triyam
Data Management
Solutions for Healthcare

Information Security Policy

Version 3.0

Adapted from:

Health Information Technology Research Center (HITRC)
Privacy & Security Community of Company (Toolkit Workgroup)
The National Learning Consortium (NLC)

Last Revision Date
12/01/2023

Document Owner
Sudhakar Mohanraj

Review frequency
Half-Yearly

Document History

Version	Modified date	Modified by	Brief Description of Modification
1.0	01/30/2018	EHR2.0	Initial document
1.1	06/26/2018	N.R.Lakshmi Devi	Implementation details
1.2	07/02/2018	N.R.Lakshmi Devi	Corrections based on feedback from Pandimani
1.3	08/29/2018	Harish	Corrections based on Sudhakar's comments
1.4	09/08/2018	Harish	Corrections based on Sudhakar's comments(from page 15 to 25)
1.5	09/12/2018	Harish/Lakshmi	Corrections based on Sudhakar's comments(from page 15 to 25)
1.6	11/13/2018	Harish/Lakshmi	Updated page 25 to 35
1.7	11/21/2018	Harish/Lakshmi	Reviewed all pages again and made the required corrections
1.8	02/14/2019	Harish/Lakshmi	Corrections based on review comments from Palaniappan V
1.9	03/07/2019	Harish/Lakshmi	Modifications based on the review comments by Palaniappan V
2.0	03/13/2019	Harish/Lakshmi	Modifications based on the review comments by Palaniappan V
2.1	03/27/2019	Harish/Lakshmi	Modifications based on tasks created in Teamwork
2.2	04/06/2019	Harish/Lakshmi	Modifications based on the review tasks created in Teamwork
2.3	04/16/2019	Lakshmi	Addition of the data classification section and portal for Data Breach recording
2.4	08/28/2019	Lakshmi	Modifications based on review Comments
2.5	09/25/2019	Lakshmi	This version with the changes done so far was uploaded to confluence
2.6	11/13/2019	Shashi/Lakshmi	CST Team changed; other changes as applicable to current context
2.7	02/07/2020	Harish/Prem	

2.8	11/30/2021	Sujatha/Sandilyan/Ravi	CST Team changed, Configuration Management Section introduced; other changes as applicable to current context
2.9	01/04/2023	Sujatha/Sandilyan/Ravi	CST Team composition changed in line with new Organization structure, Patch Management and Vendor Management Sections introduced
3.0	12/01/2023	Sujatha/Sandilyan/Ravi	1. Chief Security and Privacy Officer changed from Veera Palaniappan to Sudhakar Mohanraj. 2. Document owner name also changed inline and frequency of review changed from yearly to half-yearly. CST org structure revisited. 3. Antivirus software changed from F-Secure to Seqrite. 4. Updated use of KnowBe4 for phishing simulation and security training 5. Introduced exclusive section for Vulnerability Management and Incident Management 6. G-Suite replaced with Google Workspace 7. Disposal of paper and / or external media – shredding policy updated 8. Migrated the policy to Triyam's new rebranded Word template

Instructions

The Information Security Policy should be distributed to all staff members and enforced as stated. It may be necessary to make changes as necessary based on the needs of our environment as well as other federal and state regulatory requirements.

Table of Contents

1 Introduction

1.1 PURPOSE

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

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

1.2 SCOPE

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

1.3 ACRONYMS / DEFINITIONS

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

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

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

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

CST – Confidentiality and Security Team

DoD – Department of Defense

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

External Media –i.e. CD-ROMs, DVDs, floppy disks, flash drives, USB/thumb drives, tapes

Firewall – a dedicated piece of hardware or software running on a computer which allows or denies traffic passing through it, based on a set of rules.

FTP / SFTP – File Transfer Protocol / Secured File Transfer Protocol

HIPAA - Health Insurance Portability and Accountability Act

IT - Information Technology

LAN – Local Area Network – a computer network that covers a small geographic area, i.e. a group of buildings, an office.

SOW - Statement of Work - An agreement between two or more parties that details the working relationship between the parties and lists a body of work to be completed.

User - Any person authorized to access an information resource.

Privileged Users – system administrators and others specifically identified and authorized by Company management.

PHI – Protected Health Information

PII – Personal Identifiable Information

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

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

VLAN – Virtual Local Area Network – A logical network, typically created within a network device, usually used to segment network traffic for administrative, performance and/or security purposes.

VPN – Virtual Private Network – Provides a secure passage through the public Internet.

Vault – to securely store credentials to key assets

Virus - a software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the computer it attacks. A true virus cannot spread to another computer without human assistance.

1.4 APPLICABLE STATUTES / REGULATIONS

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

Center for Medicaid and Medicare (CMS) - https://www.cms.gov/

Health and Human Services (HHS) - https://www.hhs.gov/

Office for Civil Rights - https://www.hhs.gov/ocr/index.html

State Department of Health and Human Services - https://healthfinder.gov/FindServices/SearchContext.aspx?show=1&topic=820

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

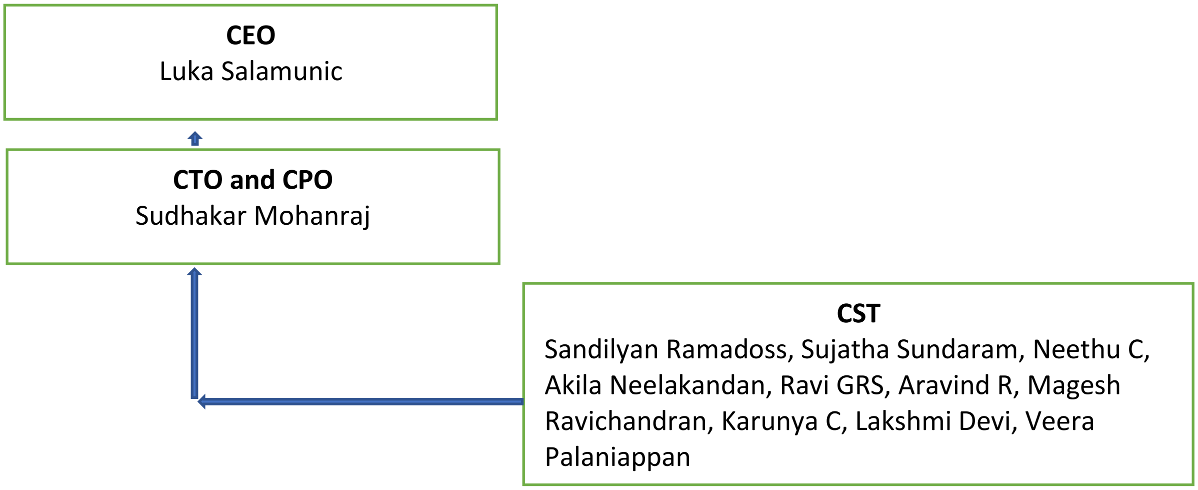
1.5 SECURITY AND PRIVACY OFFICER

The Practice has established a Security and Privacy Officer as required by HIPAA. This Chief Security and Privacy Officer (CPO) will oversee all ongoing activities related to the development, implementation, and maintenance of the information security and Practice privacy policies in accordance with applicable federal and state laws. CPO will serve as security point of contact for any questions, escalations, or incidents.

The current Security and Privacy Officer (CPO) for the Practice is: **Sudhakar Mohanraj**

1.6 CONFIDENTIALITY & SECURITY TEAM (CST)

The Company has established a Confidentiality & Security Team made up of key personnel whose responsibility is to identify areas of concern within the Company and act as the first line of defense in enhancing the appropriate security posture. All members identified within this policy are assigned to their positions by the CEO.



CEO
Luka Salamunic

CTO and CPO
Sudhakar Mohanraj

CST
Sandilyan Ramadoss, Sujatha Sundaram, Neethu C, Akila Neelakandan, Ravi GRS, Aravind R, Magesh Ravichandran, Karunya C, Lakshmi Devi, Veera Palaniappan

CO – The Confidentiality Officer is Sudhakar Mohanraj. This role is responsible for annual security training of all staff on confidentiality issues.

CPO – The Chief Security and Privacy Officer is Sudhakar Mohanraj. This role is responsible for making sure that the policies and procedures are modified as needed from time to time and HIPAA privacy compliance issues brought in by the CST team or other members are escalated to the CEO and remedial actions taken and informed to all the employees of Triyam.

CST – Confidentiality and Security Team

The CST team will perform regular periodic audits of tasks defined, report gaps and provide recommendations. CST will also perform surprise audits to cover specific areas as determined appropriate, from time to time.

The CST will meet quarterly at a minimum to discuss security issues and to review concerns and audit gaps that arose/were reported during the quarter. The CST will identify areas that should be addressed during monthly training and review/update security policies as necessary.

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

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

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

1.7 DEFINITION OF PROTECTED HEALTH INFORMATION (PHI)

Any information about health status, provision of health care, or payment for health care that can be linked to a specific individual qualifies as PHI. There is a set of 18 PHI Identifiers which, if included in a record, require the record to be protected under HIPAA rules

PHI identifiers include:

- Names
- Addresses
- Geographic subdivisions smaller than a state
- All elements of dates directly related to the individual (Dates of birth, marriage, death, etc.)
- Telephone numbers
- Facsimile numbers
- Driver's license numbers
- Electronic mail addresses
- Social security numbers

- Medical record numbers
- Health plan beneficiary numbers
- Account numbers, certificate/license numbers
- Vehicle identifiers and serial numbers
- Device identifiers and serial numbers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers
- Full face photographic images and any comparable images

Example: A medical record, laboratory report, or a hospital bill are considered PHI because they contain one or more of these identifiers along with health information

1.8 DATA CLASSIFICATION

Data classification, in the context of information security, is the classification of data based on its level of sensitivity and the impact to the organization should that data be disclosed, altered or destroyed without authorization. The classification of data helps determine what baseline security controls are appropriate for safeguarding that data. All organizational data should be classified into one of three sensitivity levels, or classifications:

A. Restricted Data

Data should be classified as Restricted when the unauthorized disclosure, alteration or destruction of that data could cause a significant level of risk to the organization or its customers. Examples of Restricted data include data protected by state or federal privacy regulations and data protected by confidentiality agreements.The highest level of security controls should be applied to Restricted data.

