INFORMATION SECURITY POLICY

COMPANY NAME AND/OR LOGO1



Last Revision Date

Date2

Document Owner

Name3

Table of Contents

[Introduction 4](#_Toc270681525)

[Purpose 4](#_Toc270681526)

[Scope 4](#_Toc270681527)

[Acronyms / Definitions 5](#_Toc270681528)

[Applicable Statutes / Regulations 6](#_Toc270681529)

[Privacy Officer 6](#_Toc270681530)

[Confidentiality / Security Team (CST) 6](#_Toc270681531)

[Employee Responsibilities 8](#_Toc270681532)

[Employee Requirements 8](#_Toc270681533)

[Prohibited Activities 9](#_Toc270681534)

[Electronic Communication, E-mail, Internet Usage 10](#_Toc270681535)

[Reporting Software Malfunctions 12](#_Toc270681536)

[Report Security Incidents 12](#_Toc270681537)

[Identification and Authentication 16](#_Toc270681538)

[User Logon IDs 16](#_Toc270681539)

[Passwords 16](#_Toc270681540)

[Confidentiality Agreement 17](#_Toc270681541)

[Access Control 17](#_Toc270681542)

[Network Connectivity 19](#_Toc270681543)

[Dial-In Connections 19](#_Toc270681544)

[Dial Out Connections 19](#_Toc270681545)

[Telecommunication Equipment 19](#_Toc270681546)

[Permanent Connections 20](#_Toc270681547)

[Emphasis on Security in Third Party Contracts 20](#_Toc270681548)

[Firewalls 21](#_Toc270681549)

[Malicious Code: 22](#_Toc270681550)

[Antivirus Software Installation 22](#_Toc270681551)

[New Software Distribution 22](#_Toc270681552)

[Retention of Ownership 23](#_Toc270681553)

[Encryption 24](#_Toc270681554)

[Definition 24](#_Toc270681555)

[Encryption Key 24](#_Toc270681556)

[Installation of authentication and encryption certificates on the e-mail system 24](#_Toc270681557)

[Use of WinZip encrypted and zipped e-mail 24](#_Toc270681558)

[File Transfer Protocol (FTP) 24](#_Toc270681559)

[Secure Socket Layer (SSL) Web Interface 25](#_Toc270681560)

[Building Security 26](#_Toc270681561)

[Telecommuting 28](#_Toc270681562)

[General Requirements 28](#_Toc270681563)

[Required Equipment 28](#_Toc270681564)

[Hardware Security Protections 29](#_Toc270681565)

[Data Security Protection 29](#_Toc270681566)

[Disposal of Paper and/or External Media 30](#_Toc270681567)

[Specific Protocols and Devices 31](#_Toc270681568)

[Wireless Usage Standards and Policy 31](#_Toc270681569)

[Use of Transportable Media 32](#_Toc270681570)

[Retention / Destruction of Medical Information 34](#_Toc270681571)

[Disposal of External Media / Hardware 35](#_Toc270681572)

[Disposal of External Media 35](#_Toc270681573)

[Requirements Regarding Equipment 35](#_Toc270681574)

[Disposition of Excess Equipment 35](#_Toc270681575)

[Appendix A – Network Access Request Form 37](#_Toc270681576)

[Appendix B – Confidentiality Form 39](#_Toc270681579)

[Appendix C – Approved Software 40](#_Toc270681580)

[Appendix D – Approved Vendors 41](#_Toc270681581)

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: INTRODUCTION** | **P&P #:**  IS-1.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Introduction

## Purpose

This policy defines the technical controls and security configurations users and Information Technology (IT) administrators are required to implement in order to ensure the integrity and availability of the data environment at Company Name6, hereinafter, referred to as the **Practice**. 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 Practice with policies and guidelines concerning the acceptable use of Practice technology equipment, e-mail, Internet connections, voice-mail, facsimile, future technology resources and information processing.

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

## Scope

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

## Acronyms / Definitions

Common terms and acronyms that may be used throughout this document.

**CEO –** The Chief Executive Officer is responsible for the overall privacy and security practices of the company.

**CIO** – The Chief Information Officer

**CMO –** The Chief Medical Officer.

**CO –** The Confidentiality Officer is responsible for annual security training of all staff on confidentiality issues.

**CPO –** The Chief Privacy Officer is responsible for HIPAA privacy compliance issues.

**CST** – Confidentiality and Security Team

**DoD –** Department of Defense

**Encryption** – The process of transforming information, using an algorithm, to make it unreadable to anyone other than those who have a specific ‘need to know.’

