HIPAA

(HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT, 1996)

MANUAL
Version 2.0

Seyyone Software Solutions (P) Ltd
Coimbatore
INDIA

(Private and Confidential - For Internal Circulation only)

January 01, 2020.

"What I may see or hear in the course of the transcription or even outside of the transcription process in regard to the life of men, which on no account one must spread across, I will keep to myself, holding such things shameful to be Spoken about."

- Seyyone Hippocratic Oath

TABLE OF CONTENTS

Preface

The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) are intended to promote efficiency and reduce administrative costs in the health care system by "encouraging the development of a health information system through the establishment of standards and requirements for the electronic maintenance and transmission of certain health information''.

HIPAA requires the Secretary of Health and Human Services to enact rules to establish national standards for a host of electronic transactions between employers, health plans and health care providers. Given the sensitive nature of health information, the statute also requires DHHS to adopt standards for privacy of individually identifiable health information and security of health information systems.

Public and private health benefit programs, health care transaction clearinghouses, and health care providers that use computers for the "HIPAA transactions" are required to comply with the DHHS standards.

This HIPAA manual briefly explains various security regulations, policies and standards for accomplishing HIPAA compliance with respect to Seyyone operation.

Members of staff are requested to extend their cooperation n and strictly adhere to the policies and guidelines to accomplish and comply with HIPAA Standards.

S/d Management

Disclaimer

This Manual is designed to acquaint the employees of Seyyone with HIPAA and provide them with information about HIPAA Compliance, Security Rule and Non- compliance sanctions.

The information contained in this Manual applies to all employees of Seyyone. Following the policies described in this Manual is considered a condition of employment. However, nothing in this Manual alters an employee's status. The contents of this Manual shall not constitute nor be construed as a promise of employment or as a contract between the Company and any of its employees. The Manual is a summary of our policies, which are presented here only as a matter of information.

The employees of Seyyone are responsible for reading, understanding, and complying with the provisions of this Manual. Our objective is to provide you with a work environment that is constructive to both personal, professional growth and for Statutory Compliance.

1.1 CHANGES IN POLICY

This Manual supersedes all previous employee manuals and memos that may have been issued from time to time on subjects covered in this Manual.

However, in case our business and our organization are subject to change, we reserve the right to interpret, change, suspend, cancel, or dispute with or without notice all or any part of our policies, procedures, and benefits at any time. We will notify all employees of these changes. Changes will be effective on the dates determined by the Company, and after those dates all superseded policies will be null.

Except management, no individual supervisor or manager has the authority to change policies at any time. If you are uncertain about any policy or procedure, speak with your direct superior.

HIPAA - An Introduction

In 1996 Congress passed into law the Health Insurance Portability and Accountability Act (HIPAA). This Act is comprised of two major legislative actions:

I. A Health Insurance Reform

II. A Administrative Simplification

The Administrative Simplification provisions of HIPAA direct the federal government to adopt *national electronic standards* for automated transfer of certain health care data between health care payers, plans, and providers. This will enable the *entire* health care industry to communicate electronic data using a *single set* of standards, thus eliminating all non-standard formats currently in use.

HIPAA Administrative Simplification provisions require the Department of Health and Human Services to promulgate standards for the electronic exchange of certain administrative and financial transactions and for the security and privacy of health information. The Administrative Simplification provisions are implemented through a package of regulations, all of which apply to three distinct covered entities: health plans, health care clearinghouses, and health care providers who transmit health information electronically in connection with standardized transactions.

The Standards for Privacy of Individually Identifiable Health Information regulation establishes standards for the use and disclosure of protected health information. It also establishes some patient rights, including individuals' access to records.

SUMMARY

In order to administer their programs, the United States of America's Department of Health and Human Services, other Federal agencies, State Medicaid agencies, private health plans, health care providers, and health care clearinghouses (Medical Transcription) must assure their customers (such as patients, insured, providers, and health care plans) that the confidentiality and privacy of health care information they electronically collect, maintain, use, or transmit is secure.

Security of health information is especially important when health information can be directly linked to an individual.

Confidentiality is threatened not only by the risk of improper access to electronically stored information, but also by the risk of interception during electronic transmission of the information.

In addition to the need to ensure electronic health care information is secure and confidential, there is a potential need to associate signature capability with information being electronically stored or transmitted.

The Reality

Section 1176 of the Act establishes a civil monetary penalty for violation of the provisions in part C of title XI of the Act, subject to several limitations. Penalties may not be more than $100 per person per violation and not more than $25,000 per person for violations of a single standard for a calendar year. The procedural provisions in section 1128A of the Act, "Civil Monetary Penalties," are applicable.

Section 1177 of the Act establishes penalties for a knowing misuse of unique health identifiers and individually identifiable health information: (1) A fine of not more than $50,000 and/or imprisonment of not more than 1 year; (2) if misuse is "under false pretenses," a fine of not more than $100,000 and/or imprisonment of not more than 5 years; and (3) if misuse is with intent to sell, transfer, or use individually identifiable health information for commercial advantage, personal gain, or malicious harm, a fine of not more than $250,000 and/or imprisonment of not more than 10 years. Note that these penalties do not affect any other penalties, which may be imposed by other Federal programs, including ERISA.

I. USES AND DISCLOSURES OF HEALTH INFORMATION

It is the policy of Seyyone Software Solution P Ltd herein collectively called as “Seyyone”, that an individual’s identifiable protected health information may only be used within Seyyone premises or disclosed to entities outside Seyyone only after notification to and/or with the express permission of the management and with the compliance of HIPAA, except in cases of emergency or where specifically permitted or required by law. Access to information stored in any Seyyone file or depository, Stored electronically, or that exists in any recording device or research data base, collectively hereafter referred to as “health record”, is limited to those who have a valid business or medical need for the information or otherwise have a right to know the information. With the exception of purposes related to production and other limited exceptions, access to an individual^ protected health information must, to the extent practicable, be limited only to that necessary to accomplish the intended purpose of the approved use, disclosure or request.

II. POLICY PURPOSE

1. The purpose of the policies are to assure that protected health information contained in any form, health record is only used or disclosed for its intended purpose in accordance with general and/or specific patient notifications and permissions.

III. POLICY STANDARDS

1. An individual's protected health information may be used by any form after concerned person has provided to the individual and has made a good faith effort to obtain an acknowledgment of its receipt. If required, an authorized person may use an individual’s protected health information for other (non-routine) purposes or may disclose an individual's protected health information to external entities for non-routine purposes upon obtaining a valid authorization. When authorization is required, this requirement to obtain authorization may only be waived by the HIPAA Officer.

2. From time to time, Seyyone may disclose protected health information to other entities for use by the recipient for any purpose. Further, Seyyone may disclose protected health information to other entities to assist the recipient in obtaining payment and, under limited circumstances, may disclose identifiable health information to other entities for purposes associated with healthcare operations.

IV. MINIMUM NECESSARY STANDARDS AND SECURITY

1. Health information may only be accessed, used or disclosed by authorized personnel. With the exception of the use and disclosure of health information directly related to production, to the individual, pursuant to an authorization, as required by law and for compliance purposes, and to the extent practicable, access to health information by Seyyone employees or other authorized personnel is restricted to the minimum necessary to execute their job responsibilities. It is the responsibility of each department or administrative unit to identify those persons or classes of persons who are authorized to access, use or disclose health information and specifically to identify what health information they may have access to, and limit their access to that information.

2. Physical access to controlled areas and user accounts that provide access to protected health information are to be revoked upon the termination of an employee or trainee or when others, such as contractors or vendors, no longer require access. All protected health information in the possession of these individuals or entities is to be returned to the concerned or, in the alternative, an attestation must be received indicating that such information has been destroyed. If this is not possible due to the nature of an on-going research effort, a statement must be received by the HIPAA Officer attesting that the health information will remain confidential and safeguarded as long as it is in the possession of Seyyone.

V. POLICY SANCTIONS

1. The unauthorized access to or unauthorized use or disclosure of protected health information that exists in Seyyone health record may subject the responsible employee or trainee to disciplinary action up to and including termination from employment or suspension or expulsion from an employee or trainee program. This extends to the unauthorized use or disclosure of health information that is overheard during the course of business or health information that is otherwise learned or secured by any employee or trainee by virtue of their employment or training association within the Campus.

2. Any department or administrative units that become aware of the unauthorized use or disclosure of protected health information that causes or reasonably could cause harm should immediately report the incident to the HIPAA Officer. To the extent practicable, the concerned person should attempt to minimize the known harmful effects and/or correct instances of harm.

VI. HIPAA TRAINING

1. All employees who may use, disclose, or have access to protected health information contained in any health record must, as a condition of continued employment, complete a training program that outlines employee responsibility and patient rights under the statutory privacy regulations contained in the Health Insurance Portability and Accountability Act (HIPAA). Additionally, all employee or trainees who may use, disclose, or have access to any protected health information contained in any heath record must complete a training program of their obligations regarding patient rights under HIPAA.

Purpose:

The purpose of this policy is to provide guidance that limits the use of encryption to those algorithms that have received substantial public review and have been proven to work effectively.

Scope:

This policy applies to all Seyyone employees and affiliates.