B. Private Data

Data should be classified as Private when the unauthorized disclosure, alteration or destruction of that data could result in a moderate level of risk to the organization or its customers. By default, all organizational data that is not explicitly classified as Restricted or Public data should be treated as Private data. A reasonable level of security controls should be applied to Private data.

C. Public Data

Data should be classified as Public when the unauthorized disclosure, alteration or destruction of that data would results in little or no risk to the organization and its customers. Examples of Public data include press releases, product demo and research publications. While little or no controls are required to protect the confidentiality of public data, some level of control is required to prevent unauthorized modification or destruction of public data.

2 Employee Responsibilities

2.1 PHYSICAL SECURITY IN ACCORDANCE WITH COMPANY POLICIES :

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

2.1.1 Wear Identifying badge such that it is easily visible to others :

In order to help maintain building security, all employees should prominently display their employee identification badge. Visitors are not permitted to enter inside the production area. Where applicable, vendors have signed in Non Disclosure Agreement and/or BAA. On a rare occasion of entry of an occasional vendor is required then he is always accompanied by a Triyam employee to make sure we avoid breach of PHI

Following page in Confluence has the implementation details:

Details of Employees/Vendors NDA and BAA agreement is documented here	https://triyam.atlassian.net/wiki/spaces/FOV/pages/955940868/Employees+Vendor+of+Triyam+NDA+and+BAA+Agreement

2.1.2 Challenge Unrecognized Personnel :

It is the responsibility of all Company personnel to take positive action to provide physical security. Any unrecognized person in a restricted company office location, should be challenged as to their right to be there in that location. Any person who does not respond appropriately should be immediately reported to supervisory staff. Visitors are strictly prohibited inside the production area.

2.1.3 Unattended Computers:

Unattended computers and ePHI applications should be locked by the user when leaving the work area. This feature is discussed with all employees during the employee induction training . Company policy states that all computers will have the automatic screen lock or sign-off function set to automatically activate upon not more than ten (10) minutes of inactivity. Overriding this setting is not possible by employee as it requires system administrator privileges and this is controlled by the CST team.

Following page in Confluence has the implementation details:

Process of locking the screen in the system is documented here	https://triyam.atlassian.net/wiki/spaces/FOV/pages/695173209/Windows+and+Ubuntu+Screen+Locking

2.1.4 Use of Company Corporate Assets:

Only computer hardware and software owned by and installed by the Company is permitted to be connected to or used on Company equipment. Only software that has been approved for corporate use by the Company is installed on Company equipment. To install or uninstall any software in any system we need administrative privilege which is only with CST. Computers supplied by the Company are to be used solely for business purposes. All employees and contractors must read and understand the list of prohibited activities that are outlined below at the time of induction. Modifications or configuration changes are not permitted on computers. This can be done only by the administrator who belongs to CST.

CST audits master list of assets periodically, including user listing and licensing for software.

Following page in Confluence has the implementation details for all the above sections:

Process for approved hardware and software used by all team members is shown here.	https://triyam.atlassian.net/wiki/spaces/FOV/pages/695173235/Triyam+Asset+List+-+Hardware+and+Software

2.2 RETENTION OF OWNERSHIP:

All software programs and documentation generated or provided by employees, consultants, or contractors for the benefit of the Company are the property of the Company unless covered by a contractual agreement. Nothing contained herein applies to software purchased by Company employees at their own expense, or them using the same to develop software program or documentation through it.

2.2.1 Crashing an information system:

Deliberately crashing an information system is strictly prohibited. Deliberate crash includes – willful crashing the system or an act by user causing a system crash, even unknowingly and a repetition of the same action by that user may still be viewed as a deliberate act.

2.2.2 Attempting to break into an information resource or to bypass a security feature:

Attempting to break into an information resource or to bypass a security feature is strictly prohibited.

Attempt to break information includes all or any of the following:

a. Running password-cracking programs within the network or outside the network including cracking the administration password
b. using or accessing sniffer programs through network devices or otherwise
c. attempting to circumvent file or other resource permissions

d. Introducing, or attempting to introduce, computer viruses, Trojan horses, peer-to-peer (“P2P”) or other malicious code into an information system
e. Including installation or running of any unapproved software program without CST ‘s approval.

2.2.3 Browsing:

The Company has access to patient level health information which is protected by HIPAA regulation. Approval is granted to view the information only on a "need to know" basis. The willful, unauthorized access or inspection of confidential or sensitive information to which any one has not been approved on a "need to know" basis is prohibited. The purposeful attempt to look at or access information to which one has not been granted access by the appropriate approval procedure is strictly prohibited.

2.2.4 Personal or Unauthorized Software:

Use of personal software is prohibited. All software installed on Company computers must be approved by the Company. As a policy only whitelisted software / sites approved by CST will be used within the Company.

2.2.5 Software Use:

Violating or attempting to violate the terms of use or license agreement of any software product used by the Company is strictly prohibited.

2.2.6 System Use:

The system use is strictly for official purpose only. Engaging in any activity for any purpose that is illegal or contrary to the policies, procedures or business interests of the Company is strictly prohibited.

Following page in Confluence has the implementation details:

Process for approved hardware and software used by all team members is shown here.	https://triyam.atlassian.net/wiki/spaces/FOV/pages/695173235/Triyam+Asset+List+-+Hardware+and+Software
Internet access and control is documented here	https://triyam.atlassian.net/wiki/spaces/FOV/pages/743538756/2.4+INTERNET+ACCESS

2.3 ELECTRONIC COMMUNICATION, E-MAIL, INTERNET USAGE

As a productivity enhancement tool, the Company encourages the business use of electronic communications. All electronic communication systems and all messages generated on or handled by Company owned equipment or company owned domain name are considered to be the property of the Company – not the property of individual users. This policy applies to all Company employees and contractors and covers all electronic communications including, but not limited to, telephones, e-mail, voice mail, instant messaging, collaborative tools, Internet, fax, personal computers, and servers.

Company provided resources, such as individual computer workstations or laptops, computer systems, networks, mobile phones, e-mail, and Internet software and services are intended for business purposes only.

Generally, while it is not the policy of the Company to monitor the content of any electronic communication, the Company is responsible for servicing and protecting the Company's equipment, networks, data, and resource availability and therefore may be required to access and/or monitor electronic communications from time to time. Different methods are employed to accomplish these goals including physical analysis and verification of the elelctronic communications from the computers, network locations if any and virtual storage like cloud through firewall reports and Antivirus reports.

Following page in Confluence has the implementation details:

Protection of computers using antivirus is documented here	https://triyam.atlassian.net/wiki/spaces/FOV/pages/742686805/Antivirus+Scan+Report
Internet usage report with firewall restrictions is maintained here	https://triyam.atlassian.net/wiki/spaces/FOV/pages/743506024/Firewall+Report

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

Employee has been instructed during the induction training to structure all electronic communication with recognition of the fact that the content could be monitored, and that any electronic communication could be forwarded, intercepted, printed or stored by others.

2.4 INTERNET ACCESS

INTERNET CONSIDERATIONS

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

Internet access is provided for Company users and allocated primarily to those with business, administrative or contract needs. The Internet access provided by the Company should not be used for any other purpose including entertainment, listening to music, accessing social media websites, viewing the sports highlight of the day, games, movies, etc. Employee is not supposed to use the Internet as a radio or to constantly monitor the weather or stock market results. While seemingly trivial to a single user, the company wide use of these non-business sites consumes a huge amount of Internet bandwidth, which is therefore not available to responsible users.

Users are informed at the time of induction that individual Internet usage is monitored, and no employee is allowed to use excessive amount of time or consume large amounts of bandwidth for personal use and the same will be monitored using the firewall reports.

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

Following page in Confluence has the implementation details:

Process for approved hardware and software used by all team members is shown here.	https://triyam.atlassian.net/wiki/spaces/FOV/pages/695173235/Triyam+Asset+List+-+Hardware+and+Software
Internet access and control is documented here	https://triyam.atlassian.net/wiki/spaces/FOV/pages/743538756/2.4+INTERNET+ACCESS

2.5 SOCIAL MEDIA USAGE

Social media should be used by the Company workforce for business-related purposes subject to the restrictions set forth in this policy and only by employees approved by CST. These restrictions are intended to ensure compliance with legal and regulatory restrictions and privacy and confidentiality agreements. Social media includes items such as blogs, podcasts, discussion forums, chat rooms, micro blogging and social networks. Workforce is expected to adhere to compliance requirements and the Principles of Responsibility when using or participating in social media. All the rules that apply to other communications apply here, specifically: respecting members one another; protecting confidentiality, privacy and security; and safeguarding and proper use of Company assets.

