IT and DATA Security Policies for Plus91 and MediXcel Platform

Authors: Aditya Patkar, Ajay Mandera

Version No: 0.6

Document Code: P91-91020-04-MCD-0103

Meta Code: Data Security Policies Document Revision 0.6

Tags: MediXcel, Plus91, MCD, HIS, HMIS, Hospital Software, Diagnostic Software, Clinic Software, EHR, EMR, PHR, Patient Portal, Security, Compliance, Meaningful Use

CONFIDENTIAL

Revision History

Revision	Date	Reason for Change	Author
0.1.0	09-07-2015	Initial Draft	Ajay Mandera
0.2.0	23-03-2016	Updated Draft with new Guidelines	Ajay Mandera

0.3.0	28-04-2017	Updated Draft after MOH India release	Aditya Patkar
0.4.0	31-07-2020	Updated Draft with new Guidelines	Ajay Mandera
0.5.0	12-06-2021	Updated Draft for some policies updates	Ajay Mandera
0.6.0	12-04-2022	Updated Draft for some policies updates	Ajay Mandera

NOTES:

1. Revision Rules:

- Decimal revisions (0.x, x.x) indicate work-in-progress 0.1, 0.2, 0.3, …x.2…x.9..
- Integer revisions (x.0) indicate an approved baseline document: 1.0, 2.0, 3.0, x.0.
- Alpha revisions (A, B, C etc.) can be used for non-I/A documents.

2. The File Properties REQUIRING update prior to check-in are:

Summary Properties
- Subject Document Title (Description with Type)
- Version No. Version No. Pertaining to this document
- Comments Document Revision Level (0.1, 0.2, 1.1, 1.2, etc)
-

Custom Properties
- Owner Project Manager (eName)
- Document Code Identification Code (Auth No – Country Code City Code – Division Code – Doc Type – Revision No)
- Meta Code Internal Filing Code
- Document No. Document number and revision level (e.g. 10022_1v0, 10088_0v2, etc)
- Tags Keywords to identify this document

3. Project teams can add Main section or sub sections and even Appendices if required. In no case should the main sections defined in the current template should be deleted. Do not delete inapplicable sections from this document. Instead, indicate it is not applicable or NA

Table of Contents

Definitions and Abbreviations

CEO	The Chief Executive Officer is responsible for the overall privacy and security practices of the company.
CIO	The Chief Information Officer
CO	The Confidentiality Officer is responsible for annual security training of all staff on confidentiality issues
CST	Confidentiality and Security Team
HIPAA	Health Insurance Portability and Accountability Act of 1996
EHR	Electronic health records
EMR	Electronic Medical Records
Client	Who purchase EHR/EMR software from Plus91
On Request	Client requests for additional features in EMR/HER are called On Request features.
LAN	Local Area Network
External Media	**i.e.** CD-ROMs, DVDs, floppy disks, flash drives, USB keys, thumb drives, tapes
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.
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.
Privileged Users	system administrators and others specifically identified and authorized by Practice management.

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.
WAN	Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.
Support Users	Employees who provide L1 and L2 support to EHR clients.
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.

About Plus91

Plus91 Technologies is a Healthcare Technology Company. We create and implement Electronic Medical Records, Laboratory and Hospital Information Management Systems, Disease Management Systems, Disease Surveillance Systems and Healthcare Analytics products. Our products are used a Clinics, Labs, Hospitals and Wellness Organizations. We sell directly to Private organizations as well as do state and nationwide rollouts for Ministries and NGO's.

We strategize and manage Digital Marketing Solutions for Healthcare Providers and Healthcare value chain stakeholders.

Plus91 has for over 10 years built Healthcare IT Products and Projects and supported Digital Marketing Services. Our core-team of technology consultants, developers, testers, project managers and designers have extensive experience in understanding Healthcare requirements and mapping them to technology paradigms.

Plus91 and its Leadership is considered influential in the Digital Health IT space and is seen as a leading innovator internationally. We have been active in India, Middle East, Africa and the United States. We love to collaborate with local stakeholders and improve healthcare delivery systems all over the world.