**External Media –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 Practice management.

**Users with edit/update capabilities –** individuals who are permitted, based on job assignment, to add, delete, or change records in a database**.**

**Users with inquiry (read only) capabilities –** individuals who are prevented, based on job assignment, from adding, deleting, or changing records in a database. Their system access is limited to reading information only.

**VLAN –** 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.

## Applicable Statutes / Regulations

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

List any agencies/organization7

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

## Privacy Officer

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

Name – Telephone Number8

## Confidentiality / Security Team (CST)

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

All members identified within this policy are assigned to their positions by the CEO. The term of each member assigned is at the discretion of the CEO, but generally it is expected that the term will be one year. Members for each year will be assigned at the first meeting of the Quality Council in a new calendar year. This committee will consist of the positions within the Practice most responsible for the overall security policy planning of the organization- the CEO, PO, CMO, ISO, and the CIO (where applicable). The current members of the CST are:

Title – Name9

Title – Name

Title – Name

Title – Name

Title – Name

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 Practice and act as the first line of defense in enhancing the security posture of the Practice.

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

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

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: EMPLOYEE RESPONSIBILITIES** | **P&P #:**  IS-2.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Employee Responsibilities

## Employee Requirements

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

Wear Identifying Badge so that it may be easily viewed by others **-**

In order to help maintain building security, all employees should prominently display their employee identification badge. Contractors who may be in Practice facilities are provided with different colored identification badges10. Other people who may be within Practice facilities should be wearing visitor badges and should be chaperoned.

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

Secure Laptop with a Cable Lock **-** When out of the office all laptop computers must be secured with the use of a cable lock. Cable locks are provided with all new laptops computers during the original set up. All users will be instructed on their use and a simple user document, reviewed during employee orientation, is included on all laptop computers.

Most Practice computers will contain sensitive data either of a medical, personnel, or financial nature, and the utmost care should be taken to ensure that this data is not compromised. Laptop computers are unfortunately easy to steal, particularly during the stressful period while traveling. The cable locks are not fool proof, but do provide an additional level of security. Many laptop computers are stolen in snatch and run robberies, where the thief runs through an office or hotel room and grabs all of the equipment he/she can quickly remove. The use of a cable lock helps to thwart this type of event.

Unattended Computers **-** Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Practice policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15)11 minutes of inactivity. Employees are not allowed to take any action which would override this setting.

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

Retention of Ownership - All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Practice are the property of the Practice unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Practice 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 Practice Privacy Officer, may test the resiliency of a system. Such personnel may test for susceptibility to hardware or software failure, security against hacker attacks, and system infection.

* Browsing. The willful, unauthorized access or inspection of confidential or sensitive information to which you have not been approved on a "need to know" basis is prohibited. The Practice has access to patient level health information which is protected by HIPAA regulations which stipulate a "need to know" before approval is granted to view the information. The purposeful attempt to look at or access information to which you have not been granted access by the appropriate approval procedure is strictly prohibited.
* Personal or Unauthorized Software. Use of personal software is prohibited. All software installed on Practice computers must be approved by the Practice.
* Software Use. Violating or attempting to violate the terms of use or license agreement of any software product used by the Practice is strictly prohibited.
* System Use. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Practice is strictly prohibited.

## Electronic Communication, E-mail, Internet Usage12

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

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

1. it does not consume more than a trivial amount of employee time or resources,
2. it does not interfere with staff productivity,
3. it does not preempt any business activity,
4. it does not violate any of the following:
   1. 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.
   2. Illegal activities – Use of Practice information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
   3. Commercial use – Use of Practice information resources for personal or commercial profit is strictly prohibited.
   4. Political Activities – All political activities are strictly prohibited on Practice premises. The Practice encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Practice assets or resources.
   5. Harassment – The Practice strives to maintain a workplace free of harassment and that is sensitive to the diversity of its employees. Therefore, the Practice prohibits the use of computers, e-mail, voice mail, instant messaging, texting and the Internet in ways that are disruptive, offensive to others, or harmful to morale. For example, the display or transmission of sexually explicit images, messages, and cartoons is strictly prohibited. Other examples of misuse includes, but is not limited to, ethnic slurs, racial comments, off-color jokes, or anything that may be construed as harassing, discriminatory, derogatory, defamatory, threatening or showing disrespect for others.
   6. Junk E-mail - All communications using IT resources shall be purposeful and appropriate. Distributing “junk” mail, such as chain letters, advertisements, or unauthorized solicitations is prohibited. A chain letter is defined as a letter sent to several persons with a request that each send copies of the letter to an equal number of persons. Advertisements offer services from someone else to you. Solicitations are when someone asks you for something. If you receive any of the above, delete the e-mail message immediately. Do not forward the e-mail message to anyone.