- Workforce should not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to another person or entity when posting to Company hosted sites.
- Company hosted blogs must focus on subjects related to the organization.
- Abide by the law and respect copyright laws.
- Workforce should not post content or conduct any activity that fails to conform to any and all applicable state and federal laws. For Company and Workforce's protection, it is critical that everyone abide by the copyright laws by ensuring that they have permission to use or reproduce any copyrighted text, photos, graphics, video or other material owned by others.
- Obtain pre-approval before setting up Company hosted sites. Workforce must seek approval from their supervisor before setting up a Company hosted blog or other social media site.

- Workforce should not disclose any confidential or proprietary information of or about Company, its affiliates, vendors, or suppliers, including but not limited to business and financial information, represent that they are communicating the views of Company, or do anything that might reasonably create the impression that they are communicating on behalf of or as a representative of Company.

  Social media usage has been restricted at Triyam through the firewall and restrictions on the sites/ip's that can be accessed by the employees.

  Following page in confluence has the implementation details:

Internet usage report with firewall restrictions is maintained here	https://triyam.atlassian.net/wiki/spaces/FOV/pages/743506024/Firewall+Report

2.6 REPORTING SOFTWARE MALFUNCTIONS

Users should inform the appropriate Company personnel when the user's software does not appear to be functioning correctly. The malfunction - whether accidental or deliberate - may pose an information security risk and the employee has been informed during induction on it to take the necessary actions. If the user, or the user's manager or supervisor, suspects a computer virus infection, the Company computer virus policy should be followed, and these steps should be taken immediately by the employees:

- Stop using the computer.
- Remove the computer from network if it is connected.
- Do not carry out any commands, including commands to <Save> data.
- Do not close any of the computer's windows or programs.
- Do not turn off the computer or peripheral devices.
- Inform the appropriate personnel or Company CST team as soon as possible. Write down any unusual behavior of the computer (screen messages, unexpected disk access, unusual responses to commands) and the time when they were first noticed.
- Write down any changes in hardware, software, or software use that preceded the malfunction.
- Do not attempt to remove a suspected virus wait for CST's instructions.

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

2.7 REPORT SECURITY INCIDENTS

It is the responsibility of each employee or contractor to report perceived security incidents on a continuous basis to his / her immediate supervisor or security personnel (CST). A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users need to formally report all security incidents / potential vulnerabilities / violations of the security policy immediately to CST through an email to incident@triyam.com. An incident report ticket is automatically created in the IT Request tracking tool. The ticket is tracked to closure in the tool.

2.8 TRANSFER OF SENSITIVE/CONFIDENTIAL INFORMATION

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

Following page in confluence has the implementation details:

Fovea SQL DB Access Restriction	https://triyam.atlassian.net/wiki/spaces/FOV/pages/777584645/Fovea+SQL+DB+Access+Restriction
Azure settings for Fovea	https://triyam.atlassian.net/wiki/spaces/FOV/pages/996737025/Azure+settings+for+Fovea
Usage of G drive for communicating data	https://triyam.atlassian.net/wiki/spaces/FOV/pages/979501061/Usage+of+G+drive+for+transmitting+files+that+contains+PHI+data

2.9 SEPARATION OF PERSONAL AND WORK ENVIRONMENT

Personal software shall not be used on Company computers or networks.   Users shall not use Company purchased software on home or on non-Company computers or equipment.

If a tool is required for a project, for testing and research, a request has to be made through email to the concerned Project manager or Program Manager. Subject to approval and verification, the link is enabled through firewall and the tool is downloaded onto a particular machine and tested on a trial basis.

Company proprietary data, including but not limited to patient information, IT Systems information, financial information or human resource data, shall not be placed on any computer that is not the property of the Company. It is crucial to the Company to protect all data and, in order to do that effectively we must control the systems in which it is contained.   In the event that a supervisor or department head receives a request to transfer Company data to a non-Company Computer System, the supervisor or department head should notify the Security and Privacy Officer or appropriate personnel of the intentions and the need for such a transfer of data.

Non-company personal computers are never allowed to be connected to the Triyam network.

2.10 INSTALLATION OF AUTHENTICATION AND ENCRYPTION CERTIFICATES ON THE E-MAIL SYSTEM

e-mail communication is handled via Gmail at Triyam and Google Workspace features have been implemented as listed in section 2.3 above

2.11 USE OF ENCRYPTED E-MAIL

Google Workspace is used to share any PHI data only for internal use by the project teams. External sharing has been disabled in Google Workspace.

External sharing of PHI is done directly on the shared folder on the customer servers, or through Cerebrus sFTP.

Usage of G drive for communicating data	https://triyam.atlassian.net/wiki/spaces/FOV/pages/979501061/Usage+of+G+drive+for+transmitting+files+that+contains+PHI+data

Google Workspace restrictions as mentioned in section 2.3 is applicable based on the organizational units.

2.12 DE-IDENTIFICATION / RE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION (PHI)

As directed by HIPAA, all personal identifying information must be removed from all data that falls within the definition of PHI before it is made available outside of authorized personnel.

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

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

Fovea Access Restriction	https://triyam.atlassian.net/wiki/spaces/FOV/pages/777584645/DE-IDENTIFICATION+RE-IDENTIFICATION+OF+PHI
Google Workspace Policy setup at Triyam	https://triyam.atlassian.net/wiki/spaces/FOV/pages/695435310/G-Suite+Policy+set+up+at+Triyam
Google Workspace Audit Report	https://triyam.atlassian.net/wiki/spaces/FOV/pages/824311809/G-Suite+Audit+Report

3 Identification and Authentication

3.1 USER LOGIN IDS

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

Users shall be responsible for the use and misuse of their individual login ID.

Workstations (Laptops / VMs) are connected to the company network using Azure AD. A unique Azure AD login is configured for each user. Password is set for this login. Subsequently, a login pin is configured. The user will use the login pin every time to log into the workstation and connect to the network.

3.2 PASSWORDS

User Account Passwords

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

The password is set for the first time when the user is configured in Azure AD for a given workstation.

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

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

Change Frequency – Passwords must be changed every 60 days.

Reuse - The previous five passwords cannot be reused for the desktop and laptops. For Fovea the previous 1 passwords cannot be reused by the user.

A four digit numeric PIN is also setup at the time of Azure AD configuration. Users can either login through the Azure AD password or PIN.

The VMs (Virtual Machines) can be accessed only through Triyam's VPN using the Azure AD PIN.

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

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

The password policies have been enforced through Azure AD.

Password details for Fovea and other internal systems used within the company are provided in this Confluence link	https://triyam.atlassian.net/wiki/spaces/FOV/pages/777584652/Password+Policies

Password Manager:

The credentials for logging into Azure AD, Fovea, all other internal systems, VPN and customer systems are to be stored securely in a tool called MyVault.

MyVault is a Triyam hosted Password Manager to help keep users' data safe. It is used to store Triyam users' credentials encrypted and only users can access their data. Access can be shared encrypted with Triyam internal team & users only. It is mandatory for all employees / consultants to use MyVault for storing their credentials. Credentials should not be stored / shared through other medium (like Google Chat, G-Drive, physical notepads, etc).

Features:

1. Client Side Encryption (all browser)
2. Multilayer Transport Encryption (with TLS 1.2)
3. Autofill - (of all login forms)
4. Multifactor Authentication (with support for Yubikey, Duo and Google Authenticator)
5. Password Generator (for random passwords similar)
6. Groups of sharing
7. Secure Notes to store other information
8. Bookmarks of websites and application sites
9. Password Sharing (securely between users)
10. History of secrets (Old versions of secrets (e.g. passwords) are stored and are accessible in the history)

3.3 CONFIDENTIALITY AGREEMENT

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

Temporary workers, consultants and third-party employees are also covered by a confidentiality agreement, unless there is a duly approved exception. Approval records of such exceptions shall be maintained.

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

Confidentiality Agreement	https://triyam.atlassian.net/wiki/spaces/FOV/pages/777682987/Confidentiality+Agreement+-+BAA

3.4 ACCESS CONTROL

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

Section 3.2 list the details of the password policy that has been implemented.

This guideline satisfies the "need to know" requirement of the HIPAA regulation, since the supervisor or department head is the person who most closely recognizes an employee's need to access data. Users may be added to the information system, network, or EHR only upon authorization of the Security and Privacy Officer or appropriate personnel who is responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

Restricted access to Fovea application	https://triyam.atlassian.net/wiki/spaces/FOV/pages/777584645/Fovea+SQL+DB+Access+Restriction
User Access restrictions in Azure	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1216577559/User+access+restrictions+in+Azure

3.5 USER LOGIN ENTITLEMENT REVIEWS

If an employee changes positions at the Company, employee’s new supervisor or department head shall promptly notify the Information Technology (“IT”) Department of the change of roles by indicating through a mail the higher access level required for the new role

The effective date of the position change shall be indicated in the mail. so that the IT Department can ensure that the employee will have appropriate roles, access, and applications for their new job responsibilities.

Appropriate machines with IP addresses pertaining to the organizational unit for the new role is assigned to the employee and access to the appropriate role is given. For example, if a team member is being moved to a Team Lead or a Project Manager role, Wi-fi access, additional access to websites in the laptop is being given accordingly. Similarly access to projects spaces for documents, maintained in a web portal, is granted or denied accordingly. Similarly, an employee is added to the appropriate groups so that email communications are being received for the new role.

For a limited training period, it may be necessary for the employee who is changing positions to maintain their previous access as well as adding the roles and access necessary for their new job responsibilities.

Program manager and CST team makes sure that all team members have appropriate access and software to perform their roles.