Policy:

1. Algorithm Requirements:

Ciphers in use must meet or exceed the set defined as "AES-compatible" or "partially AES-compatible" according to the IETF/IRTF Cipher Catalogue, or the set defined for use in the United States National Institute of Standards and Technology (NIST) publication FIPS 140-2, or any superseding documents according to the date of implementation. The use of the Advanced Encryption Standard (AES) is strongly recommended for symmetric encryption.

Algorithms in use must meet the standards defined for use in NIST publication FIPS 140-2 or any superseding document, according to date of implementation. The use of the RSA and Elliptic Curve Cryptography (ECC) algorithms is strongly recommended for asymmetric encryption.

2. Key Agreement and Authentication

Key exchanges must use one of the following cryptographic protocols: Diffie-Hellman, IKE, or Elliptic curve Diffie-Hellman (ECDH).

End points must be authenticated prior to the exchange or derivation of session keys.

Public keys used to establish trust must be authenticated prior to use. Examples of authentication include transmission via cryptographically signed message or manual verification of the public key hash.

All servers used for authentication (for example, RADIUS or TACACS) must have installed a valid certificate signed by a known trusted provider.

All servers and applications using SSL or TLS must have the certificates signed by a known, trusted provider.

3. Control of peripherals

Cryptographic keys must be generated and stored in a secure manner that prevents loss, theft, or compromise.

Key generation must be seeded from an industry standard random number generator (RNG).

Policy Compliance:

1. Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, business tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the InfoSec team in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Process

None

Policy Statement:

It is the policy of Seyyone that access to all company owned assets & information is limited to authorized purposes as approved by the authority

Access Control protects information by managing access to all entry and exit points, both logical and physical. Adequate perimeter security and logical security measures must protect against unauthorized access to sensitive information on a Seyyone facility, network, or application. These measures ensure that only authorized users, as warranted by security rule and statuary regulation, have access to specific computer resources, networks, data, and applications.

Objective:

- To control access to information
- To communicate the need for access control.
- To prevent unauthorized access to information systems
- To establish specific requirements for protecting against unauthorized access.
- To create an infrastructure that will foster data sharing without sacrificing security of Information resources.
- To prevent unauthorized user access
- Protection of network services
- To prevent unauthorized computer access (OS Access control)

Scope:

The scope of Access Control Policy is applicable to all members of Seyyone including management and restricted to Seyyone premises and is not applicable to outsource member or partner.

Procedure:

1. Privilege management:

All personnel will be given access control based on the Privilege provided by the management on the basis of Role and Responsibility.

2. Enforcing paths from user terminals to Server

All client/Workstation are configures to communicate/work according to the predetermined path decided by the IT Security Department. Enforcing paths for the workstation will prevent unauthorized intervention and access.

3. Control of peripherals

All peripherals (Printer, Scanner etc.) in the Seyyone premises will be guarded by appropriate security mechanism formulated/sited by HIPAA Physical Security Policy.

4. Access Control List:

All EPHI accessed by the Seyyone personnel will be routed under predetermined ACL for each Data or file.

5. Written/Expressed Policy Hand Book

All employees of Seyyone at the time of joining the organization will be provided with Policies and procedure & Responsibility Handbook, which act as guidelines for ensuring the HIPAA Policies.

6. Policies and Procedures strictly enforced (Even Fines)

With reference to the HIPAA Compliance Sec Enforcement & Grievance Policy of Seyyone, all personnel will be enforced to comply with the expressed policies and procedure, any non-compliance will be escalated to the appropriate channel, which may result in imposing sanctions and fines (Non-compliance may be lead to termination of the employee).

Tools & Methodologies

Job Description and Privilege

User name & Password

Access Control List (Allotment List)

IP Tables (Group wise rights table)

Forms, Templates & Check List:

Allotment Sheet

File server access control

Policy Statement:

All computers connected to the Seyyone computer network resources shall have the most current antivirus software correctly installed, configured, activated, and updated with the latest version of virus definitions to prevent virus propagation or other forms of malicious code to other networked devices and shall be disconnected from the network until the infection has been removed.

Objective:

- To prevent infection of Seyyone computers and computer systems by computer viruses and other malicious code. This policy is intended to prevent major and widespread damage to user applications, files and hardware.
- To protect network resources against malicious virus attack
- To ensure virus free IT resource

Scope:

The scope of the Antivirus policy is applicable to all Server, client systems and networks installed in Seyyone premises.

Procedure:

- If the installation source is Seyyone distributed CD-ROM, the antivirus software shall be installed before establishing any connection to the network. Upon establishing the initial network connection, the virus definitions shall be updated to the most current version immediately and before loading or installing any other software or data.

- If the installation source is a Seyyone server, the computer shall be connected to the network for the sole purpose of installing antivirus software from that server. The installation shall be performed immediately upon establishing the initial network connection and virus updates downloaded and installed before loading or installing any other software or data.

  Under all other circumstances, any computer connected to the network shall have antivirus software properly installed, configured, and updated before being connected to the network. Seyyone strongly enforce that:

- Virus definitions should be updated daily before retrieving email.
- All files on all hard drives should be scanned weekly.
- Any unexpected virus intrusion and abnormal behavior should be properly informed to systems.

When an enterprise-wide virus attack is in progress, Seyyone shall notify all concerned via the best available method and all files on all hard drives will be scanned immediately using the newest virus definitions available.

Other operating systems or computing platforms will have complete virus protection mechanisms. Seyyone Information Technology Security Officer must explicitly approve any exceptions to this policy.

Non-Compliance:

Policies and Procedures strictly enforced (Even Fines)

With reference to the HIPAA Compliance Sec Enforcement & Grievance Policy of Seyyone, all personnel will be enforced to comply with the expressed policies and procedure, any non-compliance will be escalated to the appropriate channel, which may result in imposing sanctions and fines (Non-compliance may be lead to termination of the employee).

Tools & Methodologies

- Norton Antivirus 2004 Professional
- McAfee 2004 installed all client nodes and live updated latest version
- Scheduled virus scanning weekly
- Scheduled auto virus definitions updates daily
- Auto protect enabled
- Centralized management tools installed and maintained
- Enabled web, mails, messenger protection
- Gateway virus wall installed

Forms, Templates & Check List:

1. Antivirus audit checklist

Guidelines:

1. **Do not open** any files attached to an email from an unknown, suspicious or untrustworthy source.
2. **Do not open** any files attached to an email unless you know what it is, even if it appears to come from a dear friend or someone known. Some viruses can replicate themselves and spread through email. Better be safe than sorry and confirm that they really sent it.
3. **Do not open** any files attached to an email if the subject line is questionable or unexpected. If the need to do so is there always save the file to your hard drive before doing so.
4. **Delete chain emails and junk email**. Do not forward or reply to any to them. These types of email are considered spam, which is unsolicited, intrusive mail that clogs up the network.
5. **Do not download** any files from strangers.
6. **Exercise caution** when downloading files from the Internet. Ensure that the source is a legitimate and reputable one. Verify that an anti-virus program chocks the files on the download site. If you're uncertain, don't download the file at all or download the file to a floppy and test it with anti-virus software.
7. **Update anti-virus software regularly**. Updates the products virus signature files. You may also need to update the product's scanning engine as well.

When in doubt, always be on the side of caution and do not open, download, or execute any files or email attachments. Not executing is the more important of these caveats. Check with your IT Security systems personnel for updates and assistants.

Policy Statement:

Seyyone shall maintain an asset management system for fixed assets and controlled assets that provides sufficient information to permit the preparation of year-end financial statements, allows for the purchase of adequate and appropriate insurance coverage, ensures proper use, and provides tor their maintenance, replacement and disposal.

Objective:

- To maintain appropriate protection of organizational assets
- To ensure that information assets receive an appropriate level of protection
- To ensure optimum utilization of resources

Scope:

The scope of this policy covers all tangible and intangible assets of the organization

Procedure:

1. All assets of Seyyone will be duly accounted, and monitored by real time Inventory system at various levels, it shall be divided in to Departmental Assets and Organizational asset
2. Preventive maintenance and up keeping activities of resources will be carried on a predetermined intervals.
3. Assets which pertaining to the direct production function will have a reasonable buffer stock to meet any breakdown. EOQ & EOL will be arrived.
4. All purchased and maintenance work will be routed thru the Departmental Heads
5. Labelling and Tag Identification:

1. All assets of Seyyone will be properly identified, and labelled according to the reasonable standard. Suitable Tag identification methods will be carried out for loose & movable inventories.
6. All new assets and inventories will be purchased according to the predefined procedure based on VED analysis.
7. All disposal shall be carried by a designated personnel, to avoid any EPHI to be moved out of the premises
8. Asset recording, valuation and reporting will be submitted to Management as MIS reports.

The asset shall be broadly classified as follows:

a. **Information assets** Databases and data files, system documentation, user manuals, training material, operational or support procedures, continuity plans, fall-back arrangements;
b. **Software assets** Application software, system software, development tools and utilities;
c. **Physical assets** Computer and communications equipment, magnetic media (tapes and disks), other technical equipment (power supplies, air-conditioning units), furniture, accommodation; and
d. **Services** Computing and communications services, other technical services (heating, lighting, power, air-conditioning).

The asset information may be as follows:

1. Asset number
2. Description
3. Asset classification (i.e. land, building, equipment, etc.)
4. Location (site, building and room)
5. Date of purchase
6. Purchase price
7. Serial number and model number
8. Estimated life of asset

Forms & Check List

1. Stock Register
2. Inward outward Register
3. Gate Pass

Infrastructure Maintenance Chart/Schedule

Policy Statement:

All established procedures would be audited periodically to attain minimum acceptable non-compliance.