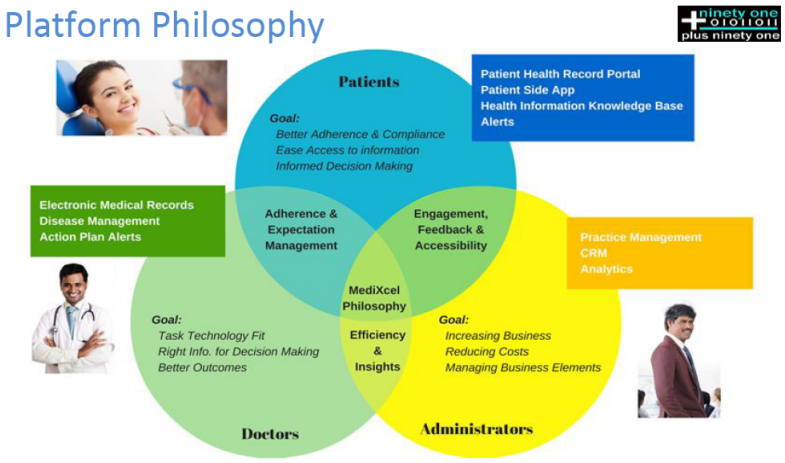

Figure 1: MediXcel - Platform Philosophy

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 Plus91, hereinafter, referred to as the **Practice**. It serves as a central policy document with which all employees and contractors must be familiar and certain policies may cover Client Sites and Client Employees who are using Applications setup within the Practice environment. It defines actions and prohibitions that all users affected by this policy 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, 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.

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:

CEO – Aditya Patkar

Director – Nrip Nihalani

Systems Manager – Ajay Mandera

QA & Support Manager– Altaf Tamboli

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.

Log Management:

Every important log of the system and services are monitored and daily alerts have been configured. Specific users of CST will receive daily log reports from the server. Special alerts have been set for the critical services, such as MySQL and HTTPD, for quick monitoring.

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.

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.

Unattended Computers - Unattended computers should be locked by the user when leaving the work area. This feature is discussed with all employees during yearly security training. Practice policy states that all computers will have the automatic screen lock function set to automatically activate upon fifteen (15) minutes of inactivity. 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 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 local laws or regulations of India or Client country 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 Usage

As a productivity enhancement tool, The Practice encourages the business use of electronic communications. However, all electronic communication systems and all messages generated on or handled by Practice owned equipment are considered the property of the Practice – not the property of individual users. Consequently, this policy applies to all Practice 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, email, 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:
    a) Copyright violations – This includes the act of pirating software, music, books and/or videos or the use of pirated software, music, books and/or videos and the illegal duplication and/or distribution of information and other intellectual property that is under copyright.
    b) Illegal activities – Use of Practice information resources for or in support of illegal purposes as defined by federal, state or local law is strictly prohibited.
    c) Commercial use – Use of Practice information resources for personal or commercial profit is strictly prohibited.
    d) Political Activities – All political activities are strictly prohibited on Practice premises. The Practice encourages all of its employees to vote and to participate in the election process, but these activities must not be performed using Practice assets or resources.

e) Harassment – The Practice strives to maintain a workplace free of harassment and that is sensitive to the diversity of its 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.

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

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

The Practice reserves the right, at its discretion, to review any 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 or to visit social media websites. 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 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 CBI or any local law enforcement agencies at client locations.

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. For data like, but not limited to, ePHI, Medical data, any related data, users must follow the Data Management policy.

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/department head or to the System administrator. Users shall not use Practice purchased software on home or on non-Practice computers or equipment, special permission required to do this from Practice.

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/department head or Privacy officer. 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.

Identification and Authentication

User Logon

Individual users shall have a unique logon through their fingerprint. An access control system shall identify each user and prevent unauthorized users from entering or using information resources.

