Telephone Town Hall Meeting (TTHM)

Information Security Policy

Version 2.3

INFORMATION SECURITY POLICY

Developed By:

TELEPHONE TOWN HALL MEETING

LAST REVISION DATE

June 14th, 2024

DOCUMENT OWNER

Ian Cerveny Director of Operations &
Security and Privacy Officer

TABLE OF CONTENTS

Sources:

TTHM HIPPA Compliance System for Business Associates (HCM), TTHM Non-Solicitation/Disclosure Agreement,
TTHM DR Plan, HITRUST, CSF, HIPAA Privacy Rule

TTHM.COM	Policy
Title: Introduction	
Approval Date: 06/14/2024	**Review: Annual**
Effective Date: 06/03/2024	**Information Technology**

1 Introduction

1.1 PURPOSE

This policy document 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 Telephone Town Hall Meeting, hereinafter referred to as TTHM. It serves as a central policy document with which all employees, vendors and contractors must be familiar and defines actions and prohibitions that all users must follow. The policy provides sales, executive and production staff within TTHM with policies and guidelines concerning the acceptable use of TTHM technology equipment, e-mail, Internet connections, voicemail, facsimile, future technology resources and information processing.

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

1.2 SCOPE

This policy document defines common security requirements for all TTHM 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 TTHM and entities in the private sector, in cases where TTHM has a legal, contractual, or fiduciary duty to protect said resources while in TTHM custody. In the event of a conflict, the more restrictive measures apply.

This policy covers the TTHM network system which is comprised of various hardware, software, communication equipment and other devices designed to assist TTHM in the creation, receipt, storage, processing, and transmission of information and the production of outreach on behalf of clients. This definition includes equipment connected to any TTHM domain or VLAN, either hardwired or wirelessly, and includes all stand-alone equipment that is deployed by TTHM at its office locations or at remote locales.

1.3 ACRONYMS / DEFINITIONS

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

Access – means the ability or the means necessary to read, write, modify, or communicate data/information or otherwise use any system resource.

Authentication – means the corroboration that a person is the one claimed,

Addressable Implementation Specifications – These are also instructions for meeting requirements of the Security Rule, but provide the organization with additional flexibility in determining what is reasonable and appropriate with respect to compliance.

BA – Business Associate

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

CIO – The Chief Information Officer

CMMC – Cybersecurity Maturity Model Certification currently on version 2.0 (CMMC 2.0)

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

Confidential Information – Confidential Information can include Protected Healthcare Information (PHI), Personally Identifiable Information (PII), Controlled Unclassified Information (CUI) and Protected Proprietary Information (PPI) provided by a client to TTHM in order to facilitate outreach.

Covered Entity – A healthcare provider, health plan, or healthcare clearinghouse. In the case of providers, specifically those providers that transmit protected health information in electronic form in connection with a transaction under the standard.

CPO – The Chief Privacy Officer is responsible for regulatory and compliance issues.

CST – Confidentiality and Security Team

CUI – Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

DHHS – Department of Health and Human Services

Disclosure – The release of protected information outside of an organization to another entity or employee of another entity.

DoD – Department of Defense

Encryption – The process of transforming information, using an algorithm, rendering it unusable, unreadable, and indecipherable to unauthorized persons.

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

FCI – Federal Contract Information

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

FTP – File Transfer Protocol

HIPAA – Health Insurance Portability and Accountability Act

HITRUST / HITRUST CSF – a certifiable framework that provides organizations globally a comprehensive, flexible, and efficient approach to regulatory/standards compliance and risk management.

Information System (IS) – means the hardware and software applications that comprise an organization's computer system.

IT – Information Technology

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

NDA – A Non-Disclosure Agreement (NDA) is a contract by which one or more parties agree not to disclose confidential or protected information that they have shared with each other as a necessary part of doing business.

Required Implementation Specifications – These are instructions for meeting requirements within the Security Rule. If an implementation specification is required, policies and procedures must be put in place to meet the requirement.

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.

Personally Identifiable Information (PII) – Information that, when used alone or with other relevant data, can identify an individual.

Protected Health Information (PHI) – Any personal health information that can potentially identify an individual, that was created, used, or disclosed in the course of providing healthcare services, whether it was a diagnosis or treatment.

Policies – serve as our written goals or statements of what needs to be achieved in order for a requirement to be successfully met. When necessary, the policies point to written procedures. Security policies are maintained in the TTHM Information Security Policies manual and the HIPAA compliance manual.

PPI – Protected Proprietary Information – any information which a client has provided to TTHM and which that client has expressed should be kept confidential in order to safeguard specified or unspecified personal, corporate, public or political interests.

Procedures – the specific instructions of what must be done, and by who to meet the requirements stated in the policy. Additional procedural details may be recorded in Security Risk Analysis documentation, or in other locations or documentation designated by the Security Officer.

Privileged Users – system administrators and others specifically identified and authorized by TTHM/BA management.

Sensitive Data – This includes any data in which disclosure may be harmful. These include PII, PHI and CUI.

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

Users with inquiry (read only) capabilities – individuals who are prevented, based on job assignment, from adding,

deleting, or changing records in a database. Their system access is limited to reading information only.

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

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

WAN – Wide Area Network – A computer network that enables communication across a broad area, i.e. regional, national.

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

1.4 HEALTHCARE DEFINITIONS AND TERMS

1.4.1 Healthcare Clearinghouse

Healthcare Clearinghouse - An entity that does one of the following:

- Processes or facilitates the processing of information that is received in a non-standard format, or contains non-standard data content, into standard data elements or a standard transaction; or
- Receives a standard transaction and processes or facilitates the processing of information into non-standard format or non-standard data content for a receiving entity.

Healthcare clearinghouses include billing services, repricing companies, community health information systems, and "value added networks," to name a few.

1.4.2 Healthcare Information Provider

Health Information Organization - An organization that facilitates the transfer of healthcare information electronically among organizations in a healthcare system. The same type of business may be known as a Health Information Exchange Organization or Regional Health Information Organization.

Other Healthcare Terms

Healthcare Provider - Any individual or institution that furnishes healthcare services, bills for, and is paid for those services. Examples of individual providers are physicians, dentists, and other licensed healthcare practitioners. Examples of institutional providers include hospitals, nursing homes, home health agencies, rehabilitation services, clinics, and clinical laboratories. Suppliers of durable medical equipment are also considered providers under HIPAA.

Health Plan - A program that pays the cost of healthcare services.

Individual - The person who is usually the subject of protected health information {i.e., a patient).

Office/Organization - Refers to the business associate (or owner of this policy manual) that provides services on behalf of covered entities.

Personal Representative - An individual who is legally authorized to make decisions related to healthcare information on behalf of an individual. Business associates must treat an individual's personal representative as the individual with respect to uses and disclosures of the individual's PHI, as well as the individual's rights under the Privacy Rule. The scope of the personal representative's authority may be verified in a legal document or specified by the patient.

Protected Health Information (PHI) - Any information that identifies an individual and describes his/her health status, sex, age, ethnicity, or other demographic characteristics, whether or not that information is stored or transmitted electronically.

Treatment - The definition of treatment under HIPAA is broader than the normal usage of the term. Under HIPAA, it not only includes providing health-related services, but also coordinating and managing care by one or more healthcare providers. It also includes coordination or management of healthcare between a healthcare provider and a third party, consultations among healthcare providers relating to an individual, and referrals from one healthcare provider to another.