Objective:

Audits may be conducted:

- To Ensure integrity, confidentiality and availability of information and resources
- To Investigate possible security incidents for conformance to Seyyone security policies
- To monitor user or system activity where appropriate.

Scope:

This policy covers all computer and communication devices owned and operated by Seyyone. This Policy also covers any computer and communications device that are present on Seyyone premises.

The scope of this Policy covers the hardware, software and or procedural mechanisms that will be implemented by Seyyone production process to record and examine activity in information systems that contain or use EPHI.

The Audit policy binds all functions of physical, technical and human resources of Seyyone

Procedure:

HIPAA Compliance Officer

Seyyone employs a full time Security and Privacy Officer to oversee any activities that are related to the development, implementation, maintenance of, and adherence to all policies and procedures that cover the privacy of, and access to, patient health information. The Privacy officer also reviews, revises and formulates all policies necessary to guide the proper access and minimum disclosure transcription records. He also assists in the development of training materials and systems to optimise Seyyone HIPAA compliance. The Security Privacy Officer reports directly to the Management and gives monthly reports on the company's compliance effectiveness.

1) Audit Control Mechanisms

(a) Each Production Unit with systems containing medium and high risk EPHI will utilize a mechanism to log and store system activity.

(b) Each system's audit log must include, but is not limited to, User ID, Login Date/Time, and Activity Time. Audit logs may include system and application log-in reports, activity reports, exception reports or other mechanisms to document and manage system and application activity.

(c) System audit logs must be reviewed on a regular basis.

(d) Implementation of an audit control mechanism for systems containing low risk EPHI is not required.

2) Audit Control and Review Plan

An Audit Control and Review Plan must be established by each department and approved by the HIPAA IT Security Team. If the Seyyone EPHI inventories changes, its Audit Control and Review Plan must be revaluated and resubmitted to HIPAA Security Team. The plan must include:

- Systems and applications to be logged
- Information to be logged for each system
- Log-in reports for each system
- Procedures to review all audit logs and activity reports

3) System Imposed Audit Trial:

4) Software Controlled Audit Trial:

5) Periodic MIS Report

6) Policies and Procedures strictly enforced (Even Fines)

With reference to the HIPAA Compliance Sec Enforcement & Grievance Policy of Seyyone, all personnel will be enforced to comply with the expressed policies and procedure, any non-compliance will be escalated to the appropriate channel, which may result in imposing sanctions and fines (Non-compliance may be lead to termination of the employee).

Tools & Methodologies

- Periodic auditing with checklist for anti virus
- Periodic auditing device and media control with check list
- Version control auditing
- User log auditing
- Intrusion detection auditing
- Backup auditing

Forms, Templates & Check List:

The following checklist have been employed for Auditing:

1. Authentication Forms (Refer Annexure)

1. Password change/Control form
2. Employee clearance form (Technical Clearance)
3. Privilege requisition form

2. Access control forms (Refer Annexure)

1. File Based access control List (Allotment Sheet)
2. Folder Level access control (Samba folder access control sheet)
3. Machine Usage Register (Exceptional)
4. Monitoring of system access/security form

3. Physical Security control form (Refer Annexure)

1. Key control form
2. Inward-outward register
3. Visitor's entry book
4. Stock Register
5. Equipment/infrastructure preventive maintenance checklist
6. Event Reporting/Non Compliance form

Policy Statement:

Seyyone and its members are committed to conducting business in compliance with all applicable laws, regulations and Seyyone policies. Seyyone has adopted this policy to set forth the authentication requirements for access to Seyyone EPHI.

Objective:

To ensure

- Confidentiality

  Unauthorized users cannot access data

- Integrity

  Unauthorized users cannot manipulate/destroy data

- Availability

  Unauthorized users cannot make system resources unavailable to legitimate users

Scope:

The scope of this Policy covers the procedures to be implemented by each Seyyone members, which ensures Transcription component to verify that a person or entity seeking access to EPHI is the person or entity claimed.

Procedure:

1. Workforce members seeking access to any network, system, or application that contains EPHI must satisfy a user authentication mechanism such as unique user identification and password, biometric input, or a user identification smart card to verify their authenticity.

2. Workforce members seeking access to any network, system, or application must not misrepresent themselves by using another person's User ID and Password, smart card, or other authentication information.

3. Workforce members are not permitted to allow other persons or entities to use their unique User ID and password, smart card, or other authentication information.

4. A reasonable effort is made to verify the identity of the receiving person or entity prior to transmitting EPHI.

5. Unique individual identifier for each user/Uniform user ID across organization:

   Unique individual personnel user ID have been assigned to all employees across the organization, right from attendance entry and to system authentication unique predefined user ID will be used at Seyyone.

6. Screen Lock/Seeking automatic password after a specified time:

   All workstation and servers are configured with the screen lock, which will seek password after a specified time, which ensures minimum EPHI accessibility.

7. Enforcement of periodic changes of password:

   All user and administrative password of Seyyone will be changed at a predetermined interval; employees are strictly enforced to follow the password policy of the organization

8. Different Security for terminals in different location:

   Users/Terminals are discriminated by groups and domains to allocate group level /domain level access control, the classified users and domains will exists in various different location, separate access control policies for each group/domain is enforced.

9. Termination of accounts/user ID when employee leaves:

As per the Recruitment Policy of Seyyone, user ID, password and all access control of a terminated/leaving person will be Void and deleted/destroyed in all possible ways.

10. Written/Expressed Policy Hand Book

All employees of Seyyone at the time of joining the organization will be provided with Policies and procedure & Responsibility Handbook, which act as guidelines for ensuring the HIPAA Policies

11. Policies and Procedures strictly Enforced (Even Fines)

With reference to the HIPAA Compliance Sec Enforcement & Grievance Policy of Seyyone, all personnel will be enforced to comply with the expressed policies and procedure, any non-compliance will be escalated to the appropriate channel, which may result in imposing sanctions and fines (Non-compliance may be lead to termination of the employee).

Tools & Methodologies

Authentication Procedure Model

CLASSIFICATION DESCRIPTION PROCEDURE

Classification	Description	Procedure
Level - 1 PUBLIC	Non-Sensitive information that can be freely released to anyone. Examples: - product brochures - corporate website	No action - no need to verify identity of requestor.
Level - 2 INTERNAL	Information intended for use only Between employees and partners. Examples: - personnel reporting structure - employee names and titles - internal phone numbers - names of departments & projects	Verify identity of requestor to ensure they are indeed an active employee or verify that a nondisclosure agreement is on file and management approval of non-employee partner is confirmed.

Level - 3 CONFIDENTIAL	Sensitive information that is shared only between employees and partners that have a *verified* need to know. Examples: - social security numbers - credit card numbers - salary information - quotations - computer configuration info - computer system procedure - source code - all remote access info - manufacturing processes - marketing data - business plans - product / part specification - customer list - trade secrets	Same as Internal procedure above plus... Verify need to know with content owner before disclosing any information to the requestor. Note: - Only management personnel may authorize discloser of this level of information to non-employees. - Shared all documents that contain any confidential information before throwing away.
Level - 4 RESTRICTED	Information that is not to be shared. Example : Passwords	Never disclose restricted information to anyone under any circumstance, especially you password – not even to the IT Help Desk or IT Security.

Forms, Templates & Check List:

1. Password change control form
2. Unique User ID across organization
3. Privilege requisition/control form
4. Key Tag

Policy Statement:

Seyyone is committed in policy, principle, and practice to maintain an environment, which is divest of illegal discriminatory behavior and provides equal opportunity for all persons regardless of race, color, religion, creed, gender, age, marital status, national origin, mental or physical disability and veteran status.

Objective:

The objectives of this policy are as follows:

1. To avoid breaches of any criminal or civil law, statutory, regulatory or contractual obligations and of any security requirements
2. To ensure compliance of systems with organizational security policies and standards
3. To maximize the effectiveness of and to minimize interference to/from the system audit process.

Scope:

The HIPAA Compliance and Grievance Policy of Seyyone are drafted to accomplish the following:

1. Protect PHI from accidental or intentional misuse or disclosure;
2. Establish a procedure for handling grievances for violations of the privacy policies;
3. Impose sanctions against individuals and employees that violate privacy policies;
4. Mitigate errant disclosures by the organization member;
5. Prevent retaliation for complaints about non-compliance

Procedure:

1. Training of employees on their privacy policies and are required re-training them if material changes are made to policies.

Policy Statement:

Seyyone and its members are committed to conducting business in compliance with all applicable laws, regulations and Seyyone policies. Seyyone has adopted this policy to ensure that the receipt and removal of hardware and electronic media containing EPHI complies with the Security Regulations.

Scope:

The scope of this policy is to outline the policy and procedures that govern the receipt and removal of hardware and electronic media that contain EPHI into and out of a facility and the movement of such items within the facility.

Policy:

1) General Application of Policy

a) These policies and procedures pertain to the use of hard drives, storage systems, removable disks, floppy drives, CD ROMs, PCMCIA cards, memory sticks, and all other forms of removable media and storage devices.

b) The procedures developed pursuant to this Policy must be documented and submitted to the HIPAA Security Office for approval.