All user login IDs are audited at least twice yearly and all inactive logon fingerprints are revoked. The Practice Human Resources Department notifies the Security Officer or appropriate personnel upon the departure of all employees, at which time logins are revoked.

Users who desire to obtain access to Practice systems or networks must have a completed and signed Network Access Form. 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 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 90 days. Compromised passwords shall be changed immediately. At certain client practices if given in writing the rule maybe relaxed or tightened.

Reuse - The previous three 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.

Sessions Management -Session identifiers are rotated on every login attempt by the Platform so that malicious actor cannot use session fixation attack. This is done to prevent session hijacking of an existing session of the user.

Confidentiality Agreement

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

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

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 should 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 or an email 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.

Termination of User Logon Account

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the IT Department by indicating "Remove Access" on

the employee's Network Access Request Form 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 and other access devices as well as Practice equipment and property is returned to the Practice prior to the employee leaving the Practice on their final day of employment.

Network Connectivity

LAN/WAN Connectivity Guidelines

Access to Practice information resources through LAN/WAN are permitted only from Practice equipment. At no point are privately owned or managed, or third-party owned or managed devices (laptops, personal computers, Mobiles, Smart devices etc.) permitted to connect to Practice LAN/WAN. For any exception, the consent of a Privacy officer is must to have.

Use of the Internet

- All employee use of the internet shall be for Practice purposes only.
- Employee use of the internet is monitored and logged including all sites visited, the duration of the visits, amount of data downloaded, and types of data downloaded. The time of recorded activity may also be logged.

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.

Malicious Code

Antivirus Software Installation

Computers running in Practice are having Linux Operating systems with up-to date security patches installed. However virus scanners are installed to prevent adding malicious code on the Practice servers and workstations.Virus Scanners and data files are monitored by appropriate administrative staff that is responsible for keeping all virus patterns up to date.

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.

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.

Encryption

Definition

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

Encryption Key

An encryption key specifies the particular transformation of plain text into ciphertext, 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.

Encryption Key Management

Encrypted keys have been stored in a secure cloud environment, which has restricted access, only selected user has the access to those keys. New keys replace the expired keys and delete the expired key on a cloud platform, this process is manual and System Administrators will do it.

By default keys are refreshed annually. However, from time to time as a security measure keys can rotated randomly to ensure unpredictability.

Server and Data Encryption (AWS Environment)

MediXcel architecture has 2 servers, Application and Database server. Both the servers are behind the AWS firewall and both the server's harddisks are encrypted at rest.

The data in transit will have end-to-end encryption using HTTPS (TLS).

Data at rest is also encrypted using an industry standard AES-256 encryption algorithm.

Secure File Transfer Protocol (SFTP)

Files may be transferred to secure FTP sites through the use of appropriate security precautions. Requests for any SFTP transfers should be directed to the Privacy Officer or appropriate personnel.

Secure Shell (SSH)

Linux EHR servers must be accessed through Secure Shell(SSH), no other methods are allowed. Requests for any server's SSH access should be directed to the Privacy Officer or appropriate personnel.

Secure Socket Layer (SSL) Web Interface

All EHR hosted servers must be equipped with SSL certificates. It is System Administrator's responsibility to have them on Servers. EHR or Medical Data should be accessed through SSL only.

Specific Protocols and Devices

6.1 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 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.

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 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 Practice employees 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 local laws of India or location where the Client is operating the software. As a benchmark Plus91 will use the Health Insurance Portability and Accountability Act ("HIPAA") from the United States of America.

USB key devices are handy devices that 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.

- 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.

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.

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 years.

Data Deletion - Plus91 and MediXcel by default follow all the norms for Data Deletion as laid down in HIPAA guidelines. Additional measures are also added in based on local country guidelines e.g. GDPR (EU) / DISHA (India) etc

- Some standard measures followed are:
    - All hard drives are fully wiped with all confidential information being deleted. Once this is done, new, benign programs should be written to the hard drive. This helps make sure that the confidential data has been overwritten. Preferably, this step is repeated several times to make sure the original confidential data has been completely removed from the hard drive.
    - Any and all traditional hard drives are degaussed.
    - For SSD drives a SSD shredder is used to ensure data is wiped.