Payment, Treatment, or Healthcare Operations - This defines how protected health information may be used or disclosed for the purposes of providing treatment to an individual, collecting payment for treatment, or other healthcare operations. The use and disclosure of protected healthcare information for these purposes is further defined as:

- Use and Disclosure for Treatment - Use or disclosure of protected health information that is necessary when providing care or treatment for an individual.
- Use and Disclosure for Payment - Use or disclosure of protected health information to third parties that is necessary for payment for health-related goods or services provided to an individual.
- Use and Disclosure for Healthcare Operations - Use and disclosure is limited to specific activities such as:
    - Education on available benefits and services;
    - Quality assessment and improvement activities;
    - Provider credentialing and certification;
    - Underwriting, rating, or other insurance-related activities;
    - Medical review, legal services, and auditing functions; and
    - Business planning and development.
- Business management and administrative activities including:
    - Compliance with privacy requirements;
    - Customer service and support;
    - Internal grievance procedures;

- Due diligence in connection with the sale or transfer of assets;
- Creating de-identified information; and
- Patient safety activities {as defined in PSQIA regulation 42 CFR 3.20).

Use - Use is a fundamental concept under HIPAA and refers to sharing information. Employing, applying, utilizing, examining, or analyzing individually identifiable health information by workforce members is considered "use." Information is "used" when it is shared within an organization. Information is "disclosed" when it is transmitted outside of an organization.

1.5 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.

HIPAA Privacy Rule HITRUST
CSF
Cybersecurity Maturity Model Certification (CMMC 2.0 framework)
National Institute of Standards and Technology (NIST)
Office of the Under Secretary of Defense for Acquisition and Sustainment of the United States Department of Defense (DoD)
FedRAMP
The State of Colorado The
United States (US)
The European Union (EU) and Asia-Pacific Economic Cooperation (APEC)

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

1.5.1 State Laws

State Law - State privacy laws that are ***contrary*** to federal HIPAA privacy requirements will be preempted by the federal laws, except where State laws are ***more stringent.***

Contrary, when used to compare a provision of State law to a federal HIPAA requirement, means:

- A covered entity would find it impossible to comply with both the State and federal requirements; or
- The provision of State law stands as an obstacle to the accomplishment and execution of the full purposes and objectives of the federal requirement.

More stringent, in the context of a comparison of a provision of State law and a federal HIPAA requirement, means a **State Law** that meets one or more of the following criteria:

- With respect to a use or disclosure, the law prohibits or restricts a use or disclosure in

circumstances under which such use or disclosure otherwise would be permitted.

- With respect to the rights of an individual who is the subject of the sensitive data such as PHI, permits greater rights of access or amendment; except to preempt any State law to the extent that it authorizes or prohibits disclosure of sensitive data such as PHI about a minor to a parent, guardian, or person acting in loco parentis of such minor.
- With respect to information to be provided to an individual who is the subject of sensitive data such as PHI, provides the greater amount of information about a use, disclosure, rights and remedies.

1.6 PRIVACY AND SECURITY OFFICER

Designation of a Security Officer is a requirement of the Security Rule. The Security Officer is responsible for implementation of security policies and procedures, completion of annual security risk assessments, and completion of identified corrective actions. The Security Officer, Privacy Officer and Compliance Manager may all be the same individual.

TTHM has established a Privacy and Security Officer as required by regulation. This Security and Privacy Officer will oversee all ongoing activities related to the development, implementation, and maintenance of TTHM privacy policies in accordance with applicable federal and state laws.

The current Security and Privacy Officer for TTHM is Ian Cerveny.

1.7 CONFIDENCIALITY OFFICER (CO)

The Confidentiality Officer (CO) is responsible for annual security training of all staff on confidentiality issues. **The current Confidentiality Officer (CO) for TTHM is Allison Court.**

1.8 COMPLIANCE MANAGER

The Compliance Manager is the individual responsible for implementation of the policies and guidelines and for updating their content, as necessary. The Compliance Manager is also responsible for workforce member training and documentation, and assisting the employer in evaluating and maintaining the effectiveness of the overall compliance system.

Designation of a Compliance Manager is not required of business associates. However, because business associates are responsible for compliance with many HIPAA rules, a Compliance Manager will be designated to organize any compliance efforts of the organization.

The current Compliance Manager for TTHM is Ben Cerveny.

1.9 COMPLIANCE COMMITTEE (CC)

It is recommended, but not required, that a Compliance Committee (CC) be established to assist the Compliance Manager and Security Officer with implementing and maintaining policies and actions required by HIPAA's standards and rules. The use of a Compliance Committee is optional and depends upon the size of the organization and available personnel.

TTHM has established a Compliance Committee made up of key personnel whose responsibility it is to assist the Compliance Manager in verifying compliance of the organization to any and all applicable Governance Regulation and Compliance (GRC) activities.

Meetings to confirm compliance will be held no less than **semi-annually**. The current members of the **Compliance Committee (CC)** are:

Ian Cerveny – Director of Operations & Security and Privacy Officer
Ben Cerveny – Compliance Manager
Allison Court – Confidentiality Officer
Preston Underwood – Director of Meeting Operations

1.10 CONFIDENTIALITY / SECURITY TEAM (CST)

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

All members identified within this policy are assigned to their positions by the CEO. The term of each member assigned is at the discretion of the CEO, but generally it is expected that the term will be one year. Members for each year will be assigned at the first meeting of the CST in a new calendar year. This committee will consist of the positions within TTHM most responsible for the overall security policy planning of the organization. The current members of the CST are:

Ian Cerveny – Director of Operations & Security and Privacy Officer
Ben Cerveny – Compliance Manager
Preston Underwood – Director of Meeting Operations
Allison Court – Confidentiality Officer

The CST will meet semi-annually to discuss security issues and to review concerns that arose during the previous six months. The CST will identify areas that should be addressed during annual training and review/update security policies as necessary.

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

The CST is responsible for maintaining a log of security concerns or confidentiality issues. This log must be maintained on a routine basis, and must include the dates of an event, the actions taken to address the event, and

recommendations for personnel actions, if appropriate. This log will be reviewed during the semi-annual meetings.

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

2 Information / Identity Access Management (IAM)

2.1 IDENTIFICATION AND AUTHENTICATION

Policy - Information / Identity Access Management (IAM) is a standard with one required specification and two addressable specifications. The purpose of policies and procedures for information access management is to provide workforce members and other authorized entities with appropriate access to sensitive data such as EPHI, PHI, PII, CUI and PPI.

The first specification requires the organization to obtain documentation from any business associate that the EPHI that is provided to them will be used and/or disclosed appropriately. The specifications for Access Authorization and Access Establishment and Modification are addressable and have applicable procedures in sections below.

Procedure - The Standard for Information Access Management is met by implementing the policies and procedures in sections:

(i) 2.1.1 Isolating Clearinghouse Functions,

(ii) 2.1.2 Access Authorization and;

(iii) 2.1.3 Access Establishment, Modification and Destruction.

2.1.1 Access Authorization

Policy - Only the Security Officer or designated individuals may authorize and grant sensitive data such as EPHI access to workforce members, technical support personnel, and other entities. The organization will define the information a user can access by granting or limiting access to systems, workstations, applications, files, records, fields, etc.

When non-workforce members require access to computers (i.e. for hardware installation, etc.), or to locations

where sensitive data such as EPHI may be accessed, such entities are required to sign and date a Vendor Non-Disclosure Agreement. If a non-workforce member is intentionally provided access to sensitive data such as EPHI in order to perform a service for the organization, a Vendor Non-Disclosure Agreement must be established with the entity prior to sensitive data being disseminated.

Procedure - All access requests for current employees and subsequently for new hires must be preceded by the reading and signing of an Employee Non-Disclosure Agreement. All access requirements for vendors and contractors involved in event production and service delivery must be preceded by the reading and signing a Vendor Non-Disclosure Agreement, both by the vendor and by the individual(s) providing services in their capacity as an employee or subcontractor of that vendor.