3.6 TERMINATION OF USER LOGIN ACCOUNT

Upon exit / termination notification of an employee, employee’s supervisor and HR department head shall promptly notify the IT Department and CST by indicating “Remove Access” to the employee from Azure AD, Confluence, Teamwork, Google Workspace, Virtual machines and Fovea. A detailed Exit Checklist is initiated for the employee to ensure that all the access and privileges held by the employee are thoroughly removed before the relieving order is handed over to the employee.

If employee’s termination is voluntary and employee provides notice, employee’s supervisor or Program manager shall promptly notify the IT Department of employee’s last scheduled workday so that their user account(s) can be configured to expire. The HR department head shall be responsible for ensuring that all keys, ID badges, and other access devices as well as Company equipment and property is returned to the Company prior to employee leaving the Company on their last working day of employment.

An Exit Checklist is maintained and made sure, it is followed by revoking access to email and deleting the user after data has been transferred, revoking access to project documents if any, revoking access to project tasks, and deleting them from appropriate groups used for communication internally.

For the user logins created for the Source Systems in Fovea, we receive mails from the customer when a staff of the facility leaves, and we deactivate that account in Fovea based on this mail. These mails are tracked as tickets using Hubspot. Also on need basis, for specific customers, we review the list of users, and send them the list to make sure that they verify and request for removal of logins of the staff who are no longer with the facility, or any other changes.

4 Network Connectivity

4.1 INBOUND CONNECTIONS

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

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

Access privileges are granted only upon the request of a department head with the submission of the Network Access Form / IT ticket raised in IT ticketing tool and the approval of the Security and Privacy Officer or appropriate personnel.

4.2 OUTBOUND CONNECTIONS

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

We have OutBound Connections in our Company. Employees gain access to Client's machines through Virtual Private Network (VPN). The connections established are done by authentic users. The credentials are made unique and is changed from time to time.

4.3 TELECOMMUNICATION EQUIPMENT

Certain direct link connections may require a dedicated or leased networked connection. These facilities are authorized only by the Security and Privacy Officer or appropriate personnel and ordered by the appropriate personnel.

Web based GotoMeeting software and Google Hangouts are used for the meetings. These are the two mechanisms for telecommunication used at Triyam.

Google Hangouts meetings are used for internal meetings. For meetings with the customer, GotoMeeting is used. Triyam has 2 login ids used by Program, Project managers and Team leads- support@triyam.com and meeting@triyam.com for conducting the remote meetings.

4.4 THIRD PARTY CONNECTIONS

The security of Company systems can be jeopardized from third party locations if security policies and resources are inadequate. When there is a need to connect to a third-party location, full security measures should be in place. These security measures include but are not limited to:

- Risk analysis of the third party connection
- Networking security best Practices, including firewalls and encryption
- Third party contracts

Any third party requirements are taken up only after the BAA agreement is signed and restricted access is provided so that they can access no other information other than the bare minimum required for executing their tasks.

4.5 EMPHASIS ON SECURITY IN THIRD PARTY CONTRACTS

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

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

19 Because annual confidentiality training is required under the HIPAA regulation, a formal procedure should be established to ensure that the training takes place, that there is a method to determine who must take the training, who will administer the training, and the process to determine the content of the training established.

20 A detailed list of the security measures which will be undertaken by all parties to the agreement should be published in advance of the agreement.

Confidentiality Agreement - BAA	https://triyam.atlassian.net/wiki/spaces/FOV/pages/777682987/Confidentiality+Agreement+-+BAA

4.6 FIREWALLS

Configure the firewall to protect against and prevent external attacks; actively manage the rules within firewall settings. A firewall can take the form of a software product or a hardware device. In either case its job is to inspect all traffic passing through (to or from) the internet or a local network and determine, according to pre-established criteria, whether the traffic should be allowed in or out. Approval from the Security and Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to a Company router or firewall.

Firewall has been implemented and appropriate license has been purchased. Restriction policies such as full restriction to social media links, whitelisting of some static IP's that need access to internet sites (such as YouTube), sites for research or knowledge related analysis for a certain period of time and later removing them from the list are done by the network personnel, based on the request from the appropriate Program Managers through email.

Internet Access	https://triyam.atlassian.net/wiki/spaces/FOV/pages/743538756/2.4+INTERNET+ACCESS
Firewall Audit report	https://triyam.atlassian.net/wiki/spaces/FOV/pages/743506024/Firewall+Report

5 Software

5.1 ANTIVIRUS SOFTWARE INSTALLATION

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

Configuration – Seqrite EPS (End Point Security) is the antivirus software currently implemented by the Company. Updates are received directly from Seqrite portal as and when they are available.

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

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

Seqrite is the antivirus installed in all the PC's and the antivirus scan is run periodically every Friday night. Scanned reports (generated by Monday morning) are monitored on a weekly basis and the report is attached to Teamwork for review.

Seqrite Report	https://triyam.teamwork.com/app/tasks/13851691

5.2 NEW SOFTWARE DISTRIBUTION

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

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

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

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

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

All USB devices and CD-ROM drives, have been blocked at Triyam.

The following link has the list of approved assets:

CST approved list of software & tools	https://drive.google.com/drive/folders/1-wAkCjfBLGMs9IPcU-ESRxXCnKIl6oXS?usp=share_link
Process for requesting new software / tool	https://triyam.atlassian.net/wiki/spaces/FOV/pages/695173235/Triyam+Asset+List+-+Hardware+and+Software

For any research related tasks, wherein a team wants to try a new approach or a new tool, these are installed for testing purpose by the administrators (who belong to the CST team).

For these to be installed, the member needs to notify the Program manager/PM of the respective team with a cc to the CST member and this tool shall be installed based on the approval by the Program manager/PM of the team. The administrators before installing shall make sure that the tool is not affected by virus and is safe to be used.

Once these tools are researched and verified and known to be safe, Licensed versions shall be purchased after the approval from CEO and installed in the client machines. In case any such tool needs to be downloaded from the internet/cloud, we request the customer to whitelist the required IP.'s, and then install from the whitelisted IP's.

6 Encryption

6.1 DEFINITION

Encryption is the translation of data into an unreadable format for anyone who doesn't have the correct key. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text*;* encrypted data is referred to as cipher text**.** Encryption software has to be implemented at Triyam.

6.2 ENCRYPTION KEY

An encryption key specifies the particular transformation of data into cipher data, or vice versa during decryption. AES encryption or equivalent at minimum should be used for the encryption algorithm because of its strength and speed. Company protects all encryption keys against loss or modification, also protecting secret and private keys against unauthorized disclosure. Keys are managed securely with audit logging capabilities. Copies of the keys are maintained in a secondary location for retrieval, yet, must not be copied to the same location as encrypted data.

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

The PHI information archived for customers is uploaded onto Fovea and is only visible from the application. Fovea uses asp.net membership provider for passwords hashing in the application.

The data stored in Triyam's product Fovea has the Dynamic Data masking (DDM) feature on DDM limits sensitive data exposure by masking it to non-privileged users.

Prevent unauthorized access to sensitive data by enabling customers to designate how much of the sensitive data to reveal with minimal impact on the application layer.

DDM can be configured on the database to hide sensitive data in the result sets of queries over designated database fields, while the data in the database is not changed.

Re-identification – is possible by accessing the data through the front-end application using Fovea.

The batch status report updates and any other sample reports are transmitted only via Google Workspace accessed through the company e-mail ids.

The report folders are shared only to the required customer via the Shared Drive/folders on the customer server, or through Cerebrus SFTP, where a separate folder is maintained for each customer.

Details of encryption done in Azure is provided in the below link:

Azure settings for Fovea	https://triyam.atlassian.net/wiki/spaces/FOV/pages/996737025/Azure+settings+for+Fovea

Encryption settings in Fovea is audited by the CST team on a periodic basis.

6.3 INSTALLATION OF AUTHENTICATION AND ENCRYPTION CERTIFICATES ON THE E-MAIL SYSTEM

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

Google Workspace is used for mail transmissions.

6.4 USE OF ENCRYPTED E-MAIL

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

Google Workspace is used for mail transmissions.

6.5 FILE TRANSFER PROTOCOL (FTP)

Files to be shared with customer, or files to be sent by customer (in case there is no Shared Drive), are transmitted via Cerberus SFTP (secured FTP)

Any PHI archival related data is uploaded into Fovea directly from the customer’s machines.

6.6 SECURE SOCKET LAYER (SSL) WEB INTERFACE

Any EHR hosted (ASP or Cloud or Software-as-a-Services) system, if applicable, will require access to a secure SSL website. Any such access must be requested using the Network Access Request Form or other methods and have appropriate approval from the supervisor or department head as well as the Security and Privacy Officer or appropriate personnel before any access is granted.

Fovea hosted by Triyam has the SSL implemented and access is restricted to authorized users.

SSL certificate for Fovea live and non-live environments are renewed annually. Evidence is available in Azure and screenshots of this evidence are also maintained in a secure drive for audit purpose. CST team verifies if the annual renewal happens on time.

7 Building and Physical Security

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

There is a security staff who is available during the day and night hours. Entrance to the building during non-working hours is controlled by the security staff.

Employees are given door-access card and can enter the premises only after scanning the access card ,and visitors have to enter their details and state the reason for the visit to the premises.

In order to help maintain building security, all employees should prominently display their employee identification badge.

Security/door access card and identification badge is taken back from employees who are exiting the company. The access is revoked.

The door to the reception area is locked at all times and requires appropriate credentials or escort past the reception or waiting area door(s). If there is a visitor/un-recognised person, reception member checks with the HR manager and gets prior approval before letting them in at the waiting hall.

The reception area is staffed at all times during the working hours of 9:00 am to 6:00 pm.