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

The Practice reserves the right, at its discretion, to review any 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 Practice 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.

**Internet Access**

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

Users must understand that individual Internet usage is monitored, and if 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 Practice routers and firewalls. This list is constantly monitored and updated as necessary. Any employee visiting pornographic sites will be disciplined and may be terminated.

## Reporting Software Malfunctions

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

* 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 Practice ISO as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
* 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.

## Report Security Incidents

It is the responsibility of each Practice 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 Practice CST. Members of the CST are specified above in this document.

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

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

**Transfer of Sensitive/Confidential Information**

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

**Transferring Software and Files between Home and Work**

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

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

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

**Internet Considerations**

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

The following security and administration issues shall govern Internet usage.

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

* An Internet, or other external network connection, is established;
* Practice 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 Practice. The network can be used to market services related to the Practice, however use of the network for personal profit or gain is prohibited.
* 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 Practice Privacy Officer or appropriate personnel, to ensure they are safely maintained/stored. The use of encryption software and keys, which have not been escrowed as prescribed above, is prohibited, and may make the user subject to disciplinary action.

**Installation of authentication and encryption certificates on the e-mail system**

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

**Use of WinZip encrypted and zipped e-mail**

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

**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.

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: IDENTIFICATION and AUTHENTICATION** | **P&P #:**  IS-3.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# 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 / using information resources. Security requirements for user identification include:

* Each user shall be assigned a unique identifier.
* Users shall be responsible for the use/misuse of their individual logon id.

All user login ids are audited at least twice yearly13 and all inactive logon ids are revoked. The Practice HR department notifies the ISO upon the departure of all employees and contractors, at which time login ids are revoked.

The logon id is locked/revoked after a maximum of three (3)14 unsuccessful logon attempts which then require the passwords to be reset by the appropriate Administrator.

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

## Passwords

**User Account Passwords**

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

Password Length – Passwords are required to be a minimum of eight characters15.

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 90 days16. Compromised passwords shall be changed immediately.

Reuse - The previous twelve17 passwords cannot be reused.

Restrictions on Sharing Passwords - Passwords shall not be shared, or 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 Practice information resources shall sign, as a condition for employment, an appropriate confidentiality agreement (Appendix B). The agreement shall include the following statement, or a paraphrase of it:

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

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

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

## Access Control

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

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 Form. This form can only be initiated by the appropriate department head, and must be signed by the department head, and by the Privacy 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 Privacy 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.

**Identification and Authentication Requirements**

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

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: NETWORK CONNECTIVITY** | **P&P #:**  IS-4.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Network Connectivity

## Dial-In Connections

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

Dial-up numbers shall be unlisted.

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

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

## Dial Out Connections

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

## Telecommunication Equipment

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

* + - phone lines
    - fax lines
    - calling cards
    - phone head sets
    - software type phones installed on workstations
    - conference calling contracts
    - cell phones
    - Blackberry type devices
    - call routing software
    - call reporting software
    - phone system administration equipment
    - T1/Network lines
    - long distance lines
    - 800 lines
    - local phone lines
    - PRI circuits
    - telephone equipment

## Permanent Connections

The security of Practice systems can be jeopardized from third party locations if security practices and resources are inadequate. When there is a need to connect to a third party location, a risk analysis should be conducted. The risk analysis should consider the type of access required, the value of the information, the security measures employed by the third party, and the implications for the security of Practice systems. The Privacy Officer or appropriate personnel should be involved in the process, design and approval.

## Emphasis on Security in Third Party Contracts

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

* Applicable sections of the Practice Information Security Policy have been reviewed and considered.
* Policies and standards established in the Practice 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 Practice 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 Practice router or firewall.

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: MALICIOUS CODE** | **P&P #:**  IS-5.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Malicious Code:

## Antivirus Software Installation

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

Configuration **-** The antivirus software currently implemented by the Practice is McAfee VirusScan 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 Practice network may be maintained. Appropriate administrative staff is responsible for providing reports for auditing and emergency situations as requested by the Privacy Officer or appropriate personnel.