2) Destruction of Storage Devices or Removable Media

a) Prior to destroying or disposing of any storage device or removable media, care must be taken to ensure that the device or media does not contain EPHI.

b) If the device or media contains the only copy of EPHI that is required or needed, a retrievable copy of the EPHI must be made prior to disposal.

c) If the device or media contains EPHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or me dia prior to disposal. A typical reformat is not sufficient, as it does not overwrite the data.

3) Reuse of Storage Devices or Removable Media

a) Prior to making storage devices and removable media available for reuse, care must be taken to ensure that the device or media does not contain EPHI.

b) If the device or media contains the only copy of EPHI that is required or needed, a retrievable copy of the EPHI must be made prior to reuse.

c) If the device or media contains EPHI that is not required or needed, and is not a unique copy, a data destruction tool must be used to destroy the data on the device or media prior to reuse. A typical reformat is not sufficient, as it does not overwrite the data.

d) If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, the use of a data destruction tool between uses is not necessary.

4) Movement of Equipment Housing EPHI

a) Each Business Unit shall develop a procedure to determine when an exact retrievable copy of EPHI is required prior to the movement of equipment storing such EPHI.

b) When using storage devices and removable media to transport EPHI each Business Unit/Production Units must develop a procedure to track and maintain records of the movement of such devices and the media and the parties responsible for the device and media during its movement.

Policy Statement:

Seyyone will recover from disaster incident in the minimum amount of time, with minimum disruption and at minimum cost.

Objective:

This disaster recovery plan has the following primary objectives:

1. Present an orderly course of action for restoring critical computing capability to the SEYYONE campus within said period of initiation of the plan.
2. Set criteria for making the decision to recover at a cold site or repair the affected site.
3. Describe an organizational structure for carrying out the plan.
4. Provide information concerning personnel that will be required to carry out the plan and the computing expertise required.
5. Identify the equipment, floor plan, procedures, and other items necessary for the recovery.

Procedure:

Personnel

Immediately following the disaster, a planned sequence of events begins. Key personnel are notified and recovery teams are grouped to implement the plan. Personnel currently employed are listed in the plan. However, the plan has been designed to be usable even if some or all of the personnel are unavailable.

Salvage Operations at Disaster Site

Early efforts are targeted at protecting and preserving the computer equipment. In particular, any magnetic storage media (hard drives, magnetic tapes, diskettes) are identified and either protected from the elements or removed to a clean, dry environment away from the disaster site.

Designate Recovery Site

At the same time, a survey of the disaster scene is done by the designated personnel to estimate the amount of time required to put the facility (in this case, the building and utilities) back into working order. A decision is then made whether to use the Cold Site, a location some distance away from the scene of the disaster where computing and networking capabilities can be temporarily restored until the primary site is ready. Work begins almost immediately at repairing or rebuilding the primary site. This may take months, the details of which are beyond the scope of this document.

Purchase of New Equipment

The recovery process relies heavily upon vendors to quickly provide replacements for the resources that cannot be salvaged. The University will rely upon emergency procurement procedures documented in this plan and approved by the University's purchasing office and the Office of State Purchasing to quickly place orders for equipment, supplies, software, and any other needs.

Begin Reassembly at Recovery Site

Salvaged and new components are reassembled at the recovery site according to the instructions contained in this plan. Since all plans of this type are subject to the inherent changes that occur in the computer industry, it may become necessary for recovery personnel to deviate from the plan, especially if the plan has not been keep up-to-date. If vendors cannot provide a certain piece of equipment on a timely basis, it may be necessary for the recovery personnel to make last-minute substitutions. After the equipment reassembly phase is complete, the work turns to concentrate on the data recovery procedures.

Restore Data from Backups

Data recovery relies entirely upon the use of backups stored in locations off-site from the Administrative Services Building. Backups can take the form of magnetic tape, CDROMs, disk drives, and other storage media. Early data recovery efforts focus on restoring the operating system(s) for each computer system. Next, first line recovery of application and user data from the backup tapes is done. Individual application owners may need to be involved at this point, so terms are assigned for each major application area to ensure that data is restored properly.

Restore Applications Data

It is at this point that the disaster recovery plans for users and departments (e.g., the application owners) must merge with the completion of the Computing Services plan. Since some time may have elapsed between the time that the off-site backups were made and the time of the disaster, application owners must have means for restoring each running application database to the point of the disaster. They must also take all new data collected since that point and input it into the application databases. When this process is complete, the University computer systems can reopen for business. Some applications may be available only to a limited few key personnel, while others may be available to anyone who can access the computer systems.

Move Back to Restored Permanent Facility

If the recovery process has taken place at the Cold Site, physical restoration of the Administrative Services Building (or an alternate facility) will have begun. When that facility is ready for occupancy, the systems assembled at the Cold Site arc to be moved back to their permanent home. This plan does not attempt to address the logistics of this move, which should be vastly less complicated than the work done to do the recovery at the Cold Site.

Operational Recoverability Handbook

Operational Recoverability handbook for software list and installation procedures has been created for the following functions.

- Redundant server configuration
- Virus attacks
- Mail and firewall reconfiguration
- Workstation installation
- EPHI logistics

Contingency Plan

Policy Statement:

Seyyone and its members are committed to conducting business in compliance with all applicable laws, regulations and Seyyone policies. Seyyone has adopted this policy to ensure that its response to an emergency or other occurrence that damages systems that contain EPHI complies with the Security Regulations.

Scope:

The scope of this Policy covers the procedures that each production function must develop for implementation in the event of an emergency, disaster or other occurrence (i.e., fire, vandalism, system failure and natural disaster) when any system that contains EPHI is affected, including:

- Applications and data criticality analysis
- Data backup
- Disaster Recovery Planning
- Emergency mode operation plan

1) Applications and Data Criticality Analysis

a) Each production function must assess the relative criticality of specific applications and data within the unit for purposes of developing its Data Backup Plan, its Disaster Recovery Plan and its Emergency Mode Operation Plan.

b) The assessment of data and application criticality should be conducted periodically and at least annually to ensure that appropriate procedures are in place for data and applications at each level of risk.

2) Data Backup Plan

a) Each function must establish and implement a Data Backup Plan pursuant to which it would create and maintain retrievable exact copies of all EPHI determined to be medium and high risk.

b) The Data Backup Plan must apply to all medium and high risk files, records, images, voice or video files that may contain EPHI.

c) The Data Backup Plan must require that all media used for backing up EPHI be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up.

d) If an off-site storage facility or backup service is used, a written contract or Business Associate Agreement must be used to ensure that the Business Associate will safeguard the EPHI in an appropriate manner.

e) Data backup procedures outlined in the Data Backup Plan must be tested on a periodic basis to ensure that exact copies of EPHI can be retrieved and made available.

f) Each Business Unit with medium and high risk EPHI must submit its Data Backup Plan to the HIPAA Security Office for approval.

3) Disaster Recovery Plan

a) To ensure that each Business Unit can recover from the loss of data due to an emergency or disaster such as fire, vandalism, terrorism, system failure, or natural disaster effecting systems containing EPHI, each Business Unit must establish and implement a Disaster Recover Plan pursuant to which it can restore or recover any loss of EPHI and the systems needed to make that EPHI available in a timely manner.

b) The Disaster Recovery Plan should include procedures to restore EPHI from data backups in the case of a disaster causing data loss.

c) The Disaster Recovery Plan should include procedures to log system outages, failures, and data loss to critical systems, and procedures to train the appropriate personnel to implement the disaster recovery plan.

d) The Disaster Recovery Plan must be documented and easily available to the necessary personnel at all time, who should be trained to implement the Disaster Recovery Plan.

e) The disaster recovery procedures outlined in the Disaster Recovery Plan must be tested on a periodic basis to ensure that EPHI and the systems needed to make EPHI available can be restored or recovered.

f) Each Business Unit with medium and high risk EPHI must submit its Disaster Recovery Plan to the HIPAA Security Office for approval.

4) Emergency Mode Operation Plan

a) Each unit must establish and implement (as needed) procedures to enable continuation of critical business processes for protection of the security of EPHI while operating in emergency mode.

b) Emergency mode operation procedures outlined in the Emergency Mode Operation Plan must be tested on a periodic basis to ensure that critical business processes can continue in a satisfactory manner while operating in emergency mode.

c) Each unit with medium and high risk EPHI must submit its Emergency Mode Operation Plan to the HIPAA Security Office for approval.

Identifying resources absolutely be secure and in order of priority:

- Mission critical
- Redundant back-up system(s)
- Secondary
- Base systems

Access to network documentation

- > Network diagrams
- > Trending data

- > Protocol utilization
- > Data points Access points
- > Major vendors' point of contact information (ISP, firewall vendor)
- > IP Tables

System restoration order:

Security violation reports
Denied access messages
Failed passwords/login attempts
Attempts to access back doors
Periodic drills to test systems and procedures

"DISCLOSURES OF PROTECTED HEALTH INFORMATION TO THOSE INVOLVED IN THE TRANSCRIPTION PROCESS"

Policy Statement

In conducting the operations of the Seyyone, Seyyone will manage protected health information ("PHP) in a manner that prevents unnecessary or inadvertent access to, use of or disclosure of PHI.