The Security Officer will grant access to sensitive data such as EPHI based on the minimum amount of Confidential Information needed by each individual to complete his or her assigned tasks in consultation with management personnel. The Security Officer will either grant access to information systems him/herself or will delegate the responsibility to a designated individual (e.g., IT personnel or service provider). The Compliance Manager will maintain documentation of compliance with this policy through signed NDA's and notification of completion of required annual training.

2.1.2 Access Establishment, Modification and Destruction

Policy - The organization shall implement procedures for establishment, modification and termination of access to information system(s) and to Confidential Information.

As assigned duties change, access to Confidential Information may need modification. If the organization grants global access to workforce members, access may only require modification in the case of termination.

Procedure - TTHM Schedulers will note events and services where Confidential Information is provided by a client, track which employees and vendors received that Confidential Information, and provide a reminder at the conclusion of each work week to destroy Confidential Information received during that week.

The Compliance Manager will provide TTHM employees and vendors with the most current TTHM Security Policy Handbook and ensure that a Non-Disclosure Agreement is signed by each individual before receipt of Confidential Information. The Director of Meeting Operations shall clearly communicate a timeline for destruction of Confidential Information received by employees and vendors.

Destruction - Destruction of physical and digital copies of Confidential Information received in order to facilitate events or services on behalf of clients must take place within one (1) week of the conclusion of the event or of services being rendered. The only exception is data provided to facilitate event setup or service delivery, which must be destroyed within thirty-one (31) days of the conclusion of the event or of services being rendered, or within thirty-one (31) days of final reporting being delivered to the client.

There are two acceptable methods for disposing of paper records containing Confidential Information: using a cross-cut shredder or placing the paper(s) in a burn bag. Do not use a recycle bin to dispose of paper records containing personal information, even after shredding.

Destruction of digital copies of Confidential Information by TTHM employees must be performed using BitRaser® File

Eraser or comparable software that has been approved by the Security Officer.

2.2 USER LOGON IDS

Individual users handling client data that includes Confidential Information shall have unique logon IDs and passwords when accessing information systems to process or store such data. An access control system shall identify each user and prevent unauthorized users from entering or using information resources. Security requirements for user identification include:

- Each user shall be assigned a unique identifier.
- Users shall be responsible for the use and misuse of their individual logon ID.

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

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

2.3 ACCESS CARDS AND CODES

Telephone Town Hall Meeting - TTHM is a **100% remote based** organization. With this in mind, the following applies:

1. **Only TTHM Confidentiality / Security Team (CST) members and Tele-Town Hall® system managers may access entire client databases that include Confidential Information.**
2. No other employees or any other vendors, contractors, or sub-contractors should ever require access to entire client databases used to facilitate TTHM services.
3. Tele-Town Hall® system access will be granted to other TTHM employees, vendors, contractors or sub-contractors to facilitate live event productions and texting services utilizing web-based control platforms within that system. Such access will be limited to information displayed within Tele-Town Hall® control platforms as needed by each individual to complete his or her assigned tasks, and only when an employee or vendor NDA has been signed by that individual.

2.4 PASSWORDS

User Account Passwords

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

Password Length and Complexity – Passwords/Passphrases are required to meet the following complexity requirements:

- Not contain the user's account name or parts of the user's full name that exceed two consecutive characters
- Be at least eight characters in length
- Contain characters from three of the following four categories:
    1. English uppercase characters (A through Z)
    2. English lowercase characters (a through z)
    3. Base 10 digits (0 through 9)
    4. Non-alphabetic characters (for example, !, $, #, %)

Complexity requirements are enforced when passwords are changed or created.

Change Frequency – Passwords must be changed every 180 days. Compromised passwords shall be changed immediately.

Reuse - The previous six passwords cannot be reused.

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

Restrictions on Recording Passwords - Passwords are masked or suppressed on all online screens. and are stored in an encrypted format.

2.5 CONFIDENTIALITY AGREEMENT

TTHM Employees, Vendors, Contractors and Subcontractors must sign, as a condition for employment or contracting, a Non-Disclosure Agreement that addresses confidentiality and the handling of Confidential Information. Additionally, Employees are given an Employee Handbook that further reinforces their obligations to protect and keep confidential TTHM and Client information, as defined in those documents.

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.

2.6 ACCESS CONTROL

The organization shall implement procedures to address two required specifications; Unique User Identification and Emergency Access Procedure. Procedures shall also be implemented with two addressable specifications; Automatic Legoff and Encryption/Decryption to meet the Security Rule's requirements for Access Control.

Information resources are protected by the use of access control systems. Access control systems include both internal (i.e., passwords, encryption, access control lists, constrained user interfaces, etc.) and external (i.e., port

protection devices, firewalls, host-based authentication, etc.).

Rules for access to resources (including internal and external telecommunications and networks) have been established by the information/application owner or manager responsible for the resources.

This guideline satisfies the "need to know" requirement of many regulations, 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, **only** upon the written approval of the Security Officer or appropriate personnel who is responsible for adding the employee to the network in a manner and fashion that ensures the employee is granted access to data only as specifically requested.

Multi-Factor Authentication (MFA)

Given the state of the modern era, single factor access (usually passwords) is no longer sufficiently secure for most business applications. With this in mind TTHM utilizes the MFA service, which is required to connect to all TTHM resources.

Identification and Authentication Requirements

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

2.7 TERMINATION OF USER LOGON ACCOUNT

Upon termination of an employee, whether voluntary or involuntary, employee's supervisor or department head shall promptly notify the Systems Administrator and other personnel as appropriate. If employee's termination is voluntary and employee provides notice, employee's supervisor or department head shall promptly notify the Systems Administrator and appropriate personnel of employee's last scheduled workday so that their user account(s) can be configured to expire. The employee's department head, or designated HR representative, shall be responsible for ensuring that all keys, ID badges, and other access devices as well as TTHM equipment and property is returned to TTHM prior to the employee leaving TTHM on their final day of employment.

No less than annually, the Systems Administrator or their designees shall provide a list of active user accounts for both network and application access for review. Department heads shall review the employee access lists within five (5) business days of receipt. If any of the employees on the list are no longer employed by TTHM, the department head will immediately notify the IT Department of the employee's termination status.

3 Third-Party Security Standards

3.1 EMPHASIS ON SECURITY IN THIRD PARTY CONTRACTS

Access to TTHM 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.

- A risk assessment of the additional liabilities that will attach to each of the parties to the agreement.
- Each service, access, account, and/or permission made available should only be the minimum necessary for the third party to perform their contractual obligations.
- If required under the contract, permission should be sought to screen authorized users.
- The right to monitor and revoke user activity should be included in each agreement.
- Language on restrictions on copying and disclosing information should be included in all agreements.
- Measures to ensure the return or destruction of programs and information at the end of the contract should be written into the agreement.
- If physical protection measures are necessary because of contract stipulations, these should be included in the agreement.

3.2 CONFIDENTIAL/SENSITIVE INFORMATION

Each Business Associate's (BA) relationship with TTHM and its clients is one of trust and confidence. Because of the nature of employee's duties, Business Associate (BA) will have access to sensitive business information critical to the business operations of TTHM and its customers.

Telephone Town Hall Meeting (TTHM) has the pleasure of serving clients in many industries. Our clients trust us with some of their most sensitive data including Protected Healthcare Information (PHI), Personally Identifiable Information (PII), Controlled Unclassified Information (CUI) and Protected Proprietary Information (PPI). These clients require some of the strictest level of confidentiality possible whenever dealing with sensitive information. Failure to maintain confidentiality is a major threat to the success of our clients. Some of these are listed below.