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.

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.

Change Management

Statement of Policy

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

Procedure

The IT staff or other designated Practice employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system.

The employee implementing the change will ensure that all necessary data backups are performed prior to the change.

The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

Audit Controls

Statement of Policy

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

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

Procedure

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

Information System Activity Review

Statement of Policy

To establish the process for conducting, on a periodic basis, an operational review of system activity including, but not limited to, user accounts, system access, file access, security incidents, audit logs, and access reports. Practice shall conduct on a regular basis an internal review of records of system activity to minimize security violations.

Procedure

1. See policy entitled Audit Controls for a description of the technical mechanisms that track and record activities on Practice's information systems that contain or use ePHI.
2. The Information Technology Services shall be responsible for conducting reviews of Practice's information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.
3. The Security Officer shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.
4. Such reviews shall be conducted annually. Audits also shall be conducted if Practice has reason to suspect wrongdoing. In conducting these reviews, the Information Technology Services shall examine audit logs for security-significant events including, but not limited to, the following:
    a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.
    b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.
    c. Security incidents – Examine records from security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.
    d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

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

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

Data Security Policy

Statement of Policy

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

The purpose of this policy is to protect Practice's ePHI from improper access, alteration or destruction. This policy applies to all data including but not limited to patient information, IT Systems information, financial information or human resource data.

Procedure

Data Access:

The purpose of the data access policy is to ensure that users have appropriate access to ePHI data and information.

- Only Privileged Users can access the EHR Servers.
- Employees must not keep the Medical data on their workstations.

- Users can not directly download the EHR data received from clients on their office workstations or private laptops. For such cases, instructions from Privacy officers must be followed.
- Access to EHR packages must be controlled by project managers(for the internal team) and PHI should not be accessible/viewable for support users.

Data Integrity:

Practice shall acquire appropriate network-based and host-based intrusion detection systems. The Security Officer shall be responsible for installing, maintaining, and updating such systems.

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

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

1. Practice will install and regularly update antivirus software/scanners on all workstations to detect and prevent malicious code from altering or destroying data.
2. Developers are not allowed to download EHR databases or any ePHI data without taking formal permission from Privacy officer.

Server and Database Access:

All practice's and client's servers are hosted on secure cloud servers or on secured on Premise locations. Only privileged users will get the limited access to these servers.

1. Sharing of server access with other users is strictly prohibited. Only system administrators, with consent of Privacy officer, will provide access to other users on formal request.
2. The activity of users on the servers will be monitored and logged.
3. System administrators will be responsible for providing limited access to developers, and will ensure no PHI data access is provided to developers.
4. Database access must be limited to application server and jump server and/or secure location, must not be accessed from any other location.

Remote Work

- While working remotely, users must use workstations provided by the organization.
- In case of any issues with the workstation provided by Plus91, the IT team will provide an AWS workspace(remote workstation) to work on. Usage of a Personal system for office work is not allowed.

Device Management and Hardening

- **Servers with OS :**
    - Keep Server OS update to date with latest patches. Security patches should be on auto update.
    - Delete unwanted services from the server.
    - Enable firewall if not on AWS, in caase of AWS servers use Amazon Firewall.
    - Limiting the access of the server to only privileged users.
    - Incase of Database servers, block the access of MySQL service for outside environment.
    - If Server is hosted on premises, proper security measures must be taken.
    - Use the encrypted harddisk irrespective of where the server is located/hosted.
    - Password rotation every half year.
- **Laptops and PCs :**
    - Keep system OS up to date with latest updates.
    - Delete unwanted services and files from the system.
    - Scan systems periodically for the malwares.
    - Restrict access from outside network or untrusted network.
    - Not allowed to install unnecessary 3rd party software on a system.
    - Not allowed to store any personal data or patient/client data on system.
- **Remote workstations:**
    - Keep system OS up to date with latest updates.
    - Delete unwanted services and files from the system.
    - Scan systems periodically for the malwares.
    - Restrict access from outside network or untrusted network.
    - Not allowed to store any personal data or patient/client data on system.
    - Restrict admin access to one session.