Seyyone may disclose to a member of its workforce, or other related individual, or any other person identified by the management, PHI directly relevant to such person's involvement with the Transcription process or payment related to Transcription

Seyyone may, consistently with the procedures set forth below, also use or disclose PHI to notify, or assist in the process of transcription or another person responsible for the care of the production function related to the operations of the company.

PROCEDURE

As to all PHI received by Seyyone, staff will:

- Identify the source of PHI and identify the employees who may receive it and use it to perform production functions;
- Ensure that the PHI will be stored in a secure environment;
- Not disclose PHI to any individuals not necessary to perform the function for which the PHI was obtained.
- All physical files pertaining to Seyyone operations will be stored in a locked room. Only designated staff will access to this room.
- If physical records containing PHI are to be destroyed, they will be put in a locked bin that is picked up by a designated personnel and shredded/destroyed in a secure manner. Security codes, locks and/or key cards will be changed or re-programmed as necessary when an employee terminates.
- When working on a file that contains PHI, the designated personnel will keep those files secured at all times. If these personnel must leave their office, either at the end of the day orotherwise, the workstation or the system will be locked file must be locked/protected. No files, papers, disks, CD or any other materials containing PHI will be left unsecured at any time.
- Employees with access to files containing EPHI will utilize password protocols that protect the security of data stored on the network. Computers will not display PHI in a manner or at a time when it would allow for the inadvertent disclosure of PHI, and an employee's computer will never display PHI when the employee is not at the computer.
- Fax machines and printers dedicated for use by Seyyone will be located in a secured room accessible only by designated personnel. Printed materials or faxes containing PHI must be physically secured at all times. If copying is required, materials containing PHI must not be left unattended on the copier/printer.

- Any person who erroneously receives a facsimile, e-mail or other correspondence that should have been directed to Seyyone will promptly forward the correspondence to designated personnel without reading it, and without disclosing it to anyone else.
- For each routine function that requires Seyyone to disclose PHI, ensure that the PHI is transmitted securely to only the intended recipient.

Selected Privacy-Related Procedures and Policies

Use of PHI: Never use PHI for any purpose other than what is prescribed by the clients.

Access to the facility: Access into our facility is via locked doors. The access code/key is changed each time an employee leaves the company.

Badges: Employees are required to wear a photo ID badge on the work site.

Office Space: The design of the office space separates visitors from areas of the office where PHI is stored and worked on.

Paper & PHI: All paper that contains PHI is shredded after it is no longer needed for business.

Computer Systems: Computer systems require passwords, updated quarterly. Upon termination, any employee access codes are deactivated. Computer-sharing programs are not permitted.

Internet: Seyyone hosts its own e-mail and FTP servers, and an encrypted VPN.

E-mails sent or received via Seyyone e-mail shall be business-related only. No personal use shall be allowed, or use of personal e-mail accounts while in the office.

PHI Transmission Protocol: All communication of PHI must be logged and approved. Disclaimer statements must accompany all transmissions, and transmission by e-mail must be encrypted.

Termination: Upon termination, employees are to return all confidential information within twenty-four hours. The employee shall also deliver to Seyyone a written statement certifying that all materials have been returned and that PHI has been swept clean from any medium used to store or process PHI (hard drives, CDs, etc.)

a) Confidential: Where the access is restricted to a specific list of people. These could be company plans, secret manufacturing processes, formulas, etc.

b) Company only: Where the access is restricted to internal employees only. These could be customer databases, Transcription procedures, etc.

c) Shared: Where the resources are shared within groups or with people outside of the organization. This could be operational information and contact information like the internal telephone book to be shared with business partners and agents.

d) Unclassified: Where the resources are publicly accessible. For example, the company sales brochure and other publicity material.

Policy Provisions: All networks housing EPHI repositories must be appropriately secured. To ensure that all networks that contain EPHI based systems and applications are appropriately secured, the following policies and procedures must be followed:

1. Networks containing EPHI-based systems and applications must implement perimeter security and access control with a firewall. Firewalls must be configured to support the following minimum requirements:

- Limit network access to only authorized workforce members and entities.
- Limit network access to only legitimate or established connections. An established connection is return traffic in response to an application request submitted from within the secure network.
- Console and other management ports must be appropriately secured or disabled.
- Implement mechanism to log failed access attempts.
- Must be located in a physically secure environment.

2. The configuration of firewalls used to protect networks containing EPHI-based systems and applications must be documented internally by each production Unit. This documentation should include a configuration plan that outlines and explains the firewall rules.

3. The configuration of firewalls used to protect networks containing EPHI-based systems and applications must be submitted to and approved by the HIPAA Security officer

4. This policy includes, but is not limited to, the aforementioned procedures. This policy and its procedures must be reviewed and evaluated on a periodic basis to ensure that they maintain their technical viability and effectiveness.

5. Non-compliance with this policy may result in immediate disciplinary action, up to and including termination of employment and criminal prosecution.

Alternative communication methods for intruder attacks/penetrations:

Firewall intruder-alert detection system

Cell phones

Numeric pager codes

Fax machines

Policy Statement:

Seyyone and its member are committed to conducting business in compliance with all applicable laws, regulations and Seyyone policies. Seyyone has adopted this policy to outline the requirements for transmission of Seyyone EPHI to ensure the security and integrity of such EPHI.

Scope:

The scope of this Policy covers the technical security measures that each function that is a HIPAA covered entity component part will implement to guard against unauthorized access to or modification of EPHI that is being transmitted over an electronic communications network or via any form of removable media.

INTERNET/EMAIL USAGE POLICY

Objectives:

The objectives of this policy are to:

(a) Protect personnel's by informing them of the rights and responsibilities associated with use of intranet, Internet and email services;

(b) Prevent misuse of departmental assets;

(c) Protect the department from legal liability;

(d) Protect intranet, Internet and email services from attacks and outages;

(e) Protect against loss of information;

(f) Ensure capture and retention of corporate electronic records.

Personnel's using Internet/Email will have to strictly follow the under lined guidelines.

1. Not attempting any unauthorized access to information and systems, whether internal or external, including email services **(Yahoo mail, Rediff mail, Hotmail greetings portals e.t.c) and intranet and Internet services or sites.**

2. Using updated anti-virus software for checking malicious virus attacks

3. Maintaining security and confidentiality of user-ids and passwords

4. Don't subscribe or provide the Seyyone emails Id's for mass circulation or tutorials of any kind to avoid junk mails

5. Delete suspected anonymous emails and attachments even without opening them.

6. Strictly not downloading or installing any freeware/software

7. Using chat facility for the said official business only

Email/Internet privilege given to employees for the purposes of accomplishing official business, professional duties including research and, where appropriate, professional development.

TRANSMISSION POLICY

Procedure

1) EPHI Transmissions to Non-Seyyone and other Entities

a) To appropriately guard against unauthorized access to or modification of EPHI that is being transmitted from Seyyone Transcription operations

b) All transmissions of EPIII from the Seyyone networks must utilize an encryption mechanism between the sending and receiving entities or the file, document, or folder containing said EPHI must be encrypted before transmission.

c) Prior to transmitting EPHI from the Seyyone network outside of the any networks the receiving person or entity must be authenticated.

d) All transmissions of EPHI from the Seyyone and network outside of the Seyyone should include only the minimum amount of PHI.

e) For transmission of EPHI from the Seyyone network to outside networks utilizing an email or messaging system.

2) EPHI Transmissions between Seyyone and Other outsource member /partner

a) When transmitting EPHI over an electronic network between Seyyone and outsource member /partner the EPHI must be password protected or encrypted before transmission as described below.

b) All transmissions of EPHI from the Seyyone domain network must utilize an encryption mechanism.

c) All transmissions of EPHI from Seyyone into the Seyyone domain must utilize a mechanism to encrypt or password-protect the EPHI.

d) All transmissions from Seyyone into the Seyyone domain that do not contain EPHI require no additional security mechanisms.

3) EPHI Transmissions Using Electronic Removable Media

a) When transmitting EPHI via removable media, including but not limited to, floppy disks. CD ROM. memory cards, magnetic tape and removable hard drives, the sending party must:

Use an encryption mechanism to protect against unauthorized access or modification

Authenticate the person or entity requesting said EPHI in accordance with HIPAA Security Policy of Seyyone

Send the minimum amount of said EPHI required by the receiving person or entity.

b) If using removable media for the purpose of system backups and disaster recovery and the aforementioned removable media is stored and transported in a secured environment, no additional security mechanisms are required.

4) EPHI Transmissions Using Email or Messaging Systems

a) The transmission of EPHI from Seyyone to a client via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

The client/vendor has been made fully aware of the risks associated with transmitting EPHI via email or messaging systems.

The client/vendor has formally authorized Seyyone to utilize an email or messaging system to transmit EPHI to them.

The client/vendor identity has been authenticated.

The email or message contains no excessive history or attachments.

b) The transmission of EPHI from Seyyone to an outside entity via an email or messaging system is permitted if the sender has ensured that the following conditions are met:

The receiving entity has been authenticated. The receiving entity is aware of the transmission and is ready to receive said transmission.

The sender and receiver are able to implement a compatible encryption mechanism. All attachments containing EPHI are encrypted.

c) The transmission of EPHI within Seyyone via an email or messaging system is permitted without additional security measures or safeguards so long as only a minimal amount of EPHI is being transmitted and the EPHI is not high risk, sensitive or critical. EPHI that is high risk, sensitive or critical should not be sent through clear text email;

Such EPHI should be sent via encrypted. If an email or message includes an attachment that contains EPHI, the attachment must be encrypted or password protected before transmission.

d) Email accounts that are used to send or receive EPHI must not be forwarded to non- Seyyone accounts.