## New Software Distribution

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

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

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

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

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

## Retention of Ownership

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

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: ENCRYPTION** | **P&P #:**  IS-6.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Encryption

## Definition

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

## Encryption Key

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

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

## Installation of authentication and encryption certificates on the e-mail system

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

## Use of WinZip encrypted and zipped e-mail

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

## 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 EHR 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.

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: BUILDING SECURITY** | **P&P #:**  IS-7.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Building Security

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

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 system21. Attempted entrance without this code results in immediate notification to the police department.
* Only specific Practice 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 PM22.
* Any unrecognized person in a restricted office location should be challenged as to their right to be there. All visitors must sign in at the front desk, wear a visitor badge(excluding patients), and be accompanied by a Practice staff member. In some situations, non-Practice personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times
* 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 know23.
* 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 department24.
* All outside windows have glass breakage sensors which, if tripped, will result in immediate notification to the police department25.
* 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 basis26.
* Fire Protection: Use of local building codes will be observed. Manufacturer’s recommendations on the fire protection of individual hardware will be followed.

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: TELECOMMUTING** | **P&P #:**  IS-8.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Telecommuting

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

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

## 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.

## Required Equipment

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

**Practice Provided:**

Practice supplied workstation28.

A cable lock to secure the workstation to a fixed object.

If using VPN, a Practice issued hardware firewall is required.

If printing, a Practice supplied printer.

If approved by your supervisor, a Practice supplied phone.

**Employee Provided:**

Broadband connection and fees,

Paper shredder,

Secure office environment isolated from visitors and family,

A lockable file cabinet or safe to secure documents when away from

the home office.

## Hardware Security Protections

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

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

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

Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected by HIPAA or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 1529 minutes of inactivity.

## Data Security Protection

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

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

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

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

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

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

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

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

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

## Disposal of Paper and/or External Media

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

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

* + - 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.

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: SPECIFIC PROTOCOLS AND DEVICES** | **P&P #:**  IS-9.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Specific Protocols and Devices

## Wireless Usage Standards and Policy

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

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

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

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

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

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

## Use of Transportable Media

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

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

The use of transportable media in various formats is common practice within the Practice. All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Practice networks. Transportable media received from an external source could potentially pose a threat to Practice networks. ***Sensitive data*** includes all human resource data, financial data, Practice proprietary information, and personal health information (“PHI”) protected by the Health Insurance Portability and Accountability Act (“HIPAA”).

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

Rules governing the use of transportable media include:

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

Example: Do not copy a work spreadsheet to your USB key and take it home to work on your home PC.

* Data may be exchanged between Practice workstations/networks and workstations used within the Practice. The very nature of data exchange requires that under certain situations data be exchanged in this manner.

Examples of necessary data exchange include:

Data provided to auditors via USB key during the course of the audit.

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

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

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

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: RETENTION / DESTRUCTION of PAPER DOCUMENTS** | **P&P #:**  IS-10.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Retention / Destruction of Medical Information

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

Record Retention - Documents relating to uses and disclosures, authorization forms, business partner contracts, notices of information practice, responses to a patient who wants to amend or correct their information, the patient's statement of disagreement, and a complaint record are maintained for a period of 6 years3o0.

Record Destruction - All hardcopy medical records that require destruction are shredded using NIST 800-88 guidelines.

|  |  |
| --- | --- |
| Company Name or Logo1  **Policy and Procedure** | |
| **Title: DISPOSAL OF EXTERNAL MEDIA / HARDWARE** | **P&P #:**  IS-11.0 |
| **Approval Date: Date**4 | **Review: Annual** |
| **Effective Date: Date**5 | **Information Technology** |

# Disposal of External Media / Hardware

## Disposal of External Media

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

The following steps must be adhered to:

* 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.

## Requirements Regarding Equipment

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

## Disposition of Excess Equipment

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

* 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.