Contingency Plan

Statement of Policy

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

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

Procedure

Data Backup Plan

- Practice, under the direction of the Security Officer, shall implement a data backup plan to create and maintain retrievable exact copies of ePHI.
- Every workstation on Practice shall be backed up monthly and backup is stored on secure location. All EHR Server's databases shall be backed up weekly on every Sunday and kept in a remote location. Every day's data shall be backed up only on request by a particular client. 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 a 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:
  - 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
  - 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:
  - Current copies of the information systems inventory and network configuration developed and updated as part of Practice's risk analysis.
  - Current copy of the written backup procedures developed and updated pursuant to this policy.
  - An inventory of hard copy forms and documents needed to record clinical, registration, and financial interactions with patients.
  - Identification of an emergency response team. Members of such team shall be responsible for the following:

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

- The disaster recovery team shall meet on at least an annual basis to:
    - Review the effectiveness of the plan in responding to any disaster or emergency experienced by Practice;
    - 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
    - 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.

Security Awareness and Training

Statement of Policy

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

All workforce members shall receive appropriate training concerning Practice's security policies and procedures. Such training shall be provided on Employee joining and on an ongoing basis to all new employees. Such training shall be repeated annually for all employees.

Procedure

a. Security Training Program : 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 Indian Data Protection Laws, Indian EHR Standard and the HIPAA Security Rule including the updates to HIPAA regulations found in the Health Information Technology for Economic and Clinical Health (HITECH) Act. From time to time Client Location Local Laws as needed will also be referred to based on updated regulations. 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.

i. The Security Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of ePHI, e.g., addition of new hardware or software, and increased threats.

b. Security Reminders

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

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

c. Protection from Malicious Software

i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning the prevention, detection, containment, and eradication of malicious software. Such training shall include the following:

a) Guidance on opening suspicious e-mail attachments, e-mail from unfamiliar senders, and hoax e-mail,

b) The importance of updating anti-virus software and how to check a workstation or other device to determine if virus protection is current,

c) Instructions to never download files from unknown or suspicious sources,

d) Recognizing signs of a potential virus that could sneak past antivirus software or could arrive prior to an update to anti-virus software,

e) The importance of backing up critical data on a regular basis and storing the data in a safe place,

f) Damage caused by viruses and worms, and

g) What to do if a virus or worm is detected.

D. Password Management

i. As part of the aforementioned Security Training Program and Security Reminders, the Security Officer shall provide training concerning password management. Such training shall address the importance of confidential passwords in maintaining computer security, as well as the following requirements relating to passwords:

a) Passwords must be changed every 90 days.

b) A user cannot reuse the last 3 passwords.

c) Passwords must be at least eight characters and contain upper case letters, lower case letters, numbers, and special characters.

d) Commonly used words, names, initials, birthdays, or phone numbers should not be used as passwords.

e) A password must be promptly changed if it is suspected of being disclosed, or known to have been disclosed.

f) Passwords must not be disclosed to other workforce members (including anyone claiming to need a password to "fix" a computer or handle an emergency situation) or individuals, including family members.

g) Passwords must not be written down, posted, or exposed in an insecure manner such as on a notepad or posted on the workstation.

h) Employees should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.

i) Any employee who is directed by the Security Officer to change his/her password to conform to the aforementioned standards shall do so immediately.