5) Additional Requirements

a) All encryption mechanisms implemented to comply with this policy must support a minimum of, but not limited to, 128-bit encryption.

b) When transmitting EPHI electronically, regardless of the transmission system being used, Workforce members must take reasonable precautions to ensure that the receiving party is who they claim to be and has a legitimate need for the EPHI requested.

c) If the EPHI being transmitted is not to be used for treatment, payment or health care operations, only the minimum required amount of PIII should be transmitted. With reference to Business associate agreement

Protection of External Electronic Communications

Organizations shall encrypt all patient-identifiable information before transmitting it over public networks, such as the Internet.

Policies shall be in place to discourage the inclusion of patient identifiable information in unencrypted e-mail.

Email Retention Policy

The Email Retention Policy is intended to help employees determine what information sent or received by email should be retained and for how long.

The information covered in these guidelines includes, but is not limited to, information that is either stored or shared via electronic mail or instant messaging technologies.

All employees should familiarize themselves with the email retention topic areas prescribed by the HIPAA manual

Policy Statement:

The Organizational Behavior of Seyyone is to cultivate and establish a vision for achieving quality service to the client with trustworthy and confidence practice, which forms as a culture of the organization.

Procedure:

- Security & Confidentiality committees:
- Role of an Information Security Officer
- Training Program for all employees (Including Management)
- Sanctions for violations
- 5 Security remainders and user education
- Expressed Security policies and documentation
- Confidentiality of records
- Personnel Clearance procedures

Security Best Practices:

Attacker awareness (Guidelines)

Warning signs of a possible attacker

- The person refuses to provide a direct call-back phone number.
- Their request is not ordinary.
- They try to claim authority.
- They stress urgency.
- They threat negative consequences if you don't comply.
- They show discomfort when questioned.
- They will often use name-dropping to get what they want.
- They will often compliment, flatter or flirt with you to get what they want.

Electronic storage and transfer of information

1. Always take a '‘default deny5’ stance in providing access to information. Only provide the minimum level of access necessary to meet specific business requirements. For example, if you are storing a file on the network to share with others, only provide write access (the ability to change the file) to those few that have a real business need to change the file. Provide everyone else “read-only” access. Contact your I.T. Help Desk or I.T. Security for assistance.

2. Set up a process to proactively audit who has access to your information. Remove or disable all unused access folders and privileges on a regular basis. Provide only active personnel that have a real business need with access to your information.

   Log and monitor access of sensitive information and notify your management and IT Security of any noticeable misuse.

3. If you have a choice between storing Internal or Confidential information on your local hard drive or a company network drive choose to store your information on the company network drive. Company network drives are more secure and are backed up on a regular basis. If you have no choice but to store Internal or confidential information on your local hard drive make sure to password protect your sensitive files. Also be sure to back up your local hard drive on a regular basis.

Your backup will come in handy if ever your PC is compromised or stolen. Again, contact your IT Help Desk to determine the best tools and method for you.

Policy of Statement:

Seyyone will establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

Scope:

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Seyyone facility, has access to the Seyyone network, or stores any non-public network information.

Policy:

1. Password Creation

- All user-level and system-level passwords must conform to the *Password Construction Guidelines*.
- Users must use a separate, unique password for each of their work related accounts. Users may not use any work related passwords for their own, personal accounts.
- User accounts that have system-level privileges granted through group memberships or programs such as **"sudo"** must have a unique password from all other accounts held by that user to access system-level privileges. In addition, it is highly recommend that some form of multi-factor authentication is used for any privileged accounts

2. Password Creation Guidelines

- Strong passwords are long, the more characters you have the stronger the password. We recommend a minimum of 15 characters in your password. In addition, we highly encourage the use of passphrases, passwords made up of multiple words which includes alphanumeric, capital letters, special characters.

3. Password Change

- Passwords should be changed in periodic intervals.
- Passwords should be changed immediately when there is reason to believe a password has been compromised.
- Password cracking or guessing may be performed on a periodic or random basis by the InfoSec Team or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it to be in compliance with the Password Construction Guidelines.

4. Password Protection

- Passwords must not be shared with anyone, including supervisors and co-workers. All passwords are to be treated as sensitive, confidential Seyyone information.
- Passwords must not be inserted into email messages, Alliance cases or other forms of electronic communication. Must be revealed over telephone or mobile network.
- Do not use the "Remember Password" feature of applications (for example, web browsers).
- Any user suspecting that his/her password may have been compromised must report the incident and change all passwords.

5. Policy Compliance

1. Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, periodic walk-throughs, video monitoring, tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the InfoSec Team in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6. Related Standards, Policies and Process

None

Policy Statement:

Seyyone will prevent & protect all of its assets from external, internal threats, which may include technical and administrative interruptions.

Objective:

- To prevent unauthorized physical access, damage and interference to business premises and information
- To prevent loss, damage or compromise of assets and interruption to business activities
- To prevent compromise or theft of information and information processing facilities.

Procedures:

Control Mechanisms

- All resources which deal with EPHI will be placed in a Secure Strong room which will be under lock and key, access to those facilities should be based on card controlled entity gate, manned reception desk.
- There will be several physical barriers around the business premises, which will be protected thru Locks.
- All external doors of the to the Production area will be protected by alarms, locks & manned security
- Access to sites will be for authorized persons only.
- All employees should be required to wear some form of visible identification (Identity cards).
- Visitors to secure areas should be allowed after entering their date and time of entry and exit in the register provided at the front desk
- Access to sensitive facilities should be controlled and restricted and audit trial to be maintained.
- Key facilities should be cited to avoid access by unauthorized personnel.
- Directories and internal telephone books should not have the numbers of sensitive importance.
- Delivery area should be such that the personnel bringing the supplies do not have access to sensitive areas/production area.

Preventive Power Control Mechanisms

- Multiple feeds of power supply
- UPS
- Backup generator
- Emergency power switches near emergency exits
- Emergency lighting
- Lightning arresters

Security Methods & Practices:

- All power and telecomm lines should be adequately protected.
- Networking cabling should be suitably protected.
- Power cabling should be segregated from communication lines.
- Alternative routing for transmission media.
- Locked box for hubs and switches.
- Sensitive or critical business information should be locked in fire resistant safe or cabinet.
- Periodic maintenance of equipment's and records for the same while sending out.
- Insurance cover for all equipment's while inside premises and while sending out Manufacturer's instructions for protecting equipment's should be observed at all times.
- Paper and computer media to be stored in suitable locked cabinets.
- Pc's and workstations should not be left logged on when unattended and should be protected by key locks, and passwords or other controls.
- Photocopiers, fax machines to be locked after office hours.
- Sensitive or classified information, when printed should be cleared from printers immediately.
- Equipment, information, software should not be taken out without authorization and the same should be logged out and logged back in when returned.

Physical Personnel Security:

Controls:

- Job description should have Information System security as a part.
- Character checks during recruitment.
- Check for the completeness of CV of the candidate.
- Independent identity check.
- In case of access to sensitive areas and information, routine credit check are a must for those staff having access.
- Similar screening process for outside vendors and temporary staffs.
- Supervision requirement of new and inexperienced staff.
- Knowledge of staff personal circumstances.
- Confidentiality agreements or Non-disclosure agreements for employees
- Procedure for reporting security incident as quickly as possible should be in place
- Computer/software which malfunctions should be isolated immediately
- Users should not be allowed to remove any software that malfunctions. It should be handled by designates person only.
- Formal disciplinary process for employees who have violated the organizational security policies and process should be available.
- Employee's legal responsibilities and right regarding HIPAA, should be clarified and included in the terms and conditions of employment.

OPERATIONAL SECURITY (Protected Resources 1)

- Password files
- Application program libraries
- Source code
- Vendor software
  - Operating System
    - Libraries
    - Utilities
    - Directories
    - Address Tables
  - Proprietary packages
- Communications HW/SW
- Main storage
- Disk & tape storage

Protected Resources (2)

- Processing equipment
- Stand-alone computers
- Printers
- Sensitive/Critical data
  - Files
  - Programs
- System utilities
- System logs/audit trails
  - Violation reports
- Backup files
- Sensitive forms
- Printouts
- People

General Guidelines:

- Shoulder surfing over Operator's shoulder
- Physical access to printouts - rerouting
- Access control to print queues
- Access control to printers

Layered Defense

- Protection of printouts
- Heading/Trailing banners with recipient name and location
- Print "No Output" when report is empty
- Positive identification and logging of printouts
- Sign for receipt of sensitive printouts
- Protection of print queues
- Audit of facility and processes

Policy Statement:

Policy is established for those qualified personnel and ensure their background security check for trust worthiness & comply with procedures of the company.