- Major Healthcare Insurance Providers
- Advocacy Organizations
- Campaigns and Legislators
- Emergency Management
- Transit Authorities
- Labor Unions
- School Districts
- State and Local Governments
- United States Federal Government Agencies and Departments
- Members of the United States Senate
- Members of the United States House of Representatives (Congress)
- Retirees

Business Associate (BA) will also have access to sensitive and confidential information belonging to TTHM's customers as a result of their employment with TTHM. Such information is the sole property of the customer and Business Associate (BA) shall not under any circumstance disclose such information to anyone absent the customer's explicit consent or Court order. This paragraph does not prevent Business Associate (BA) from disclosing information necessary for TTHM or its Business Associate (BA)s to conduct its business with the customer. Any compromise or potential compromise of confidential information should be reported immediately to the Business Associate (BA)'s direct supervisor.

3.3 CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Controlled Unclassified Information (CUI) is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.

3.4 SUBCONTRACTORS (BUSINESS ASSOCIATES – BA)

3.4.1 Business Associates

Business Associates - A person or organization that creates. receives. maintains. or transmits sensitive data such as protected health information (PHI) on behalf of a covered entity in order to perform a function, activity, or service for the covered entity. A business associate can be an independent contractor, but cannot be an employee of the same organization. The definition of Business Associate has been expanded to include:

A Health Information Organization, E-prescribing Gateway, or other person that provides data transmission services with respect to protected health information to a covered entity and that requires routine access to sensitive data such as protected health information (PHI);

A person who offers sensitive data such as a personal health record to one or more individuals on behalf of a covered entity;

Patient Safety Organizations that receive reports of patient safety events and concerns (that include sensitive data such as protected health information - PHI) from a covered entity, and that provide analyses of the information on behalf of the covered entity;

Entities that maintain or store sensitive data such as PHI on behalf of a covered entity. even if they do not actually view the protected health information; and

Subcontractors or Vendors who perform a service on behalf of a business associate that involves use or disclosure of a covered entity's protected health information will be considered business associates in the sense that they will incur liability for acts of non-compliance. However, it will be the responsibility of the business associate, and not the covered entity, to obtain satisfactory assurances in the form of a written contract affirming that the subcontractor will appropriately safeguard sensitive data such as PHI.

3.4.2 Subcontractors

The Privacy Rule requires that our office identify subcontractors to whom we provide sensitive data such as PHI in order to perform a function or activity on our behalf. We are also required to develop and implement written agreements with subcontractors that will provide our office with satisfactory assurances regarding the privacy of sensitive data such as protected health information that is provided to the subcontractors.

Subcontractors must comply with applicable Privacy and Security Rule requirements in the same manner as a covered entity and business associate, and likewise will incur liability for acts of noncompliance.

A subcontractor is a person or entity who performs a function or activity involving the use or disclosure of sensitive data such as PHI on the behalf of our office. A subcontractor can be an independent contractor, but cannot be an employee of the same organization.

Subcontractors are directly liable for violations of the applicable provisions of the HIPAA Rules, as are covered entities and business associates. According to the Omnibus Rule, "Covered *entities* must *ensure that they obtain satisfactory* assurances required *by the* Rules *from their* business associates, and ***business associates*** must do the same with regard to subcontractors, and so on. No matter how far "down the chain" the information flows.

This ensures that individuals' sensitive data such as health information remains protected by all parties that create, receive, maintain, or transmit the information in order for a covered entity to perform its health care functions."

A subcontractor is considered a business associate if the function, activity, or service they provide involves creation, receipt, maintenance, or transmission of protected health information. These downstream business associates are referred to as subcontractors in the Omnibus Rule.

3.4.3 Minimum Disclosure

The information provided to a subcontractor shall be the minimum necessary information needed for the subcontractor to perform the services listed in the business associate agreement.

3.4.4 Acceptable Use

A Business Associate (BA) has no reasonable expectation of privacy while using TTHM or its clients' IT Resources or the Network and not TTHM nor its client(s) or other BAs are responsible for the confidentiality of any personal information a BA transmits via IT Resources and/or the Network. TTHM reserves the right to monitor, access, and disclose the contents of or communication on IT Resources, the Network, or Data including BA's e-mail, text messages, instant messages voicemail, etc., at its discretion and at any time. TTHM has the right to access, review, delete, and/or disclose any Data, including but not limited to, files, records or email messages, text messages, voicemail messages, etc., stored on or transmitted through IT Resources and the Network without notice or authorization.

TTHM reserves the right at all times to disclose information about a BA or a BA's use of IT Resources, the Network, or Data to outside parties, including law enforcement and government agencies, if TTHM is required to do so by law or if TTHM has a good faith belief that disclosure is reasonably necessary to

(i) conform to the edicts of the law or comply with legal process,

(ii) protect and defend the rights and property of TTHM,

(iii) act under exigent circumstances to protect the personal safety of TTHM BAs, customers, or the public, or

(iv) to satisfy any applicable law, regulation, legal process or governmental request

TTHM/BA also reserves the right to limit a BA's use of IT Resources, the Network, or Data in order for TTHM to manage network connectivity, security concerns, and emergency/crisis events.

All passwords and encryption keys used on IT Resources or the Network by a BA must be kept confidential. The existence of passwords or encryption does not restrict or impair TTHM's ability or right to access electronic communications. All information regarding access to TTHM's IT Resources or Network, such as user identifications, phone numbers, access codes, and passwords, must be provided upon request and/or termination and is confidential and may not be disclosed to non-TTHM personnel.

BAs shall not (1) share an e-mail password with another person, for any reason, unless explicitly instructed to do so by Human Resources or the COO (2) provide e-mail access to an unauthorized BA, or (3) access another BA's e-mail box without explicit authorization from management. BAs also shall not use the same password in any other place or system outside of TTHM.

BAs have a duty to protect electronic information from being inadvertently compromised when using off- site connections. Remote access accounts are considered "as needed" accounts and account activity are monitored. It is the responsibility of any BA with such privileges to ensure a connection is not used by other persons to gain

access to TTHM Computing Assets, the Network, and/or Data. All remote connections require two-factor authentication.

IT Resources and the Network may **never** be used to transmit off-color jokes, ethnic slurs, racial epithets, or any joke or comment or image that may be construed inappropriate or disparaging of others based on sex, race, age, religious or political beliefs, disability, national origin, parenthood status, marital status, or any other protected class or characteristic, or which create an intimidating or unprofessional work environment.

BAs may not visit internet sites that contain obscene, pornographic, hateful, or other objectionable material. BAs are responsible for all behaviors performed on TTHM IT Resources and the Network under his or her assigned credentials. BAs should always sign out of their account before leaving a workstation.

3.5 COMPANY RECORDS AND FILES

All records, files, plans, documents and the like relating to the business of the Company. Any of the previous list is owned by the Company. Any of these a Business Associate (BA) prepares, uses, or comes in contact with shall be and shall remain the sole property of the Company and may not be copied without written permission of the Company and shall be returned to the Company on termination or cessation of your employment, or at the Company's request at any time.

3.6 BUISINESS ASSOCIATES AGREEMENTS

The Privacy Rule permits our office to disclose sensitive data to a subcontractor who performs a function or activity on our behalf, or provides a service that involves the creation, use, or disclosure of protected health information, provided that our office obtains satisfactory assurances that the subcontractor will properly safeguard the information.

We shall establish such written satisfactory assurances in the form of a written agreement (see below and HCM Form 4.11), Business Associate Agreement) with our identified subcontractors. The function of the business associate agreement is to describe the specific purpose of any permitted uses or disclosures of protected health information and to indicate the types of persons or entities to whom the information may be disclosed. The agreement does not authorize the subcontractor to use or disclose sensitive data such as PHI in the same manner that our office is entitled to use or disclose it.