Any unrecognized person in a restricted office location should be challenged as to their right to be there.

All visitors must sign in at the front desk and be accompanied by a Company staff member. In some situations, non-Company personnel, who have signed the confidentiality agreement, do not need to be accompanied at all times.

Movement of machines from secured area is not allowed and when members need to move machines it can be done only with help from the network engineer. Computer monitors face away from viewing range of unauthorized personnel and gets auto locked after 10 minutes of idle time.

Building has a power backup by means of a generator.

Fire Protection: Use of local building codes will be observed. Manufacturer’s recommendations on the fire protection of individual hardware will be followed.

Fire extinguishers are placed in the building.

The building is equipped with security (CCTV) cameras to record activities in the parking lot, within the area encompassing the front entrance, on the entrance/staircase pathways in all floors, and also in the Food court. All activities in these areas are recorded on a 24 hours-a-day, 365 days per year basis.

8 Telecommuting

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

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

Remote web-based meetings are conducted using Gotomeeting application.

8.1 GENERAL REQUIREMENTS

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

1 **Need to Know:** Telecommuting Users will have the access based on the same 'need to know' principle, as they have when in the office.

2 **Password Use:** The use of a strong password, changed at least every 60 days, is even more critical in the telecommuting environment. Do not share your password or write it down where a family member or visitor can see it.

3 **Training:** Personnel who telecommute must complete the same annual privacy training as all other employees.

4 **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee is assigned.

Employees make sure that only the intended guests join the remote meetings. Normally introductions with the customer help us get this step done. Anyone who is not supposed to be a part of this meeting would be dismissed by the organizer. Passwords are changed once in 60 days for the GoToMeeting IDs. Training is a part of the induction program for all employees and anyone conducting the meeting from Triyam would have the HIPAA training completed.

8.2 EQUIPMENT CONSIDERATIONS

Employees approved for telecommuting must understand that the Company may not provide all equipment necessary to ensure proper protection of information to which the employee has access. However, the following lists define the equipment and environment required:

Company Provided:

Company supplied workstation- PC's and laptops are provided by Triyam

To be taken care by Employee:

Broadband connection

Secure office environment isolated from visitors and family – this is a part of the NDA signed by the employee

8.3 HARDWARE SECURITY PROTECTIONS

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

Client machine access for EHR's are through VPN or Citrix. Firewall restrictions have been made to internally to make sure that no unauthorized site has been accessed. Virus scanner cannot be disabled as the users do not have administrator privilege.

Security Locks: C and D drive have been locked using the Windows bit locking feature. There are some laptops where bit locker could not be implemented and these machines can never be borrowed, and not allowed to be taken outside the work cubicles.

Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected by HIPAA or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after not more than 10 minutes of inactivity.

Most of the PC's have automatic lock feature after an inactivity of ten minutes. Some machines where scripts are being executed, locking has not been possible since it is causing the scripts to stop.

8.4 DATA SECURITY PROTECTION

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

Seqrite is the virus protection installed on all machines and VMs. A complete scan happens once every week and it is always active. The security patches are also scanned, and virus scan software is also upgraded based on new release.

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

PC's and laptops have the USB drives disabled. Backups can be taken via Google Workspace. CST team will help members with the backup and restore, in situations when their machines are changed.

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

VPN or Citrix servers are used for connecting to customer workstations. Any data used for testing in Azure VMs is deleted as a part of the closure tasks as soon as the project is closed. Also these are audited by CST.

Network / System Access

Access to any external system has to be approved by the program manager and a request made to the CST team. Based on approval from the CST team the network engineer helps make the access. These are tracked using the network access form / IT ticket raised in IT ticketing tool and the copies are filed.

E-mail:

PHI is never sent via mail and always shared via SFTP/Shared Drive on customer server and team is trained on this process. If they share any screenshots they make sure that the PHI data is blocked off (coloured with black) before it is shared.

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

If members need to connect from external networks, prior approval needs to be requested from the program managers, who will approve based on the need. Audit logs and access notification indication helps us track and monitor the access.

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

Access to PHI is regulated and is provided only to the project teams and data is tested on the Client's machine and not brought into local machines as far as possible. If they are brought in TL's and PM's make sure that it is deleted after the process has been completed.

Hard Copy Reports or Work Papers:

Members normally handle only soft copies of the files. Hard copies are not applicable.

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

Employees are educated during the HIPAA training sessions and made aware of this rule.

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

BAA are established with all external agencies, and file transfers to customers are handled only by Project Managers and Program managers,

End point data protection

End points are protected by restricting access to non-admin users to PHI data. Restrictions to the sites that can be accessed is controlled via firewall.

End Point Security	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1045365346/End+Point+Security

8.5 DISPOSAL OF PAPER AND/OR EXTERNAL MEDIA

Shredding:

As a policy, paper records are not maintained or printed by Triyam teams due to confidentiality of PHI data handled. USBs are disabled. However, HR and Finance team may need to maintain some paper records to satisfy local regulatory requirements. An exclusive shredder is made available to these teams to dispose paper records beyond their retention period.

Disposal of Electronic Media: All external media containing data that is no longer needed must be sanitized or destroyed in accordance with HIPAA compliant procedures.

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

At Triyam any external disk procured from the customer is returned back as soon the backup is restored in Azure and no external electronic media is used as a part of the data conversion process. In cases where the PHI files are copied to an external disk it is copied onto sftp and transferred in a controlled environment from a single machine at onsite and shipped to the customer to the address specified. The disc is protected using the secure keys and this key information is sent across via a Google Workspace mail to the customer.

9 Specific Protocols and Devices

9.1 WIRELESS USAGE STANDARDS AND POLICY

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

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

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

- A currently supported version of an operating system with the latest security updates
- Antivirus software updated to the latest definition, depending on operating system
- At minimum WPA2 or stronger wireless protocol
- Appropriate VPN Client, if applicable
- Supported Internet browser with latest security updates

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

Training Requirements **–** As a part of the initial training, the usage of wifi is listed and the precautions in terms of not connecting from unprotected network is emphasized. This training session will cover the basics of connecting to wireless networks, securing your computer when connected to a wireless network, and the proper method for disconnecting from wireless networks.

Wireless usage	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1045725674/WIRELESS+USAGE+STANDARDS+AND+POLICY

9.2 USE OF REMOVABLE MEDIA

Removable media included within the scope of this policy includes, but is not limited to, SD cards, DVDs, CD-ROMs, and USB devices. All removable media must be authorized by the Company before use.

The purpose of this policy is to guide employees/contractors of the Company in the proper use of removable media when a legitimate business requirement exists to transfer data to and from Company networks.

All users must be aware that sensitive data could potentially be lost or compromised when moved outside of Company networks. Removable media received from an external source could potentially pose a threat to Company networks. Sensitive data includes all human resource data, financial data, Company proprietary information, and protected health information ("PHI") protected by the Health Insurance Portability and Accountability Act ("HIPAA").

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

Data backups from media is stored in Azure and this has the encryption enabled and cannot be accessed by any unauthorized personnel. Similarly any data copied to an external media is secure as it is password protected.

In cases where we receive the copy of the database through removable media, we make sure that it is restored safely to Azure and not brought into the regular network. It is being handled only by a single point of contact at the onsite office.

Removable media is returned/sent back to the customer after the data is restored.

Removable media is not allowed to be used in the laptops/desktops used by employees. This has been restricted using Seqrite EPS.

Hardware Security	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1045430631/Use+of+Removable+Media

10 Retention / Destruction of Medical Information

Since Triyam is only into archival of patient data, the information retention/destruction will be based on customer inputs/US regulatory laws.

Record Retention -

Archived data is maintained in Azure by Triyam and responses to patients and record amendment is done by the end users of Fovea at the facilities who are bound by an NDA as per the contract. The above policy is not directly applicable to Triyam as Triyam is into archiving the data so that customers can retain the same for a period of 6 years as per the law. Also when they migrate from one system to another they would require to refer to the old legacy records.

Record Destruction – If a project is no longer required by the customer, access to all users in Fovea and data to that project is removed from Fovea and this way the soft copy of the data is no longer visible to anyone. Since activation of the users triggers a mail and also the list of users are audited on a weekly basis, access to this data (if done) shall be traced immediately.

11 Disposal of External Media / Hardware

11.1 DISPOSAL OF EXTERNAL MEDIA

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

The following steps must be adhered to:

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

External media is returned back to the customer in cases where a copy of the database is procured at onsite. Data is all maintained and is handled in Azure and no other external media is used by employees of Triyam.

A. REQUIREMENTS REGARDING EQUIPMENT

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

Medical equipment are not used at Triyam. Also laptops and desktops used do not contain PHI. The PHI files are stored only in Azure and when the project is in progress it is stored in the virtual machines and very rarely in the local desktops/laptops of the team members. Even in such cases these files are deleted as a part of the closure activities. So laptops/desktops used by the team contains no PHI information.

B. DISPOSITION OF EXCESS EQUIPMENT

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

- Older machines are regularly utilized for spare parts.
- Older machines are used on an emergency replacement basis.
- Older machines are used for testing new software.
- Older machines are used as backups for other production equipment.

- Older machines are used when it is necessary to provide a second machine for personnel who travel on a regular basis.
- Older machines are used to provide a second machine for personnel who often work from home.

In any of the above cases the Company will ensure PHI is properly sanitized from the equipment before stored in inventory.

At Triyam, all older laptops are stored in inventory and these machines are formatted before being allocated to another member. This is being handled by the CST team members. These machines do not contain any PHI information.