Security Management Process

Statement of Policy

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

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

Procedure

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

Every 18 months, Security Officer shall request a 3rd party who follows OWASP standards for the vulnerability test of the application and have the application tested by them.

a. The risk analysis shall proceed in the following manner:

i. Document Practice's current information systems.

a) Update/develop information systems inventory. List the following information for all hardware (i.e., network devices, workstations, printers, scanners, mobile devices) and software (i.e., operating system, various applications, interfaces): date acquired, location, vendor, licenses, maintenance schedule, and function. Update/develop network diagram illustrating how organization's information system network is configured.

b) Update/develop facility layout showing location of all information systems equipment, power sources, and other telecommunications

equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.

c) 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. For each application identified, identify the various security controls currently in place and locate any written policies and procedures relating to such controls.

d) Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of ePHI created, received, maintained, or transmitted by Practice. Consider the following:

I. Natural threats, e.g., earthquakes, storm damage.

II. Environmental threats, e.g., fire and smoke damage, power outage, utility problems.

III. Human threats

a) Accidental acts, e.g., input errors and omissions, faulty application programming or processing procedures, failure to update/upgrade software/security devices, lack of adequate financial and human resources to support necessary security controls

b) Inappropriate activities, e.g., inappropriate conduct, abuse of privileges or rights, workplace violence, waste of corporate assets, harassment

c) Illegal operations and intentional attacks, e.g., eavesdropping, snooping, fraud, theft, vandalism, sabotage, blackmail

d) External attacks, e.g., malicious cracking, scanning, demon dialing, virus introduction

i. Identify and document vulnerabilities in Practice's information systems. A vulnerability is a flaw or weakness in security policies and procedures, design, implementation, or controls that could be accidentally triggered or intentionally exploited, resulting in unauthorized access to ePHI, modification of ePHI, denial of service, or repudiation (i.e., the inability to identify the source and hold some person accountable for an action). To accomplish this task, conduct a self-analysis utilizing the standards and implementation specifications to identify vulnerabilities.

e) Determine and document probability and criticality of identified risks.

i. Assign probability level, i.e., likelihood of a security incident involving identified risk.

- "Very Likely" (3) is defined as having a probable chance of occurrence.
- "Likely" (2) is defined as having a significant chance of occurrence.
- "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.

ii. Assign criticality level.

- "High" (3) is defined as having a catastrophic impact on the medical practice including a significant number of medical records which may have been lost or compromised.

- "Medium" (2) is defined as having a significant impact including a moderate number of medical records within the practice which may have been lost or compromised.
- "Low" (1) is defined as a modest or insignificant impact including the loss or compromise of some medical records.

iii. Determine risk score for each identified risk. Multiply the probability score and criticality score. Those risks with a higher risk score require more immediate attention.

f) 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.

g) Develop and document an implementation strategy for critical security measures and safeguards.

- Determine timeline for implementation.
- Determine costs of such measures and safeguards and secure funding.
- Assign responsibility for implementing specific measures and safeguards to appropriate person(s).
- Make necessary adjustments based on implementation experiences.
- Document actual completion dates.

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

c. The Security Officer shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security Officer shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in the Indian Data Protection Laws or the Indian EHR Standards or HIPAA Security Regulations; new local laws or

regulations affecting the security of ePHI in a particular country where the Client is located; changes in technology, environmental processes, or business processes that may affect Security policies or procedures; or the occurrence of a serious security incident. Follow-up evaluations shall include the following:

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

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

Sanction Policy

Policy

It is the policy of the Practice that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. The Practice will impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization.

The Practice will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Practice's information security and privacy policies or local laws or regulations.

Purpose

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

Definitions

Workforce member means employees, volunteers, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity. This includes full and part time employees, affiliates, associates, volunteers, and staff from third party entities who provide service to the covered entity.

Sensitive information, includes, but not limited to, the following:

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

Availability refers to data or information is accessible and useable upon demand by an authorized person.

Confidentiality refers to data or information is not made available or disclosed to unauthorized persons or processes.

Integrity refers to data or information that have not been altered or destroyed in an unauthorized manner.

Violations

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

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job.

	• Sharing computer access codes (user name & password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the Information Security Officer, Privacy Officer, Chief Information Officer, and/or authorized designee.
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

Recommended Disciplinary Actions

In the event that a workforce member violates the Practice's privacy and security policies and/or violates the Local Laws of the Country where the Software is in use or as an internal benchmark they violate what is covered under Health Insurance Portability and Accountability Act of 1996 (HIPAA) governing the protection of sensitive and patient identifiable information, the following recommended disciplinary actions will apply.