Each agreement may have different purposes and limitations depending upon the services provided by the subcontractor. Specific information regarding purposes and limitations may be contained in attachments to the agreement. This enables our office to use a basic agreement format for all subcontractors with the specifics of use and disclosure for each subcontractor contained in the attachments.

3.6.1 Elements of the Business Associate Agreement

The business associate agreement (see HCM Form 4.11) contains the following elements:

(1) The agreement identifies the uses and disclosures of sensitive data such as PHI the subcontractor is permitted or required to make. The agreement requires the subcontractor to put appropriate safeguards in place to protect against a use or disclosure not permitted by the agreement. The description of permitted uses and disclosures outlines how the subcontractor may use or disclose protected health information that our organization has provided so they may perform the services listed in the agreement. The agreement states the purposes for which the subcontractor may use or disclose sensitive data such as PHI by identifying the services they will perform for our office, as well as any specific limitations, in an attachment to the Agreement.

(2) The agreement specifies that the subcontractor will refrain from using or disclosing the sensitive data such as PHI other than as permitted by the agreement or as required by law.

(3) The agreement requires the subcontractor to use appropriate safeguards to prevent misuse and inappropriate disclosure of the protected health information.

(4) The agreement requires that the subcontractor report to our organization as soon as feasible, any unauthorized uses or disclosures (breaches) of sensitive data such as PHI that it discovers.

(5) The agreement requires that agents and subcontractors that receive sensitive data such as PHI from the business associate agree to the same restrictions and conditions that apply to the **business associate**.

(6) The agreement requires that the subcontractor provide sensitive data such as PHI in accordance with the individual's right to access, inspect, and copy their health information.

(7) The agreement requires the subcontractor to provide sensitive data such as PHI in accordance with the individual's right to have the covered entity make amendments made to his/her PHI. This means that the subcontractor will make information available for amendment and incorporate any amendments, obtained by our organization, to the PHI that is maintained by them.

(8) The agreement requires the subcontractor to provide information required to make an accounting of disclosures of sensitive data such as PHI, where such disclosures were made for purposes not related to treatment, payment, and healthcare operations. Essentially, the subcontractor, if requested by the patient, must make the necessary accounting of disclosures in the same manner as our organization is required.

(9) The agreement requires the subcontractors to make internal practices, books, and records relating to the use and disclosure of health information received from, or created or received by, the subcontractor available to DHHS for purposes of determining our organization's compliance with HIPAA requirements.

(10) The **business associate** nonetheless is expected to investigate when it receives complaints or other information that contain substantial and credible evidence of violations by a subcontractor, and it (the **business associate**) must act upon any knowledge of such violation that it possesses.

(11) In the event that the organization is aware of a material breach or violation of the subcontractor's obligation under the contract or other arrangement, the organization must take reasonable steps to cure the breach or end the violation and, if such steps are unsuccessful, the contract must authorize termination, if feasible.

(12) The agreement requires that, upon termination of the contract, the subcontractor will return or destroy all sensitive data such as PHI received from, created by or received by the business associate. If this isn't possible, then the subcontractor must agree to limit disclosures of protected information beyond the termination of the contract.

3.6.2 Renewal of the Business Associate Agreement

Business associate agreements shall have a one-year term with an automatic renewal on the anniversary date of the agreement unless otherwise terminated by our office or the subcontractor.

3.6.3 Termination of the Business Associate Agreement

As provided for under the Privacy Standards, our office may immediately terminate a business associate agreement and any related agreement if we determine that the Business Associate has breached a material provision of the agreement, including, without limitation, the confidentiality and privacy provisions of the contract.

Alternatively, our office may choose to:

(a) Provide the subcontractor with ten (10) days written notice of the existence of an alleged material breach

(b) Afford the subcontractor an opportunity to cure said alleged material breach upon mutually agreeable terms.

Failure to cure the alleged material breach shall be grounds for the immediate termination of the agreement. If termination is not feasible, our office shall report the breach to the Secretary of DHHS.

Our office shall provide a subcontractor with a written notice of termination should we elect to terminate an agreement. Notices of termination shall be sent by registered or certified mail or a courier service that provides proof of delivery.

3.7 RETENTION OF OWNERSHIP

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

3.7.1 Isolating Clearinghouse Functions

Policy - Isolation of clearinghouse functions is the responsibility of a clearinghouse within a larger organization. The organization will obtain satisfactory assurance that the use and disclosure of sensitive data such as EPHI is limited to contracted services by establishing a business associate agreement (BAA) with the clearinghouse. The BAA will ensure that sensitive data such as EPHI provided by the organization is used and disclosed only for permitted purposes and will limit any sharing of sensitive data such as EPHI with the parent organization that is not specifically necessary in order to perform the service(s) it is contracted to provide.

Procedure - The Security Officer shall ensure that an appropriate business associate agreement is in place with the clearinghouse to ensure it is using and disclosing sensitive data such as EPHI only as permitted by their service contract and regulation. If the organization has a business relationship with the parent organization and already has a business associate agreement in place with that entity, it is not necessary to also establish a BAA with the clearinghouse directly.

4 Network Connectivity and Security

4.1 TELECOMMUNICATION EQUIPMENT

Certain connections may require a dedicated or leased equipment/software. This equipment is authorized only by the Security and Privacy Officer or appropriate personnel and ordered by the appropriate personnel at TTHM/BA or the client where relevant. Telecommunication equipment and services include but are not limited to the following:

- phone lines
- fax lines
- smart phones
- phone headsets
- software type phones installed on workstations
- conference calling contracts
- cell phones
- call routing software
- call reporting software
- phone system administration equipment
- 800 lines
- local phone lines
- telephone equipment

4.2 NETWORK SECURITY STANDARDS

Authority from the Security and Privacy Officer or appropriate personnel must be received before any employee or contractor is granted access to a TTHM networking equipment. All TTHM networking equipment is and must continue to be configured with the security standards set by the Privacy Officer. The Security and Privacy Officer shall review these baselines standards no less than annually.

4.2.1 BASELINE

All implementation specifications, both addressable and required, have been reviewed in the organization's initial and subsequent periodic risk analyses. The Security Officer has determined that each addressable specification is either reasonable and appropriate, that it will be met through an equivalent alternative measure, or that the specification nor any alternative measures ore reasonable or appropriate within its environment. When determining if an addressable specification is reasonable and appropriate, the Security Officer has considered the following:

- The size, complexity, and capabilities of our organization
- Our technical infrastructure, hardware, and software security capabilities
- The costs of security measures
- The probability and criticality of potential risks to our sensitive data such as electronic protected health information.

If, after evaluation by the Security Officer, an addressable specification is determined to be appropriate and reasonable, the Security Officer shall implement the security policy and procedure or shall provide explanation of an alternative method for meeting the requirements of the specification.

As described in the standard, alternative methods may sometimes be necessary to reasonably and appropriately implement a specification. Whenever it is determined that an addressable implementation specification is not appropriate or reasonable, documentation will be completed by the Security Officer to identify an equivalent alternative or, in the case of no action taken, identify how the specification has been met or that the specification has no application for the organization.

All required implementation specifications are implemented without exception.

4.2.2 Implementation Specifications

All implementation specifications, both addressable and required, have been reviewed in the organization's initial and subsequent periodic risk analyses. The Security Officer has determined that each addressable specification is either reasonable and appropriate, that it will be met through an equivalent alternative measure, or that the specification nor any alternative measures ore reasonable or appropriate within its environment. When determining if an addressable specification is reasonable and appropriate, the Security Officer has considered the following:

(i) the size, complexity and capabilities of our organization;

(ii) our technical infrastructure, hardware, and software security capabilities;

(iii) the costs of security measures; and

(iv) the probability and criticality of potential risks to our sensitive date. This includes any electronic protected health information.