**UPDATES to Document**

|  |  |  |  |
| --- | --- | --- | --- |
| **Date** | **User** | **Section** | **Content** |
| 8/20/2010 – 8/26/2010 | Nathan Gibson | All | All content modified for template creation purposes. |
| 9/13/2010 – 9/17/2010 | Nick Heesters | All | Tracked in track changes |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Appendix A – Network Access Request Form

Employee or Contractor Request for Network Access

|  |  |
| --- | --- |
| **EMPLOYEE/CONTRACTOR INFORMATION** | |
| New Employee  New Contractor  Existing User Today’s Date:  Temporary | |
| First Name:      Last Name:       \*MI: | |
| Position: | Department:  Supervisor: |
| Full-time  Part-time | Start date or Requested due date:  Temporary or Contractor end date, if known: |
| **SECURITY & EMAIL** | | |
| New Account:  Network Account  Email  Security/Email similar to what existing user:  Include in which E-mail Group(s):        Remove from which E-mail Group(s):  Include in which Security Group(s):        Remove from which Security Group(s):  Permit access to the following network location(s):  Drive       Path       Access:  Read-only  Read/write  Full Access  Remove Access  Drive       Path       Access:  Read-only  Read/write  Full Access  Remove Access  Drive       Path       Access:  Read-only  Read/write  Full Access  Remove Access  Miscellaneous Needs *(Enter any other requests)*: | | |
| **EHR ACCESS** | | |
| EHR Account  Roles & Access:  Front Office Access:  Read-only  Read/write  Full Access  Remove Access  Clinician Access:  Read-only  Read/write  Full Access  Remove Access  Physician Access:  Read-only  Read/write  Full Access  Remove Access  Accounting Access:  Read-only  Read/write  Full Access  Remove Access  Records Management Access:  Read-only  Read/write  Full Access  Remove Access  Reporting Access:  Read-only  Read/write  Full Access  Remove Access  Administrator Access:  Read-only  Read/write  Full Access  Remove Access  Other: Specify       Access:  Read-only  Read/write  Full Access  Remove Access  Miscellaneous Needs *(Enter any other requests)*: | | |
| **HARDWARE & SOFTWARE** | | |
| Hardware:  Laptop  Desktop  Either Laptop or Desktop  Screen protector  Laptop bag  Cable lock  Multifunction printer  Netgear Router  Numeric keypad  Standard inkjet printer  Dual monitors  Docking station  iPhone  iPad  Windows Mobile Device  Software:  Adobe Acrobat (full version)  Email Encryption  Microsoft Office Professional 2003  Microsoft Office Professional 2007  MS Project 2007  MS Visio 2007  MS OneNote 2007  Fax Server - *Specify level of access:*  Miscellaneous Needs *(Enter any other requests)*: | | |
| **TELEPHONY** | | |
| Telephone:  Desk Phone  Softphone (IP Communicator)  Desk phone currently exist at location. Current extension is:  Accessories:  Wireless headset  Wired headset | | |
| **CELL PHONE / AIR CARD** | | |
| Cell phone  Air Card  Accessories:  Cell Phone Case/Holder  Car Charger  Miscellaneous Needs *(Enter any other requests)*: | | |
| **BUILDING ACCESS** | | |
| Access Requested for the following location(s):  Medical Records Room  Server Room  Lobby  Other, *Specify:*    Additional Access Restriction:  After-Hours Access, *Specify Hours:*  Other Restrictions (be specific): | | |
| **SPECIAL INSTRUCTIONS** | | |
| Manager Checklist/Reminder:   * Signature below can be of the Department Head or the Data Owner if new network access is requested. * Ensure employee badge is requested * Schedule new employee orientation, if applicable * Ensure name appears on any appropriate sign-in/out sheets * Remember to have all new employees/contractors read and sign appropriate forms,  i.e. Confidentiality Form (Appendix B) * Request appropriate training/background:   + HR Background Investigation   + Security Training   + Any additional training and/or background check | | |

|  |  |  |
| --- | --- | --- |
| **NAME** | **SIGNATURE** | **DATE** |
| **Department Head (Print Name)** |  |  |
| **Privacy Officer /  Appropriate Authority** |  |  |

# Appendix B – Confidentiality Form

**RESPONSIBILITY OF CONFIDENTIALITY**

I understand and agree to maintain and safeguard the confidentiality of privileged information of Practice Name1. Further, I understand that any unauthorized use or disclosure of information residing on the Practice information resource system may result in disciplinary action consistent with the policies and procedures of federal, state, and local agencies.

Date Signature

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Company/Firm

Date Signature of Practice  
 Privacy Officer

# Appendix C – Approved Software

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Software | Version | Approved by | Date | Description/Comments |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

# Appendix D – Approved Vendors

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Vendor | Primary Contact | Main Number | Product / Service | Description/Comments |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |