Company.

Acknowledgement of the violation and action taken must be presented and signed by employee or contractor.

Background Checks

The Company will conduct employment reference checks, investigative consumer reports, and 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 Company 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 (Appendix G). 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 Company in background checks may include, but is not limited to, some or all of the following:

- Private and government agency reports related to any history of criminal, dishonest, or violent behavior, and other reports that relate to suitability for employment
- Education (including degrees awarded and GPA)
- Employment history, abilities, and reasons for termination of employment
- Professional licensing board reports
- Address history
- Credit reports
- Social security number scans
- Civil court filings
- Motor vehicle and driving records
- 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 Company 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 Company will follow FCRA requirements, other applicable statutes, and Company procedures for providing information and reports, making decisions, and responding to applicants and employees regarding potentially adverse actions to an investigative report.

The Company 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 Company's document retention procedures.

Adapted from Carole Edman of HR Manager To Go Consultants (http://www.amof.info/sample-policy.htm).

Connectivity

Network Connections

The security of Company systems can be jeopardized from third party locations if security Company 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 Company systems. The Privacy Officer or appropriate personnel should be involved in the process, design and approval.

Third Party Contracts

Access to Company 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.

- Applicable sections of the Company Information Security Policy have been reviewed and considered.
- Policies and standards established in the Company information security program have been enforced.
- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- The right to audit contractual responsibilities should be included in the agreement or SOW.
- 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.
- A description of each service to be made available.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- A detailed list of users that have access to Company computer systems must be maintained and auditable.
- If required under the contract, permission should be sought to screen authorized users.
- ¬Dates and times when the service is to be available should be agreed upon in advance.
- 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.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Responsibilities regarding hardware and software installation and maintenance should be understood and agreement upon in advance.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.
- 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.
- Mechanisms should be in place to ensure that security measures are being followed by all parties to the agreement.
- 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.

- 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.

Firewalls

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

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.

Secure Socket Layer (SSL) Web Interface

Any hosted (ASP) system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Network Access Request Form (found in Appendix A) and have appropriate approval from the supervisor or department head as well as the Privacy Officer or appropriate personnel before any access is granted.

Building Security

It is the policy of the Company 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 Company 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 Company. All other facilities, if applicable, have similar security appropriate for that location.

Description of building, location, square footage, and the use of any generator.

- Entrance to the building during non-working hours is controlled by a security code system. Attempted entrance without this code results in immediate notification to the police department.
- Only specific Company employees are given the security code for entrance. Disclosure of the security code to non-employees is strictly prohibited.
- The security code is changed on a periodic basis and eligible employees are notified by company e-mail or voice mail. Security codes are changed upon termination of employees that had access.
- 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).
- The reception area is staffed at all times during the working hours of 8:00 AM to 5:00 PM.
- 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 Company staff member. In some situations, non-Company personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times.
- Swipe cards control access to all other doors. Each card is coded to allow admission to specific areas based on each individual's job function or need to know.
- The first floor of the building has motion detection sensors that are activated after hours. Any movement within the building will result in immediate notification to the police department.
- All outside windows have glass breakage sensors which, if tripped, will result in immediate notification to the police department.
- The building is equipped with security cameras to record activities in the parking lot and within the area encompassing the front entrance. All activities in these areas are recorded on a 24 hour a day 365 day per year basis.
- Fire Protection: Use of local building codes will be observed. Manufacturer's recommendations on the fire protection of individual hardware will be followed.

Distributed Operations

With the increased availability of broadband access and VPNs, telecommuting has become more viable for many organizations. The Company 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 Company 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 Company 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 Company'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.

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.

- Need to Know: Telecommuting Users will have the access based on the same 'need to know' as they have when in the office.
- Password Use: The use of a strong password, changed at least every 90 days27, 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.
- Training: Personnel who telecommute must complete the same annual privacy training as all other employees.
- Contract Specific: There may be additional requirements specific to the individual contracts to which an employee is assigned.

Hardware Security

Virus Protection: distributed users must never stop the update process for Virus Protection. Virus Protection software is installed on all Company 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 Company information of any type. The Company 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.

Data Security

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 Company personnel for assistance. Protect external media by keeping it in your possession when traveling.

Transferring Data to the Company: Transferring of data to the Company 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 Company.

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-Company Networks: Extreme care must be taken when connecting Company equipment to a home or hotel network. Although the Company actively monitors its security status and maintains organization wide protection policies to protect the data within all contracts, the Company has no ability to monitor or control the security procedures on non-Company 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 Company: 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 Company without the written approval of your supervisor.

Audit Controls

To ensure that Company 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.

User Audits

The Company is committed to routinely auditing users' activities in order to continually assess potential risks and vulnerabilities to ePHI in its possession. As such, the Company 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.

Event Audits

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.

Intrusion Audits

The Company 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.

Audit Reviews

The Information Technology Services shall be responsible for conducting reviews of Company'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.

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. Such reviews shall be

conducted annually. Audits also shall be conducted if Company 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.

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 Company'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).

Data Audit

To the fullest extent possible, Company shall utilize applications with built-in intelligence that automatically checks for human errors.

To prevent transmission errors as data passes from one computer to another, Company will use encryption, as determined to be appropriate, to preserve the integrity of data.

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

- Company will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.
- 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.

SSAE 16 Audit

Company will retain a certified public accounting firm (i) to perform an SSAE 16 audit or equivalent that includes Provider's Project Data management systems and (ii) to produce the corresponding Type II Report from that audit.

Mitigation Plan

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.

Company is committed to maintaining formal Company for responding to an emergency or other occurrence that damages systems containing ePHI. Company 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.

Data Backup Plan

Company, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies of ePHI.

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 Company'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.

The Security Officer shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

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.

Disaster Recovery and Emergency Mode Operations Plan

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.

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 Company'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 Company'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 Company'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.

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 Company;

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.

Breach

The following process is 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.

Possible Breach

1. Any employee who becomes aware of a possible breach of privacy involving Private Information in the custody or control of the Company 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 Company'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 Company
        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 Companies
        vi. Notifying the appropriate authorities including the local Police Department if the breach involves, or may involve, any criminal activity

Risks Associated with the Breach

1. To determine what other steps are immediately necessary, the Privacy Officer in collaboration with the Company'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 Company'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 Company'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

Breach Notification

1. The Privacy Officer will work with the department(s) involved, the Company'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 Company'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 Company 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

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 Company in investigating and mitigating the breach.

Notice to Health and Human Services (HHS) as required by HIPAA – If the Company'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 Company 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.

Training Plan

To establish a security awareness and training program for all members of Company's workforce, including management.

All workforce members shall receive appropriate training concerning Company'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.

Security Training

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.

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.

Security Reminders

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.

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.

Malicious Software Training

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.
h. Password Management

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.

Risk Plan

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

Company shall conduct an accurate and thorough risk analysis to serve as the basis for Company's HIPAA Security Rule compliance efforts. Company 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 Companys and technological advancements.

The Security Officer shall be responsible for coordinating Company's risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.

The risk analysis shall proceed in the following manner:

1. Document Company'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.

2. For each application identified, identify each licensee (*i.e.,* authorized user) by job title and describe the manner in which authorization is granted.
   a. 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.

b. Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of ePHI created, received, maintained, or transmitted by Company. Consider the following:
   i. Natural threats, e.g., earthquakes, storm damage.
   ii. Environmental threats, e.g., fire and smoke damage, power outage, utility problems.
c. Human threats
   i. 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
   ii. Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment
   iii. Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail
   iv. External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction
d. Identify and document vulnerabilities in Company'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.
e. Determine and document probability and criticality of identified risks.
f. 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.

3. Assign criticality level.
   a. "High" (3) is defined as having a catastrophic impact on the medical Company 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 Company 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.

4. 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.
   a. 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.
   b. Develop and document an implementation strategy for critical security measures and safeguards.
   c. Determine timeline for implementation.
   d. Determine costs of such measures and safeguards and secure funding.
   e. Assign responsibility for implementing specific measures and safeguards to appropriate person(s).
   f. Make necessary adjustments based on implementation experiences.

g. Document actual completion dates.
    1. Evaluate effectiveness of measures and safeguards following implementation and make appropriate adjustments.

5. 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:
    a. 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.
    b. Analysis to assess adequacy of controls within the network, operating systems and applications. As appropriate, Company shall engage outside vendors to evaluate existing physical and technical security measures and make recommendations for improvement

Emergency Operations

Notification

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

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

"Break the Glass" Access

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

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

The Company has a formal, documented emergency access procedure enabling Company 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 Company management or designated personnel.

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

All appropriate Company 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.

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 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, or designated person, records information about emergency users and the emergency access rights assigned to them.

5. The system administrator and Security Officer 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.>
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.

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).
2. Securing the password.
3. Periodically changing the password.