12 Change Management

Statement of Policy

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

Procedure

1. The IT staff or other designated Company employee who is updating, implementing, reconfiguring, or otherwise changing the system shall carefully log all changes made to the system and ensure that the change tracking is available for review if necessary.
2. The employee implementing the change will ensure that all necessary data backups are performed prior to the change.
3. The employee implementing the change shall also be familiar with the rollback process in the event that the change causes an adverse effect within the system and needs to be removed.

Change Management	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1094418439/Change+Management

13 Software Configuration Management

Statement of Policy

To ensure the Company is maintaining the right versions of the source code components of the archival solution throughout the software development life cycle, systematically managing, organizing and controlling the changes to these components, integrating and packaging them for a smooth release every time. This will help the Software development team to make incremental releases of the solution, troubleshoot issues that arise due to an update and release hot fixes, without compromising the integrity and quality of the solution.

Procedure

1. Identify source code components – The Software development team shall identify the configuration items (source code components) from the archival solution products that compose baselines at given points in time. The team shall establish relationship among items, create a mechanism to manage multiple level of control and procedure for change management system.

2. Version Control – The team shall create versions/specifications of the existing product components to build new product version with the help of VSTS, a Software Configuration Management tool.

3. Baselines and change control - a baseline is a set of mutually consistent configuration Items, which has been formally reviewed and agreed upon, and serves as the basis of further development. The team shall establish baselines at the end of each phase of software development. Merging and branching features of VSTS are used to create the baselines.

   As part of every new release, the requirements for the release (new features / enhancements to existing features / bug fixes from previous release / feedback from customers) are picked up from product back log and finalized based on priority. Each requirement is evaluated to assess technical merit, potential side effects, overall impact on other configuration objects and system functions, and the projected cost of the change. The results of the evaluation are presented during the scrum meeting and approval is sought from the Management. Previously baselined items are accordingly checked out, changes made and checked in back into VSTS. This process continues till all the items are tested, bugs are fixed and retested and the items are ready for release. Continuous baselines are created at every build, and branch completion and merging.

Source Code Management Guide	https://triyam.atlassian.net/wiki/spaces/FOV/pages/3156312122/Source+Code+Management+Guide

14 Patch Management

FOVEA

Fovea's maintenance is done once monthly or bi-monthly. This includes running SQL indexes and updating statistics for better performance, production environment monitoring and fixing alerts from Microsoft Defender.

Fovea is a web application and updates are done once within a 4 to 6-week range during non-office hours (late night). As industry standard, continuous integration and deployment is done, down time during upgrades is very minimal. All upgrades are done by Triyam's team, and no involvement of customer is necessary. There will be no impact on the customer due to any upgrade, product enhancements or release or hot fixes. Patches are categorized based on severity. Critical patches are applied on priority basis within 72 hours. In case it is not possible to apply within 72 hours, a rollback may be considered.

For on-premise deployments, application updates are done in customer environment during the deployment window provided by customer. Updates are done in their Stage environment, tested by Triyam's QA and customer's QA and then deployed in production. At any point, we make sure the customer has the latest version of Fovea not older than 6 months of the current cloud version.

Source Code Management Guide depicting how major releases and hot fixes are deployed	https://triyam.atlassian.net/wiki/spaces/FOV/pages/3156312122/Source+Code+Management+Guide
Fovea On-premise installation steps	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1204551686/On-premise+Fovea+Installation+Steps

OS AND OTHER IT RELATED SOFTWARE

OS

- OS upgrades to laptops and desktops are handled through Seqrite automatically.
- Firewall devices – OS patching is done based on alerts received from Sonic Firewall.
- Azure VMs – upgrades are handled automatically through Seqrite.

IT related software

- Seqrite EPS – auto update happens whenever new anti-virus definitions are available, for systems that are offline – update will be pushed manually

- Seqrite EPS – runs on VMs, auto update happens whenever new anti-virus definitions are available
- Browsers (Chrome, Microsoft Edge) – updates are pushed through Seqrite EPS
- Apps installed on end user systems (Microsoft 365, Adobe, etc) – patches handled by Seqrite EPS

15 Audit Controls

Statement of Policy

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

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

At Triyam, the Firewall reports are monitored fortnightly, to make sure that no unauthorized site is accessed. Also, the logins of Fovea are monitored across all environments. Any unauthorized users or users whose login domains are not attached to any facility in Fovea are not provided access to Fovea. This is controlled at the login creation level and these users shall not be affiliated to any facility till it is made sure that these are authorized users.

The access to the Fovea production database is restricted and the members who access the database are monitored through the logs in Azure. This is also monitored continuously using an ongoing task.

Fovea has audit capability that captures and stores the entire access information. Reports are available that track the transactions performed in the application, and this is checked on a need basis.

Access to Azure is also tracked using the logs and we shall be able to get the list of users who have accessed Azure recently. Also since warning mechanism is being set in Azure, any unauthorized access shall be immediately notified to the admin users.

Audit Controls	https://triyam.atlassian.net/wiki/spaces/FOV/pages/824180739/Fovea+Audit+Report

16 Information System Activity Review

Statement of Policy

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

Procedure

1. Kindly refer to "Audit Controls" Section above, for details of the technical mechanisms that track and record activities on Company's information systems that contain or use ePHI.

2. The CST Team shall be responsible for conducting reviews of Company's information systems' activities. Such person(s) shall have the appropriate technical skills with respect to the operating system and applications to access and interpret audit logs and related information appropriately.

3. The Security and Privacy Officer shall develop a report format to capture the review findings. Such report shall include the reviewer's name, date and time of performance, and significant findings describing events requiring additional action (e.g., additional investigation, employee training and/or discipline, program adjustments, modifications to safeguards). To the extent possible, such report shall be in a checklist format.

4. Such reviews shall be conducted regularly. Audits also shall be conducted if Company has reason to suspect wrongdoing. In conducting these reviews, the CST Team shall examine audit logs for security-significant events including, but not limited to, the following:

   a. Logins – Scan successful and unsuccessful login attempts. Identify multiple failed login attempts, account lockouts, and unauthorized access.

   b. File accesses – Scan successful and unsuccessful file access attempts. Identify multiple failed access attempts, unauthorized access, and unauthorized file creation, modification, or deletion.

   c. Security incidents – Examine records from firewall event logs, security devices or system audit logs for events that constitute system compromises, unsuccessful compromise attempts, malicious logic (e.g., viruses, worms), denial of service, or scanning/probing incidents.

d. User Accounts – Review of user accounts within all systems to ensure users that no longer have a business need for information systems no longer have such access to the information and/or system.

All significant findings shall be recorded and documented using an appropriate report format.

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

Audit Control	https://triyam.teamwork.com/#tasks/11531532	Firewall report audited once in a month
Audit Control	https://triyam.teamwork.com/#tasks/7680101	Live Fovea user audit report is executed once a month
Audit Control	https://triyam.teamwork.com/#/tasks/9519860	Fovea user audit in non-production environments report is executed once a month

17 Data Integrity

Statement of Policy

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

Methods to protect Company's ePHI from improper alteration or destruction include but not limited to:

- To the fullest extent possible, Company shall utilize applications with built-in intelligence that automatically checks for human errors.
- Company shall acquire appropriate work-based and host-based intrusion detection systems. The Security and Privacy Officer shall be responsible for installing, maintaining, and updating such systems.
- To prevent transmission errors as data passes from one computer to another, Company will use encryption, as determined to be appropriate, to preserve the integrity of data.
- Company will check for possible duplication of data in its computer systems to prevent poor data integration between different computer systems.
- To prevent programming or software bugs, Company will test its information systems for accuracy and functionality before it starts to use them. Company will update its systems when IT vendors release fixes to address known bugs or problems.
- Company will install and regularly update antivirus software on all workstations to detect and prevent malicious code from altering or destroying data.
- To prevent exposing magnetic media to a strong magnetic field, workforce members shall keep magnetic media away from strong magnetic fields and heat. For example, computers should not be left in automobiles during the summer months.

18 Data Backup and Contingency Plan

Statement of Policy

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

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

Procedure

1. **Data Backup Plan**

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

   b. All backups (database, blobs, etc) are handled by Azure. This task is being monitored using Teamwork using weekly and fortnightly tasks.

   c. Fovea source code is maintained in GitHub of Azure DevOps. Version history of all the changes made to the source code components and builds are maintained.

   d. The CST Team shall monitor storage and removal of backups and ensure all applicable access controls are enforced.

   e. The CST Team along QA Team shall test backup procedures once in three months, to ensure that exact copies of customer data including ePHI can be retrieved and made available. Such testing shall be documented by the CST Team. To the extent such testing indicates need for improvement in backup procedures; the CST Team shall identify and implement such improvements in a timely manner.

2. **Disaster Recovery and Emergency Mode Operations Plan (Business Continuity Plan)**

   a. The Security and Privacy Officer shall be responsible for developing and regularly updating the written disaster recovery and emergency mode operations plan for the purpose of:

i. Restoring or recovering any loss of ePHI and/or systems necessary to make ePHI available in a timely manner caused by fire, vandalism, terrorism, system failure, or other emergency; and

ii. Continuing operations during such time information systems are unavailable. Such written plan shall have a sufficient level of detail and explanation that a person unfamiliar with the system can implement the plan in case of an emergency or disaster. Copies of the plan shall be maintained on-site and at other secure off-site location.

b. The disaster recovery and emergency mode operation plan shall include the following:

i. Current copies of the information systems inventory and network configuration developed and updated as part of Company's risk analysis.

ii. Current copy of the written backup procedures developed and updated pursuant to this policy.

iii. Identification of an emergency response team. Members of such team shall be responsible for the following:

1. Determining the impact of a disaster and/or system unavailability on Company's operations.

2. In the event of a disaster, securing the site and providing ongoing physical security.

3. Retrieving lost data.

4. Identifying and implementing appropriate "work-arounds" including facility access during such time information systems are unavailable.