Procedures:

Background checks/security clearances

1. Checking public records provide critical information needed to make the best hiring decision.

2. The following checks shall be carried out as background checks

- Credit Report
- Education Verification & Credential Confirmation
- Reference Checks
- Prior Employer Verification

3. Hiring & termination* Policies and procedures from HR which includes

- how to handle employee's departure
- shutting down accounts
- forwarding e-mail and voice-mail
- Lock and combination changes -system password changes

Employees

Seyyone Transcriptions employees go through extensive security and background checks prior to employment. As part of their employment contract, employees are required to sign the following agreements:

- Non-Disclosure
- Confidentiality of information
- Consent to conduct background investigation ^ Covenant not to solicit
- Implementation of both criminal and civil actions if they have breached on security and confidentiality

Upon hiring, company employees are thoroughly trained and tested on all aspects of HIPAA compliance and security issues. Training is conducted regularly to stay abreast of industry events and new policies that will further strengthen HIPAA compliance within Seyyone Day Transcriptions operations.

Forms & Check List

Employee Clearance form, Non-Disclosure Agreement & Privilege requisition form.

Purpose:

This document describes a required minimal security configuration for all routers and switches connecting to a production network or used in a production capacity on behalf of Seyyone.

Scope:

All routers and switches connected to Seyyone production networks are configured.

Policy:

Every router must meet the following configuration standards:

- No local user accounts are configured on the router. Routers and switches must use TACACS+ for all user authentications.
- The enable password on the router or switch must be kept in a secure encrypted form. The router or switch must have enable password set to the current production router/switch password from the device's support organization.
- The following services or features must be disabled:
    - IP directed broadcasts
    - Incoming packets at the router/switch sourced with invalid addresses such as RFC1918 addresses
    - TCP small services
    - UDP small services
    - All source routing and switching
    - All web services running on router
    - Seyyone discovery protocol on Internet connected interfaces
    - Telnet, FTP, and HTTP services
    - Auto-configuration
- The following services should be disabled unless a business justification is provided:
    - Dynamic trunking
    - Scripting environments, such as the TCL shell
- The following services must be configured:
    - Password-encryption
    - NTP configured to a corporate standard source

- All routing updates shall be done using secure routing updates.
- Use corporate standardized SNMP community strings. Default strings, such as public or private must be removed. SNMP must be configured to use the most secure version of the protocol allowed for by the combination of the device and management systems.
- Access control lists must be used to limit the source and type of traffic that can terminate on the device itself.
- Access control lists for transiting the device are to be added as business needs arise.
- The router must be included in the corporate enterprise management system with a designated point of contact.
- Each router must have the following statement presented for all forms of login whether remote or local:

"UNAUTHORIZED ACCESS TO THIS NETWORK DEVICE IS PROHIBITED. *You must have explicit permission to access or configure this device. All activities performed on this device may be logged, and violations of this policy may result in disciplinary action, and may be reported to law enforcement. There is no right to privacy on this device. Use of this system shall constitute consent to monitoring."*

- Telnet may never be used across any network to manage a router, unless there is a secure tunnel protecting the entire communication path. SSH version 2 is the preferred management protocol.
- Dynamic routing protocols must use authentication in routing updates sent to neighbor's. Password hashing for the authentication string must be enabled when supported.
- The corporate router configuration standard will define the category of sensitive routing and switching devices, and require additional services or configuration on sensitive devices including:
    - IP access list accounting
    - Device logging
    - Incoming packets at the router sourced with invalid addresses, such as RFC1918 addresses, or those that could be used to spoof network traffic shall be dropped
    - Router console and modem access must be restricted by additional security controls

Policy Compliance:

1. Compliance Measurement

The InfoSec team will verify compliance to this policythrough various methods, including but not limited to, periodic walk-through, video monitoring, business tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the InfoSec Team in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Process

None

Purpose:

The purpose of this policy is to establish the requirement that all projects supported by Seyyone develop and maintain a security response plan. This ensures that security incident management team has all the necessary information to formulate a successful response should a specific security incident occur.

Scope:

This policy applies to any established and defined project or entity within Seyyone.

Policy:

The development, implementation, and execution of a Security Response Plan (SRP) are the primary responsibility of the specific project for whom the SRP is being developed in cooperation with the InfoSec Team. Projects are expected to properly facilitate the SRP for applicable to the service or products they are held accountable.

1. Service or Product Description

The product description in an SRP must clearly define the service or application to be deployed with additional attention to PHI, data flows, logical diagrams, architecture considered highly useful.

2. Contact Information

The SRP must include contact information for dedicated team members to be available during non-business hours should an incident occur and escalation be required. This may be a 24/7 requirement depending on the defined business value of the service or product, coupled with the impact to customer. The SRP document must include all phone numbers and email addresses for the dedicated team member(s).

3. Triage

The SRP must define triage steps to be coordinated with the security incident management team in a cooperative manner with the intended goal of swift security vulnerability mitigation. This step typically includes validating the reported vulnerability or compromise.

4. Identified Mitigations and Testing

The SRP must include a defined process for identifying and testing mitigations prior to deployment. These details should include both short-term mitigations as well as the remediation process.

5. Mitigation and Remediation Timelines

The SRP must include levels of response to identified vulnerabilities that define the expected timelines for repair based on severity and impact to consumer, brand, and company. These response guidelines should be carefully mapped to level of severity determined for the reported vulnerability.

Policy Compliance

1. Compliance Measurement

Each business unit must be able to demonstrate they have a written SRP in place, and should be reviewed annually.

2. Exceptions

Any exception to this policy must be approved by the InfoSec Team in advance and have a written record.

3. Non-Compliance

Any business unit found to have violated (no SRP developed prior to service or product deployment) this policy may be subject to delays in service or product release until such a time as the SRP is developed and approved. Responsible parties may be subject to disciplinary action, up to and including termination of employment, should a security incident occur in the absence of an SRP.

Related Standards, Policies and Processes

None

Purpose:

The purpose of this policy is to establish standards for the base configuration of internal server that is owned by Seyyone. Effective implementation of this policy will minimize unauthorized access to Seyyone proprietary information and technology.

Scope:

This policy applies to all Seyyone employees, contractors, consultants, who work for Seyyone in provisioning and maintaining server.

Policy:

1. General Requirements

All servers deployed at Seyyone must be owned by an operations group that is responsible for system administration. Approved server configuration guides must be established and maintained as approved by InfoSec. Operational groups should monitor configuration compliance and implement an exception policy tailored to their environment. The following items must be met:

- Servers must be registered within the corporate enterprise management system. At a minimum, the following information is required to positively identify the point of contact:
    - Server contact(s) and location, and a backup contact
    - Hardware and Operating System/Version
    - Main functions and applications, if applicable
- Information in the corporate enterprise management system must be kept up-to-date.
- Configuration changes for production servers must follow the appropriate change management procedures
- For security, compliance, and maintenance purposes, authorized personnel may monitor and audit equipment, systems, processes, and network traffic per the *Policy*.

2. Configuration Requirements

- Operating System configuration should be in accordance with approved InfoSec guidelines.
- Services and applications that will not be used must be disabled where practical.
- Access to services should be logged and/or protected through access-control methods such as a web application firewall, if possible.
- The most recent security patches must be installed on the system as soon as practical, the only exception being when immediate application would interfere with business requirements.
- Trust relationships between systems are a security risk, and their use should be avoided. Do not use a trust relationship when some other method of communication is sufficient.
- Always use standard security principles of least required access to perform a function. Do not use root when a non-privileged account will do.
- If a methodology for secure channel connection is available (i.e., technically feasible), privileged access must be performed over secure channels, (e.g., encrypted network connections using SSH or IPsec).
- Servers should be physically located in an access-controlled environment, with access keys being held only by IT admin, Operations Manager, Managing Director and Night Shift Operations lead.
- Servers are specifically prohibited from operating from uncontrolled cubicle areas.

3. Monitoring

All security-related events on critical or sensitive systems must be logged and audit trails saved as follows:

- All security related logs will be kept online for a minimum of 1 week.
- Security-related events will be reported to InfoSec, who will review logs and report incidents to IT management. Corrective measures will be prescribed as needed. Security-related events include, but are not limited to:
    - Port-scan attacks
    - Evidence of unauthorized access to privileged accounts
    - Anomalous occurrences that are not related to specific applications on the host.

Policy Compliance

1. Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the InfoSec Team in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None

Policy Statement:
Seyyone will use the Software at a minimum required level, with the objective of attaining quality, efficient & economic transcription service.

Scope:

The scope of the policy applies to all software installed and used by various departments in Seyyone premises

Procedure:

1. **Virus Checking of All Files;**

   All personnel of Seyyone will scan all files, which contain EPHI, for virus. It forms as a practice as a whole for the enterprise.

2. **Virus Checking of Electronic Mail**

   All incoming and outgoing mails will be scanned for Virus and certified a virus Free Electronic Transmission

3. **Control/Restrict User Software**

   A user will be provided only with the required software, which shall be needed to accomplish the said purpose of the user based on the Role and responsibility.

4. **Control/PC Software Loading**

   Users are restricted not to install or un-install software on their own, only the permissible software will be loaded on their PC

5. **Periodic User training on required procedures**

   Periodic awareness and user training will be provided to all members of Seyyone to accomplish the said business objective.

6. Policies and Procedures strictly enforced (Even Fines)

With reference to the HIPAA Compliance Sec Enforcement & Grievance Policy of Seyyone, all personnel will be enforced to comply with the expressed policies and procedure, any non-compliance will be escalated to the appropriate channel, which may result in imposing sanctions and fines (Non-compliance may even lead to termination of the employee).