If, after evaluation by the Security Officer an addressable specification is determined to be appropriate and reasonable, the Security Officer shall implement the security policy and procedure or shall provide explanation of an alternative method for meeting the requirements of the specification.

As described in the standard, alternative methods may sometimes be necessary to reasonably and appropriately implement a specification. Whenever it is determined that an addressable implementation specification is not appropriate or reasonable, documentation will be completed by the Security Officer to identify an equivalent alternative or, in the case of no action taken, identify how the specification has been met or that the specification has no application for the organization. All required implementation specifications are implemented without exception.

4.2.3 Administrative Safeguards

Administrative safeguards are comprised of functions that are implemented to meet the Security Rule standards. They include the assignment of overall security responsibility to an individual, security training and management of workforce members and external persons or entities involved with sensitive data such as EPHI, among other requirements.

4.2.4 Securing / Hardening of Switches Routers and Firewalls

TTHM shall implement procedures by which all switches, routers and firewalls are examined no less than annually. This evaluation will include the following;

(1) Review of appliance firmware and upgrade to latest stable and secure versions

(2) Ensuring hardening standards including password, and multi-factor authentication have been configured to TTHM standards

(3) Replacement and removal of any devices used on the TTHM network *(see Disposal of Paper and External Media - section 6.3)*

(4) Conduct security review for all network devices to insure only approved access is being granted

4.2.5 Encrypted Email

TTHM utilizes its email protection application, and its Secure Messaging feature to exchange sensitive data securely. This feature is enabled for all personnel. When sending an email with sensitive information, staff members only need to add [ENCRYPT] or [SECURE] to the subject line of the email message to encrypt the message.

4.3 MALICIOUS CODE

Policy - Workforce members will receive annual training on the procedures and security mechanisms that are in place to guard against, detect and report malicious software. An emphasis will be placed on workforce members' responsibilities in regard to preventing a malware attack that could lead to a breach of sensitive data such as protected health information (PHI).

Workforce members will be trained to immediately notify the Security Officer if a virus or other type of malware is detected.

Procedure - The Security Officer will periodically check for virus protection and anti-malware software will be installed and updated as appropriate to eliminate or minimize risks to the information system. The Security Officer shall be responsible for maintaining the anti-virus software and operating system software in a current condition (meaning all updates and security patches will be installed in a timely manner as recommended by manufacturer). The Security Officer shall ensure that workforce members are provided with periodic reminders as well as annual training regarding malicious software (see sections 5.10 and 5.11.)

TTHM utilizes Antivirus and Virtual Private Network (VPN) software that protects workstations and servers from cybersecurity threats. This software is installed on all servers and workstations in our environment and is updated automatically. Employees and BAs are prohibited from disabling or removing this software without the express written permission from the System Administrator.

5 Employee/Workforce Responsibilities

5.1 TELECOMMUTING

Telephone Town Hall Meeting - TTHM is a **100% remote based** organization. Telecommuting has become a required capability for many organizations, including TTHM. The advantages of telecommuting are critical for an organization such as TTHM. Telecommuting allows TTHM to work with only the best in our industry. TTHM considers telecommuting to be the primary work arrangement with its employees.

With this in mind this policy is applicable to all employees and business associates, contractors and sub-contractors who work with TTHM. It applies to all users who connect to TTHM/BA network, from **any location.**

While telecommuting is 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 TTHM/BA'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. TTHM expects that the minimum standards listed below to be met by all employees and business associates of TTHM.

5.1.1 General Requirements

All workforce and business associates are required to follow all corporate, security, confidentiality, HR, or Code of Conduct policies that are applicable to other employees/contractors.

- **Need to Know:** Users will have the access based on 'need to know'.
- **Password Use:** The use of a strong password, changed at least every 180 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.
- **Contract Specific:** There may be additional requirements specific to the individual contracts to which an employee or business associates is assigned.

5.1.2 Data Security Protection

Transferring Data**:** Transferring of data containing PHI/PII to TTHM requires the use of an approved VPN connection to ensure the confidentiality and integrity of the data being transmitted. Employees are prohibited from circumventing established procedures when transferring data to TTHM.

External System Access: If employees require access to an external system, they should contact their supervisor. The Security and Privacy Officer or appropriate personnel will assist in establishing a secure method of access to the external system.

E-mail: Employees should not send any sensitive information (CUI, PHI or PII) or other sensitive information via e-mail unless it is encrypted. Employees should contact the Security and Privacy Officer or appropriate personnel if they have questions/issues using email encryption.

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

Protect Data in Your Possession: Employees should view or access only the information they have a need to see to complete your work assignment. If your computer has not been set up with Bitlocker or other hard drive encryption technology, contact the Security and Privacy Officer or appropriate personnel for assistance.

Data Entry When in a Public Location: Employees should not perform work tasks that require the use of sensitive information when they are in a public area, i.e. airports, airplanes, hotel lobbies.

5.1.3 Minimum Hardware Security Protections

Virus Protection**:** Any computer connecting to TTHM's system must be equipped with TTHM-approved, commercial up-to-date Antivirus and Virtual Private Network (VPN) protection products.

Operating System and Updates**:** TTHM requires the use of supported operating systems kept up to date by automatic updates to connect to TTHM resources.

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

Lock Screens**:** No matter what location, always lock the screen before walking away from the workstation. The data on the screen may be protected or may contain confidential information. Be sure the automatic lock feature has been set to automatically turn on after 15 minutes of inactivity.

Multi-Factor Authentication (MFA) - TTHM utilizes Multi-Factor Authentication to access TTHM system resources. Employees and business associates are prohibited from overriding, disabling, or otherwise circumventing this critical security system.

5.1.4 Required Equipment

Employees and business associates must understand that TTHM will not provide all equipment necessary to ensure proper protection of information to which the employee has access. To avoid the need for a paper shredder and lockable file cabinet/safe, keep all documents digitally secure and do not print them. The following lists define the equipment and environment required by TTHM:

5.1.4.1.1 TTHM/BA Provided:

Virus Protection
VPN Software
Bitlocker or similar hardware encryption
Bitraser or similar file destruction software

5.1.4.1.2 Employee Provided:

Broadband connection and fees
Paper shredder
Secure office environment isolated from visitors and family
A lockable file cabinet or safe to secure documents when away from the home office.

5.2 ADDITIONAL EMPLOYEE REQUIREMENTS

Non-Solicitation Agreements - As a condition of employment, all employees are required to sign an Employee Non-Disclosure and Non-Solicitation Agreement with TTHM at the time of hire. TTHM updates its employment agreements from time to time and requires employees to sign and abide by the most current employment agreement as a condition of continued employment. This is typically provided to the employee at the time of employee's performance appraisal. Pay increases and incremental changes to other TTHM-provided benefits may be withheld for employees who do not have a signed current employment agreement on file. As outlined in this handbook and in the Agreement itself, nothing in this provision changes the "at will" nature of the employee's employment relationship.

5.2.1 Workforce Member Responsibility

Workforce members shall be responsible for:

Ensuring compliance with privacy policies applicable to the performance of their duties;

- Participation and completion of compliance related training as outlined in Section 5.10
- Participation and completion of any supplementary compliance related training provided by the **Compliance Manager (section 1.8)**;

- Maintaining the confidentiality of all sensitive information including protected health information;
- Assisting individuals with inquiries regarding the office's privacy policies and procedures; and
- Informing the **Compliance Manager** of any privacy problems as well as suggestions for enhancing privacy policies and procedures. Reports made in good faith shall not result in any retaliatory actions against a workforce member.