5. Taking such steps necessary to restore operations.

iv. Procedures for responding to loss of electronic data including, but not limited to retrieval and loading of backup data or methods for recreating data should backup data be unavailable. The procedures should identify the order in which data is to be restored based on the criticality analysis performed as part of Company's risk analysis

v. Telephone numbers and/or e-mail addresses for all persons to be contacted in the event of a disaster, including the following:

1. Members of the immediate response team,

2. Information systems vendors, and

3. All current workforce members.

c. The disaster recovery team shall meet on annual basis to:

i. Test and review the effectiveness of the disaster recovery and emergency mode operations plan (Business Continuity Plan, BCP) in responding to any disaster or emergency experienced by Company.

Threats to the confidentiality, integrity, and availability (referred to as "threat agents") of ePHI created, received, maintained, or transmitted by Company are identified during the annual Company risk assessment. These inputs are also fed into this process.

In the absence of any such disaster or emergency, plan drills to test the effectiveness of the plan and evaluate the results of such drills; and

ii. Review the written disaster recovery and emergency mode operations plan and make appropriate changes to the plan. The Security and Privacy Officer shall be responsible for convening and maintaining minutes of such meetings. The Security and Privacy Officer also shall be responsible for revising the plan based on the recommendations of the disaster recovery team.

Disaster recovery procedure is maintained here	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1243578394/Disaster+Recovery
Disaster recovery test, results and action items are tracked in Teamwork	https://triyam.teamwork.com/app/tasks/13014431
Annual Company Risk Assessment TW task	https://triyam.teamwork.com/app/tasks/10046381

19 Security Awareness and Training

Statement of Policy

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

All workforce members shall receive appropriate training concerning Company's security policies and procedures. Such training shall be provided prior to the effective date of the HIPAA Security Rule and on an ongoing basis to all new employees. Such training shall be repeated annually for all employees. Also, training shall be reviewed annually to ensure all necessary materials are current.

Procedure

a. Security Training Program

   i. The Security and Privacy Officer shall have responsibility for the development and delivery of initial security training. All workforce members shall receive such initial training addressing the requirements of the HIPAA Security Rule including the updates to HIPAA regulations found in the Health Information Technology for Economic and Clinical Health (HITECH) Act. Security training shall be provided to all new workforce members as part of the orientation process. Attendance and/or participation in such training shall be mandatory for all workforce members. This is tracked as part of Employee Joining Checklist. The Security and Privacy Officer shall be responsible for maintaining appropriate documentation of all training activities.

   ii. The Security and Privacy Officer shall have responsibility for the development and delivery of ongoing security training provided to workforce members in response to environmental and operational changes impacting the security of ePHI, e.g., addition of new hardware or software, and increased threats. This will be addressed as part of monthly HIPAA trainings or conducted exclusively based on need.

   iii. The Security and Privacy Officer shall have responsibility to conduct the security training annually as well and maintain attendance records.

b. Security Reminders

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

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

c. Protection from Malicious Software

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

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

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

c) Importance of protecting and maintaining integrity of customer data at all times

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

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

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

g) Damage caused by viruses and worms, and

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

d. Password Management

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

a) Passwords must be changed regularly

b) A user cannot reuse passwords until a reasonable amount of time has passed

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

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

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

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

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

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

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

e. Monitoring Login Attempts and Reporting Discrepancies

a) Staff is made aware how login attempts are monitored, and lockout will result from too many unsuccessful attempts

b) Staff is instructed how to identify and report any discrepancies concerning user logins

f. Security training related to HIPAA and handling of the attachments and security related features to be followed while accessing Triyam mail is imparted every year. As a part of the employee induction program the recorded meetings are played for the new joinees to listen and then a follow up session is conducted where their understanding of HIPAA and security rules are verified. HIPAA training is part of Employee Entry Checklist in Teamwork for each employee. Ongoing sessions are conducted once in a month to reiterate the security rules. Bi-weekly cybersecurity awareness emails are sent with the critical points listed as reminders and podcasts are sent periodically as a part of educating and training the members.

g. KnowBe4 tool will be used to run phishing simulations and also to administer security related trainings to employees.

Monthly HIPAA training	https://triyam.teamwork.com/app/tasks/10046381
Annual HIPAA training	https://triyam.teamwork.com/app/tasks/13324681
Cybersecurity awareness emails and log	https://triyam.teamwork.com/app/tasks/15187717 https://triyam.atlassian.net/wiki/spaces/FOV/pages/755367952/CYBER+SECURITY+AWARENESS

20 Security Management Process

Statement of Policy

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

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

Procedure

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

b. The risk analysis shall incorporate the following procedures as necessary:

i. Document Company's current information systems.

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

b) Update/develop facility layout as necessary showing location of all information systems equipment, power sources, telephone jacks, and other telecommunications equipment, network access points, fire and burglary alarm equipment, and storage for hazardous materials.

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

d) For each application identified:

i) Describe the data associated with that application.

ii) Determine whether the data is created by the organization or received from a third party. If data is received from a third party, identify that party and the purpose and manner of receipt.

iii) Determine whether the data is maintained within the organization only or transmitted to third parties. If data is transmitted to a third party, identify that party and the purpose and manner of transmission.

iv) Define the criticality of the application and related data as high, medium, or low. Criticality is the degree of impact on the organization if the application and/or related data were unavailable for a period of time.

v) Define the sensitivity of the data as high, medium, or low. Sensitivity is the nature of the data and the harm that could result from a breach of confidentiality or security incident.

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

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

i) Natural threats, e.g., earthquakes, storm damage.

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

iii) Human threats

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

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

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

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

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

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

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

ii) Assign criticality level.

iii) Factoring in the likelihood and impact, assign priority to those risks which require more immediate attention.

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

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

i) Determine timeline for implementation.

ii) Determine costs of such measures and safeguards and secure funding.

iii) Assign responsibility for implementing specific measures and safeguards to appropriate person(s).

iv) Make necessary adjustments based on implementation experiences.

v) Document actual completion dates.

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

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

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

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

Annual Company Risk Assessment TW task	https://triyam.teamwork.com/app/tasks/10046381

21 Vulnerability Management

Statement of Policy

To establish a continuous process for discovering, prioritizing, and resolving security vulnerabilities across the organization's IT infrastructure.

Company enterprise networks are vast systems of remote and on-premises endpoints, locally / centrally installed software, cloud apps, and third-party services. Every one of these assets plays a vital role in business operations and any of them could contain vulnerabilities that threat actors can use to sow chaos. Organization relies on the vulnerability management process to head off these cyberthreats before they strike.

Procedure

1. **Maintain Asset Inventory**

   a. CST, under the direction of the Security and Privacy Officer, shall create and maintain an inventory of all the hardware, software, and other IT assets active on the company network.

   b. This inventory will be periodically updated and reviewed. Whenever there is a major change to the Company's infrastructure landscape, the vulnerabilities associated with the change will be re-assessed.

2. **Vulnerability Discovery / Assessment**

   a. **Alert Monitoring –** CST will set alerts in various internal systems to flag off vulnerabilities. Roles and responsibilities for configuring these alerts shall be defined. Adequacy of alerts will be reviewed from time to time. Dedicated personnel will be assigned to continuously monitor the alerts and trigger the incident response process as and when critical alerts occur. Incident Response team will pull in relevant stakeholders to track the vulnerability to closure.

   b. **Annual Penetration Testing -** Company, under the direction of the Security and Privacy Officer, shall conduct annual penetration testing with the help of third party vendor.

c. **Quarterly Qualys Scans / internal scans –** Company shall conduct quarterly internal vulnerability scans or engage third party vendor to run Qualys scans. Qualys scan is a cloud-based service that gives immediate, global visibility into where our IT systems might be vulnerable to the latest Internet threats and how to protect them. It helps you to continuously identify threats and monitor unexpected changes in our network before they turn into breaches.

3. Vulnerability Prioritization and Remediation

a. The company shall prioritize the vulnerabilities identified through above mentioned methods based on criticality and impact. An action plan to remediate the vulnerabilities is drawn and the plan is closely followed up to closure. The remediation plan is published in Confluence.

4. Reassessment and monitoring

a. To confirm that mitigation and remediation efforts worked and to ensure they don't introduce any new problems, CST will periodically reassess the assets, alerts and vulnerabilities. The team also will take stock of the overall network and the general cyberthreat landscape, as changes in either one may require updates to security controls.

Penetration Testing Teamwork task link	https://triyam.teamwork.com/app/tasks/20103247
Quarterly Qualys Scan Teamwork task link	https://triyam.teamwork.com/app/tasks/21009456

22 Incident Management

Statement of Policy

To establish a robust process for identifying, managing, recording and analyzing security threats or incidents in real-time. It seeks to give a robust and comprehensive view of any security issues within our IT infrastructure.

A security incident can be anything from an active threat to an attempted intrusion to a successful compromise or data breach. Policy violations and unauthorized access to data such as health (PHI), financial, social security numbers, and personally identifiable records (PII) are all examples of security incidents.