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on privacy/security awareness • Retraining on the Practice's privacy and security policies • Retraining on the proper use of internal or required

	forms
2	• Letter of Reprimand*; or suspension • Retraining on privacy/security awareness • Retraining on the Practice's privacy and security policies • Retraining on the proper use of internal or required forms
3	• Termination of employment or contract • Reporting to the Local law if needed

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

e-Discovery Policy: Retention

Policy

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

Purpose

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

Scope

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

Definitions

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

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

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

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

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

Procedure

Guidelines for Retention of Records/Information and Schedules:

Record Retention	Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention

	period has expired, the record is approved for destruction by the record owner, and a Certificate of Destruction is executed.
Non-record Retention	Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated. For example, when the non-record information, such as an employee's personal notes, is transferred to a record, such as an incident report, the notes are no longer useful and should be discarded. Preliminary working papers and superseded drafts should be discarded, particularly after subsequent versions are finalized. Instances where an author or recipient of a document is unsure whether a document is a record as covered or described in this policy should be referred to the Compliance Officer for determination of its status and retention period.

Storage and Destruction Guidelines

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

	Destruction stage is that period after records have served their full purpose, their mandated retention period, and finally are no longer needed.
Storage of Inactive Records	All inactive records identified for storage will be kept with the appropriate servers to the designated off-site storage facility where the records will be protected, stored, and will remain accessible and cataloged for easy retrieval. Except for emergencies, the designated off-site storage facility will provide access to records during normal business hours.
Records Destruction	General Rule: Records that have satisfied their legal, fiscal, administrative, and archival requirements may be destroyed in accordance with the Records Retention Schedules. Permanent Records: Records that cannot be destroyed include records of matters in litigation or records with a permanent retention. In the event of a lawsuit or government investigation, the applicable records that are not permanent cannot be destroyed until the lawsuit or investigation has been finalized. Once the litigation/investigation has been finalized, the record may be destroyed in accordance with the Records Retention Schedules but in no case shall records used in evidence to litigation be destroyed earlier than a specified number of years from the date of the settlement of litigation. Destruction of Records Containing Confidential Information: Records must be destroyed in a manner that ensures the confidentiality of the records and renders the information unrecognizable. The approved methods to destroy records include: A Certificate of Destruction form must be approved by the appropriate management staff prior to the destruction of records. The Certificate of Destruction shall be retained by the off-site storage facility manager. Destruction of Non-Records Containing Confidential Information: Destruction Non-Records containing personal health information or other forms of confidential corporate, employee, member, or patient information of any kind shall be rendered unrecognizable for both source and content by means of shredding, pulping, etc., regardless

	of media. This material shall be deposited in on-site, locked shred collection bins or boxed, sealed, and marked for destruction. Disposal of Electronic Storage Media: Electronic storage media must be assumed to contain confidential or other sensitive information and must not leave the possession of the organization until confirmation that the media is unreadable or until the media is physically destroyed.
Records Destruction, continued	Disposal of Electronic Media: Electronic storage media, such as CD-ROMS, DVDs, tapes, tape reels, USB thumb drives, disk drives or floppy disks containing confidential or sensitive information may only be disposed of by approved destruction methods. These methods include:CD-ROMs, DVDs, magneto-optical cartridges and other storage media that do not use traditional magnetic recording approaches must be physically destroyed. Disposal of IT Assets: Department managers must coordinate with the IT Department on disposing surplus property that is no longer needed for business activities according to the Disposal of IT Assets Policy. Disposal of information system equipment, including the irreversible removal of information and software, must occur in accordance with approved procedures and will be coordinated by IT personnel.

Appendix C

Network Access Request Form

Manager:	**Department:**
Request Date:	
Employee Name: **Designation:** **Email ID:** **Mobile Number**	
Reason for Request:	