Forms & Checklist (Refer Annexure)

Access Monitoring control form

Purpose:

The purpose of this policy is to outline the requirements around installation of software in Seyyone's computing devices. To minimize the risk of loss of program functionality, the exposure of sensitive information contained within Seyyone's computing network, the risk of introducing malware, and the legal exposure of running unlicensed software.

Scope:

This policy applies to all Seyyone employees, contractors, vendors and agents with a Seyyone owned devices. This policy covers all computers, servers, smartphones, tablets and other computing devices operating within Seyyone.

Policy:

- Only authorized IT admin team will be able to install any software on Seyyone's computing devices operated within the Seyyone network, with password protected access to installation. No unauthorized employee will be able to install any software.

- Software requests must first be approved by the requester's manager and then be made to the IT admin team in email.

- The IT admin team will obtain and track the licenses, test new software for conflict and compatibility, and perform the installation.

- The version upgrade for server/ workstation operating system and application software will be evaluated by IT admin team and they own the rollout.

- Patching of all software and operation system is the responsibility of IT admin team.

Policy Compliance

1. Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the InfoSec Team in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None

Purpose:

The purpose of this policy it to define the guidelines for the disposal of technology equipment and components owned by Seyyone.

Scope:

This policy applies to any computer/technology equipment or peripheral devices that are no longer needed within Seyyone including, but not limited to the following: personal computers, servers, hard drives, laptops, smart phones, or handheld computers (i.e., Windows Mobile, iOS or Android-based devices), peripherals (i.e., keyboards, mice, speakers), printers, scanners, compact discs, portable storage devices (i.e., USB drives) and printed materials.

All Seyyone employees and affiliates must comply with this policy.

Policy:

- When Technology assets have reached the end of their useful life they should be sent to the Equipment Disposal Team for proper disposal.
- The Equipment Disposal Team will securely erase all storage mediums in accordance with current industry best practices.
- All data including, all files and licensed software shall be removed from equipment using disk sanitizing software that cleans the media overwriting each and every disk sector of the machine with zero-filled blocks.
- No computer or technology equipment may be sold to any individual.
- No computer equipment should be disposed of via skips, dumps, landfill etc.
- The Equipment Disposal Team will properly remove all data prior to final disposal.
- Hard drives may also be removed and rendered unreadable (drilling, crushing or other demolition methods).
- Computer Equipment refers to desktop, laptop, tablet or netbook computers, printers, copiers, monitors, servers, handheld devices, telephones, cell phones, disc drives or any storage device, network switches, routers, wireless access points, batteries, etc.
- Technology equipment with non-functioning memory or storage technology will have the memory or storage device removed and it will be physically destroyed.

Policy Compliance

1. Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the InfoSec Team in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None

Policy

Seyyone HIPAA team provides privacy training for all employees who perform Transcription functions/activities and who have contact with Protected Health Information ("PHI").

Procedure

- All current employees who perform Transcription functions/activities will receive training regarding the requirements of the HIPAA Privacy Rule.
- All new employees who perform Transcription functions/activities receive privacy training as part of their initial induction training.
- All employees who perform Transcription functions/activities and who change positions/designations will receive new privacy training as appropriate at the time of the change.
- All affected members of the Seyyone workforce receive retraining within a reasonable time if Seyyone materially changes any privacy policy or procedure.
- The Privacy Official according to the requirements of the Privacy Rule maintains documentation of privacy training.

Procedures:

l. Security Awareness and Training Standard

The Security Awareness and Training standard adopted by Seyyone implements security awareness and training program for all members of workforce, including management.

2. Security Reminders

Implementation specifications: Seyyone implements periodic security updates.

3. Protection from Malicious Software

Implementation specifications: Seyyone provides training on guarding against, detecting and reporting malicious software.

4. Log-in Monitoring

Implementation specifications: Seyyone provides training on monitoring login attempts and reporting discrepancies.

5. Password Management

Implementation specifications: Seyyone provides training on procedures for creating, changing, and safeguarding passwords.

6. 1nduction Training:

Seyyone provides initial training to all of our employees that have access to electronic protected health information (PHI) prior to the compliance date, and to new employees upon hire after the compliance date, This requirement applies even to part-time or individuals who may be on site for a limited time period.

7. Response and Reporting:

Implementation specifications: Seyyone establishes policies and procedures to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the workforce; and security incidents and their outcomes are documented.

Forms & Checklist (Refer Annexure)

Training Schedule

Training Attendance sheet

Policy Statement:

In order to increase the security posture of Seyyone and mitigate the threat of security related vulnerabilities Seyyone would conduct periodic Vulnerability Assessments.

Scope:

Vulnerability Assessments will assist in the discovery of security vulnerabilities, determine the threat of these vulnerabilities, and assist in decreasing the risk of these security vulnerabilities.

Procedures

Network Vulnerability Assessment:

Network based Vulnerability Assessments will be conducted from inside Seyyone trusted networks and from Seyyone De-Militarized Zones (DMZs.)

Technical Assessment:

Seyyone systems should be assessed for technical vulnerabilities such as unused services, software vulnerabilities, access requirements, and compliance with formulated security standards.

Administrative Control Assessment:

Vulnerability Assessments should be conducted on administrative controls such as documentation, process, procedure and operations.

Schedule:

Vulnerability Assessments would be conducted on a periodic schedule as warranted by the confidentiality, integrity, and availability of information and assets in each section.

Compliance:

Steps required to remediate security risks discovered in the Vulnerability Assessment will be monitored for compliance.

Service Disruption:

During the normal course of Vulnerability Assessments critical network and administrative services should not be interrupted, however a minimal amount of disruptions may occur.

Purpose:

The purpose of this policy is to provide guidance for Seyyone workstation security to protect the information received, processed and stored. Additionally, the policy provides guidance to ensure the requirements of the HIPAA Security Rule "Workstation Security" Standard 164.310(c) are met.

Scope:

This policy applies to all Seyyone employees, contractors, consultants, vendors and agents with a Seyyone owned workstation connected to the Seyyone network.

Policy:

Appropriate measures must be taken when using workstations to ensure the confidentiality, integrity and availability of sensitive information, including protected health information (PHI) and that access to sensitive information is restricted to authorized users.

- Employees using workstations shall consider the sensitivity of the information, including protected health information (PHI) that may be accessed and prevent the possibility of unauthorized access.

- Seyyone will implement physical and technical safeguards for all workstations that access electronic protected health information to restrict access to authorized users.

Appropriate measures include:

- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or logout) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screen saver with a short timeout period to ensure that workstations that were left unsecured will be protected. The password must comply with Seyyone *Password Policy*.
- Complying with all applicable password policies and procedures. See Seyyone *Password Policy*.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unauthorized software on workstations.

- Storing all sensitive information, including protected health information (PHI) on network servers
- Keeping food and drink away from workstations in order to avoid accidental spills.
- Securing laptops that contain sensitive information by using cable locks or locking laptops up in drawers or cabinets.
- Installing privacy screen filters or using other physical barriers to alleviate exposing data.
- Ensuring workstations are left on but logged off in order to facilitate after-hours updates.
- Exit running applications and close open documents
- Ensuring that all workstations use a UPS (battery backup).

Policy Compliance

1. Compliance Measurement

The InfoSec team will verify compliance to this policy through various methods, including but not limited to, tool reports, internal and external audits, and feedback to the policy owner.

2. Exceptions

Any exception to the policy must be approved by the InfoSec Team in advance.

3. Non-Compliance

An employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Related Standards, Policies and Processes

None

Purpose

This policy prohibits access to Seyyone networks via unsecured wireless communication mechanisms. Only wireless systems that meet the criteria of this policy or which exceeds HIPAA regulation have been approved for connectivity to Seyyone networks.

Scope

This policy covers all wireless data communication devices (e.g., personal computers, cellular phones, PDAs, etc.) connected or operated to any of Seyyone internal networks and premises. This includes any form of wireless communication device capable of transmitting packet data. Wireless devices and/or networks without any connectivity to Seyyone networks do not fall under the purview of this policy.

Register Access Points and Cards

All wireless Access Points / Base Stations connected to the corporate network must be registered and approved by IT Dept. These Access Points / Base Stations are subject to periodic penetration tests and audits. All wireless Network Interface Cards (i.e., PC cards) used in corporate laptop or desktop computers will be documented and monitored

Approved Technology

All wireless LAN access must use corporate-approved vendor products and security configurations.

VPN Encryption and Authentication

All computers with wireless LAN devices must utilize a corporate-approved Virtual Private Network (VPN) configured to drop all unauthenticated and unencrypted traffic. To comply with this policy, wireless implementations must maintain point-to-point hardware encryption of at least 56 bits. All implementations must support a hardware address that can be registered and tracked, i.e., a MAC address. All implementations must support and employ strong user authentication which checks against an external database such as TACACS+, RADIUS or something similar.

Setting the SSID

The SSID shall be configured so that it does not contain any identifying information about the organization, such as the company name, division title, employee name, or product identifier.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Definitions

Terms	Definitions
User Authentication	A method by which the user of a wireless system can be verified as a legitimate user independent of the computer or operating system being used.

1. Dr. C.Ravi, Managing Director
2. Dr. K.Sabapathy, President
3. Mr. K.Ramachandran, Operations Manager
4. Mr. Hari Krishnan V, HIPAA Compliance Officer
5. Mr. Jagadeesh, IT Administrator.