Additionally, all workforce members will review the organization's confidentiality statement and sign a confidentiality agreement, regarding sensitive data including protected health information that is used in the performance of their duties.

5.2.2 Workforce Member Access to Sensitive Data

Access to printed and electronic formats of sensitive data such as protected health information (PHI) is provided for all workforce members with the following limitations:

- Workforce members have authorized access to the sensitive data such as PHI that is necessary for the performance of their assigned duties in the organization.
- Access to sensitive data such as PHI shall be limited to the minimum information necessary for assigned duties and responsibilities
- Sensitive data such as PHI access and confidentiality is limited by policy of the organization and the confidentiality agreement signed by each workforce member.

5.2.3 Use and Disclosure of Sensitive Data

Sensitive Data such as Protected health information of individuals that is received and maintained by this office shall be used and/or disclosed by our workforce members for the purposes of treatment, payment and healthcare operations. This includes providing services to covered entities.

The term, "payment, treatment, or healthcare operations", defines how sensitive data such as protected health information may be used or disclosed by our office for the purposes of providing treatment for an individual, collecting payment for treatment, or other necessary uses and disclosures which affect the operations of the covered entities to which we provide services.

5.2.4 Sale of Sensitive Data

The Privacy Rule prohibits the sale of sensitive data such as protected health information without individual authorization. The sale of protected health information includes "any disclosure of sensitive data such as PHI by a covered entity or business associate where the covered entity or business associate directly or indirectly receives remuneration [financial, or non-financial benefit) from, or on behalf of the recipient of the sensitive data such as PHI in exchange for the disclosure." An individual's prior written authorization for such disclosure must include a statement that the disclosure will result in remuneration.

Sale of protected health information does not include a disclosure of sensitive data such as PHI:

- For research purposes where the only remuneration received from the recipient of the sensitive data such as PHI is a reasonable, cost-based fee to cover the cost to prepare and transmit the data (including labor, materials, and supplies for generating, storing, retrieving, and transmitting the sensitive data such as PHI). This exception does not apply to any fees charged to incur a profit from the disclosure.
- Disclosures for public health purposes.
- Disclosures that are required by law.

5.2.5 Minimum Disclosure

The information provided to a subcontractor shall be the minimum necessary information needed for the subcontractor to perform the services listed in the business associate agreement.

5.3 GENERAL INFORMATION TECHNOLOGY

The Company's premises, property, and materials are to be used for TTHM business only and not for any non-Company or personal business ventures or activities.

Information Technology - This Acceptable Use of Information Technology policy sets forth the principles that govern the proper use of TTHM's computer and other technology resources, including but not limited to all TTHM owned or enabled devices, e-mail, voice mail, instant messages, text messages and Internet access. As used in this policy, IT Resources include, but are not limited to, all TTHM owned, licensed, or managed hardware (such as computers, cell phones, land phones, pagers, tables, etc.) and software systems, and all TTHM email accounts created, processed, and stored on TTHM devices, networks, data centers, mobile devices, cloud space and internet connections regardless of their physical location or the form in which they are maintained. IT Resources are the exclusive property of TTHM. As used in this policy, "Data" includes all data such as files, email messages, Internet activity logs, system credentials (such as user name and/or password), etc., whether maintained or stored in electronic or hard copy format. This policy also encompasses all usage of TTHM's network via a physical or wireless connection, regardless of the ownership of the device connected to the internet ("Network").

Ownership - Any and all messages, work product, or other information (including, but not limited to, e- mail, instant and text messages, and voice mail messages) which (1) are created, sent, or received using IT Resources or the Network, (2) relate to the business of TTHM, and/or (3) are stored in property or space owned by TTHM or its clients, are the property of TTHM or its clients. Employees do not own the messages, work product, or other information created, sent or received using IT Resources or the Network, or messages, work product, or other information stored in property or space owned by TTHM or its clients and should not assume that their messages, work product, or other information are confidential or private. Any IT Resources or Data that are owned by TTHM or its clients and in the possession of an employee must be returned to TTHM or its client immediately upon the end of the employee's relationship with TTHM.

5.4 ACCEPTABLE USE

An Employee has no reasonable expectation of privacy while using TTHM or its clients' IT Resources or the Network and neither TTHM nor its client(s) is responsible for the confidentiality of any personal information an employee transmits via IT Resources and/or the Network. TTHM reserves the right to monitor, access, and disclose the contents of or communication on IT Resources, the Network, or Data including employee's e-mail, text messages, instant messages voicemail, etc., at its discretion and at any time. TTHM has the right to access, review, delete, and/or disclose any Data, including but not limited to, files, records or email messages, text messages, voicemail messages, etc., stored on or transmitted through IT Resources and the Network without notice or authorization.

TTHM reserves the right at all times to disclose information about an employee or an employee's use of IT Resources, the Network, or Data to outside parties, including law enforcement and government agencies, if TTHM is required to do so by law or if TTHM has a good faith belief that disclosure is reasonably necessary to

(i) conform to the edicts of the law or comply with legal process,

(ii) protect and defend the rights and property of TTHM,

(iii) act under exigent circumstances to protect the personal safety of TTHM employees, customers, or the public, or

(iv) to satisfy any applicable law, regulation, legal process or governmental request.

TTHM/BA also reserves the right to limit an employee's use of IT Resources, the Network, or Data in order for TTHM to manage network connectivity, security concerns, and emergency/crisis events.

All passwords and encryption keys used on IT Resources or the Network by an employee must be kept confidential. The existence of passwords or encryption does not restrict or impair TTHM's ability or right to access electronic communications. All information regarding access to TTHM's IT Resources or Network, such as user identifications, phone numbers, access codes, and passwords, must be provided upon request and/or termination and is confidential and may not be disclosed to non-TTHM personnel.

Employees shall not (1) share an e-mail password with another person, for any reason, unless explicitly instructed to do so by Human Resources or the COO (2) provide e-mail access to an unauthorized employee, or (3) access another employee's e-mail box without explicit authorization from management. Employees also shall not use the same password in any other place or system outside of TTHM. Passwords must not be inserted into email messages, or any electronic communication.

Employees have a duty to protect electronic information from being inadvertently compromised when using off-site connections. Remote access accounts are considered "as needed" accounts and account activity are monitored. It is the responsibility of any employee with such privileges to ensure a connection is not used by other persons to gain access to TTHM Computing Assets, the Network, and/or Data. All remote connections require two-factor authentication.

IT Resources and the Network may **never** be used to transmit off-color jokes, ethnic slurs, racial epithets, or any joke or comment or image that may be construed inappropriate or disparaging of others based on sex, race, age, religious or political beliefs, disability, national origin, parenthood status, marital status, or any other protected class or characteristic, or which create an intimidating or unprofessional work environment.

Employees may not visit internet sites that contain obscene, pornographic, hateful, or other objectionable material. Employees are responsible for all behaviors performed on TTHM IT Resources and the Network under his or her assigned credentials. Employees should always sign out of their account before leaving a workstation.

Within the limits set forth in this policy, limited personal use of IT Resources or the Network is permissible so long as the personal use does not interfere with the intended functioning of the IT Resources and Network or the performance of any employee's job duties. Employees are responsible for exercising good judgment regarding the reasonableness of personal use.

Employees may not upload, download, or otherwise transmit commercial software or any copyrighted materials except in accordance with the material's end employee license agreement. Employee may not download, install, or run any applications unless explicitly authorized to do so by an authorized Company representative. Employees may not modify any physical or logical configuration of any IT Resources without prior written authorization. Employees may not introduce any removable media or mass storage device to IT Resources or the Network unless the media's origin, ownership, and contents have been validated as being legitimate and are directly associated with the Employee's official job description.