Other incident vulnerabilities include, but not limited to:

- Malware / ransomware attacks
- Phishing
- Non-availability of Fovea application as a whole or certain features of Fovea
- Unforeseen performance issues (Fovea and other supporting internal systems)
- PHI data integrity issue
- Data leakage / breach (Customer data / Company data / Employee data)
- Any disruption / unplanned changes or deviations to production

Company shall identify a strong Incident Response team and develop a security incident response plan with a robust mechanism for quick identification, reporting and containment of incidents so as to resume / restore business as usual operations, as quickly as possible.

Procedure

- Develop a security incident response plan that includes guidance on how incidents are detected, reported, assessed, and responded to. Have battle cards / playbooks ready for a set of threat scenarios. Continuously update security incident response plan, as necessary, particularly with lessons learned from prior incidents and battle cards / playbooks for new set of threats.

- Establish an incident response team including clearly defined roles and responsibilities. This team shall include functional roles within CST as well as representation from other functions such as Dev, QA, DC, HR, Finance, Support, Training and Legal.

- Develop a comprehensive training program for every activity necessary within the incident response plan. Practice the security incident response plan with test scenarios on a consistent basis and make refinements as need be.

- It is the responsibility of each employee or contractor to report perceived security incidents on a continuous basis to his / her immediate supervisor or security personnel (CST). A User is any person authorized to access an information resource. Users are responsible for the day-to-day, hands-on security of that resource. Users need to formally report all security incidents / potential vulnerabilities / violations of the security policy immediately to CST through an email to incident@triyam.com. An incident report ticket is automatically created in the IT Request tracking tool. The ticket is tracked to closure in the tool.

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

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

- In case of any security breach that involves / impacts customer, respective personnel at customer end are notified as soon as possible and further course of action is jointly deliberated.

- After any security incident, a post-incident analysis shall be performed to learn from successes and failures and make adjustments to the security program and incident management policy / procedure, where needed.

- Any employee / contractor who is found responsible for a security incident will be imposed a sanction as per the Company's Sanction Policy.

Incident Response Plan	https://triyam.atlassian.net/wiki/spaces/FOV/pages/755040266/INCIDENT+RESPONSE+PLAN
Emergency Incident Response Process	https://docs.google.com/presentation/d/1l1ofFQPHIFf4Pud5ainlBBpb-ZCKF_i1/edit?usp=drive_link&ouid=117332864329843481584&rtpof=true&sd=true
Incident Response Template	https://docs.google.com/document/d/1f3BseDI9TxvKhbQOxb52WlKKvu7DFap6/edit?usp=drive_link&ouid=117332864329843481584&rtpof=true&sd=true
Battle Cards / Playbooks	https://drive.google.com/drive/folders/1CyvWSkii0YLE_kibjCYpRIbH4ctVZY8T
Reporting security incident	Email to incident@triyam.com
Security Breach Procedure	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1216577546/Breach+Notification+Policy
Sanction Policy	https://triyam.atlassian.net/wiki/spaces/FOV/pages/14057669/Sanction+policy+R+-+164.308+a+1+ii+C

23 Emergency Operations Procedures

Purpose

To provide procedures for managing and documenting patient encounters when the archival system is unavailable due to planned or unexpected outages.

Procedures

Notification:

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

planned downtime of archival system,
unexpected outage of archival system, and
resumption of services following an outage such that normal operations may resume.

24 Emergency Access “Break the Glass”

Policy Summary

“Break the Glass” refers to the Company of enabling a licensed practitioner to view a patient’s medical record, or a portion thereof, under emergency circumstances, when that practitioner does not have the necessary system access privileges otherwise.

Purpose

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

Enforcement

Emergency Access “Break the Glass” is planned for a future release by Triyam.

25 Sanction Policy

Policy

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

The Company will take appropriate disciplinary action against employees, contractors, or any individuals who violate the Company's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

Purpose

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

Definitions

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

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

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

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

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

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

Violations

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

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

Recommended Disciplinary Actions

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

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

-

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

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

Template of the Breach document and the details of the incident reporting process is being mentioned in the following section in confluence -

Breach Notification Policy	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1216577546/Breach+Notification+Policy
Sanction Policy	https://triyam.atlassian.net/wiki/spaces/FOV/pages/14057669/Sanction+policy+R+-+164.308+a+1+ii+C

Exceptions

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

References

U.S. Department of Health and Human Services

Health Information Privacy. Retrieved April 24, 2009, from

http://www.hhs.gov/ocr/privacy/index.html

Related Policies

Information Security Policy

Acknowledgment

I, the undersigned employee or contractor, hereby acknowledges receipt of a copy of the Sanction Policy for Triyam.

Dated this _______ day of _______________, 20___.

____

Signature of Employee/Contractor

26 Employee Background Checks

The Company will conduct employment reference checks, investigative consumer reports, and background investigations on all candidates for employment prior to making a final offer of employment and may use a third party to conduct these background checks. The Company will obtain written consent from applicants and employees prior to ordering reports from third-party providers. All background checks are subject to these notice and consent requirements.

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

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

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

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

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

Background verification of employees is done by a third party company - http://www.dcoderesearch.com . This was implemented for the core Security team members (CST) and is being further extended to all employees who are already on rolls as well as any new joinee coming into the organization.

Employee Background check logs are maintained by HR in a secure G-drive.

27 Discovery Policy: Production and Disclosure

Policy

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

Purpose

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

Scope

The Master Policy on Uses and Disclosures of PHI addresses e-discovery production and disclosure procedures related to the Federal Rules of Civil Procedures. Health information and records include both paper and electronic data related to relevant patient medical records and enterprise sources.

28 e-Discovery Policy: Retention

Policy

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

Purpose

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

Scope

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

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

Procedure

Guidelines for Retention of Records/Information and Schedules:

Record Retention

Unless otherwise stipulated, retention schedules apply to all records. Records will only be discarded when the maximum specified retention period has expired, the record is approved for destruction by the record owner, and a Certificate of Destruction is executed.

Non-record Retention

Non-records are maintained for as long as administratively needed, and retention schedules do not apply. Non-records may and should be discarded when the business use has terminated.

For example, when the non-record information, such as an employee's personal notes, is transferred to a record, such as an incident report, the notes are no longer useful and should be discarded. Preliminary working papers and superseded drafts should be discarded, particularly after subsequent versions are finalized.

Instances where an author or recipient of a document is unsure whether a document is a record as covered or described in this policy should be referred to the Compliance Officer for determination of its status and retention period.

E-mail Communication Retention

Depending on content, e-mail messages between clinicians and between patients and clinicians and documents transmitted by e-mail may be considered records and are subject to this policy. If an e-mail message would be considered a record based on its content, the retention period for that e-mail message would be the same for similar content in any other format.

The originator/sender of the e-mail message (or the recipient of a message if the sender is outside Organization) is the person responsible for retaining the message if that message is considered a record. Users must save e-mail messages in a manner consistent with departmental procedures for retaining other information of similar content. Users should be aware of *Messaging Policies* that establish disposal schedules for e-mail and manage their e-mail accordingly.

Development of Records Retention Schedules

Retention Schedule Determined by Law: All records will be maintained and retained in accordance with Federal and state laws and regulations. *[Note: minimum retention schedules are attached to this policy]*. Electronic records must follow the same retention schedule as physical records, acknowledging the format and consolidated nature of records within an application or database.

Changes to Retention Schedule: Proposed changes to the record retention schedules will be submitted to the Records Committee for initial review. The Records Committee, in consultation with the Legal Services Department, will research the legal, fiscal, administrative, and historical value of the records to determine the appropriate length of time the records will be maintained and provide an identifying code. The proposed revisions will be submitted to the Records Committee for review and approval. The approved changes will be published and communicated to the designated Records Coordinators.

Retention of Related Computer Programs: Retention of records implies the inherent ability to retrieve and view a record within a reasonable time. Retained electronic data must have retained with it the programs required to view the data. Where not economically feasible to pay for maintenance costs on retired or obsolete hardware or software only for the purpose of reading archived or retained data, then data may be converted to a more supportable format, as long as it can be demonstrated that the integrity of the information is not degraded by the conversion. Data Owners should work closely with IT personnel in order to comply with this section.

Retention of Records in Large Applications: Retention of data for large-scale applications, typically those that reside in the data center and are accessed by a larger audience, shall be the responsibility of the IT department.

Retention of Records on Individual Workstations: Primary responsibility for retention of data created at the desktop level—typically with e-mail, Microsoft “Office” applications such as Word, Excel, PowerPoint, Access, or other specialized but locally run and saved computer applications—shall be with the user/author. The user/author will ensure that the documents are properly named and saved to be recognizable by the user in the future, and physically saved to a “shared drive.” By saving a copy in this manner, IT will create an archive version of the saved document for a specified number of years after the user deletes the copy from the shared drive. Records with retention periods in excess of this period will require an alternative means of retention. Users are responsible for the security of any confidential information and/or protected health information created or maintained on their workstations.

29 Vendor Management

Policy

Maintaining confidentiality and integrity of customer data (PHI, PII and non-PHI) is of utmost priority to the Company's business. The Company shall establish and maintain a robust process to select its vendors, negotiate contracts, control costs and assess and mitigate risks associated with the vendors from time to time to ensure that customer data is protected at all times. Periodic vendor performance and risk assessments are carried out and necessary course correction is initiated.

Vendor Management Policy	https://triyam.atlassian.net/wiki/spaces/FOV/pages/1697218563/Vendor+Management+Policy
Master list of vendors	https://drive.google.com/drive/folders/1U9TdxSaY7z95UzhgRZA2l8F5deIFGPE4
Annual review of Master list of vendors and risks	https://triyam.teamwork.com/app/tasks/13556412