Data should always be stored on the Network. Data should be transferred to storage or portable devices only when absolutely necessary, and then only with prior written approval from your direct supervisor. In the case where it is necessary to transfer data to portable devices, those devices must be TTHM or client owned devices.

Employee shall immediately report any suspected or confirmed information technology security incident, compromise, or abnormality to the CEO, COO or Director of Operations & Privacy Officer, such as malware pop-ups, virus warnings, or suspected attempts to gain unauthorized access to a Computing Asset.

Any Computing Assets assigned by TTHM to an employee are expected to be cared for and safeguarded against damage, loss, theft, and other harmful activities. Should any of this, or other, Company property be lost, damaged, stolen or otherwise compromised, employees are required to notify their direct supervisor immediately. Any devices that are discovered to be acting erratically or deemed to be compromised must be immediately quarantined and/or removed from the network until reasonable determination can be made as to whether the device has been compromised. Likewise, any employee's system credentials (usernames and/or passwords) that are suspected of being compromised shall be changed and/or disabled immediately.

Disabling or compromising, or attempting to disable or compromise, the security of information on IT Resources or the Network is strictly prohibited. Unless the prior approval of management has been obtained, employees may not establish Internet or other external network connections that could allow unauthorized persons to gain access to TTHM's systems and information.

5.5 WORKFORCE SECURITY

Policy - Workforce security is a standard with three addressable implementation specifications. Workforce security procedures have been developed to ensure that all authorized workforce members have appropriate access to sensitive date such as EPHI and prevent access by those who are not authorized.

Procedure - The Security Officer is responsible for determining whether the implementation specifications are reasonable and appropriate. Whenever it is determined that an addressable implementation specification is not appropriate or reasonable, documentation will be completed by the Security Officer to identify an equivalent alternative or, in the case of no action taken, identify how the specification hos been met or that the specification hos no application for the organization. Any alternative methods of compliance will be recorded in the Security Risk Analysis

5.6 AUTHORIZATION AND/OR SUPERVISON

Policy - Authorization allows certain individuals or entities to access the organization's information system, or locations where sensitive data such as EPHI may be accessed, without direct supervision of their activities. *Supervision* is required for individuals or entities that the Security Officer hos determined should not have access to the organization's information system, or locations where sensitive data such as EPHI may be accessed, without direct observation of their activities.

Procedure - The Security Officer is responsible to approve access to information systems or locations where sensitive data such as EPHI may be accessed. If authorization is not appropriate, the Security Officer is responsible for determining whether a workforce member or other individual should be supervised when working in a location where sensitive data such as EPHI may be accessed. If supervision is not reasonable. another method of preventing access will be implemented.

5.7 COMPANY-ISSUED EQUIPMENT – TTHM

While employed with TTHM, employee will have access to TTHM electronic equipment, including but not limited to computers, mobile phones, pagers, hardware and software, (collectively, “Equipment”). All Equipment provided to employees are intended for business use.

The use of TTHM Equipment is subject to all of the Company’s policies and procedures, including, but not limited to, TTHM’s policies:

- protecting certain Confidential Information related to the Company’s operations;
- safeguarding Company property and appropriate use of Information Technology; and
- providing for Equal Employment Opportunity, including by prohibiting discrimination, harassment or retaliation.

Documents, files or data created or stored on TTHM's Equipment are the property of TTHM, as are any passwords or passcodes necessary to access that information.

All Equipment provided to employees, including all accessories belonging to any specific type of Equipment, needs to be returned to Human Resources in good working condition upon last day of employment or any time its return is requested. Should an employee fail to keep or return the Equipment in good working condition, the employee may be held liable for the full replacement cost of the Equipment, as outlined in the Technology Equipment Use, Care & Responsibility Agreement Equipment form.

5.8 COMPANY RECORDS AND FILES

All records, files, plans, documents and the like relating to the business of the Company employees prepare, use or come in contact with shall be and shall remain the sole property of the Company and may not be copied without written permission of the Company and shall be returned to the Company on termination or cessation of your employment, or at the Company's request at any time.

5.9 CONFIDENTIAL/SENSITIVE INFORMATION

Each employee's relationship with TTHM and its clients is one of trust and confidence. Because of the nature of employee's duties, employee will have access to sensitive business information critical to the business operations of TTHM and its customers.

Employee will also have access to sensitive and confidential information belonging to TTHM's customers as a result of their employment with TTHM. Such information is the sole property of the customer and Employee shall not under any circumstance disclose such information to anyone absent the customer's explicit consent or Court order. This paragraph does not prevent Employee from disclosing information necessary for TTHM or its employees to conduct its business with the customer. Any compromise or potential compromise of confidential information should be reported immediately to the employee's direct supervisor.

5.10 SECURITY AWARNESS AND TRAINING

Policy - The organization shall implement an annual training program that addresses security reminders, protection from malicious software, log-in monitoring, and password management. Training will be provided to **all** staff members and, when applicable, technical support personnel or business associates.

The Security Officer will ensure that all members of its workforce, including management, are aware of security issues and are adequately trained. Security training requires education concerning the vulnerabilities of the confidential information maintained by the organization and the organization's policies and procedures to protect it. Training will also include the method that workforce members are expected to use to report security incidents. **Training records should be kept for a minimum of six years.**

Procedure - The Security Officer will implement initial and subsequent annual training for security awareness. The

training will mainly be comprised of the material provided in the **TTHM Information Security Policy** with a focus on the information highlighted within **TTHM Security Policy Handbook**. Additional training information that is specific to the organization will be provided by the Security Officer to include site specific information, such as expected reporting methods. **Documentation shall be maintained for a minimum of six years to meet requirements of the Security Rule.**

5.11 SECURITY REMINDERS

Policy - Workforce members will be provided with periodic reminders of their responsibilities regarding the security of sensitive data such as EPHI. The annual training shall also be used as a reminder of security responsibilities.

Reminders of workforce security responsibilities can be accomplished through discussion in meetings, annual security training, and the posting or discussion of articles or information related to security. Any identified security incident should be quickly communicated, including any corrective action to prevent re- occurrence of a similar incident. The organization should document all security reminders as well as annual training.

Procedure - The Security Officer shall be responsible for providing periodic security reminders to workforce members about their responsibilities for security of the organization's sensitive data such as EPHI.

5.12 WORK PERFORMED ON PERSONAL DEVICES (BYOD)

In the modern era it is quite common for employees to user their own personal devices to perform company business. This is referred to as BYOD (Bring Your Own Device). With this in mind, employees who use their personal devices (cell phones, laptops, etc.) to perform Company business should be aware that ***electronic data*** related to such company business is the sole and exclusive property of the Company, just as with the electronic data accessed, created, or stored on Company-issued devices, and is subject to all policies and procedures concerning Company property, including the Company's right to demand access to that information at any time for any reason. This policy does not give TTHM the right to review *ANY* personal information stored on BYOD devices, but rather only company-related information which is not accessible by other means.

5.13 WORKFORCE CLEARANCE PROCEDURE

Policy - The organization will, at a minimum, perform a check of references and search the OIG Exclusions Database for prospective employees who will have access to sensitive data such as EPHI in the performance of their duties. Additional background checks will be at the discretion of management and the Security Officer. The Security Officer will *use* the information gathered to determine whether granting the prospective employee access to sensitive data such as EPHI will be appropriate. This is on addressable implementation specification and allows on organization to determine if it is reasonable and appropriate for their setting. Clearance is only to be granted by the Security Officer. Personnel who will have access to sensitive data such as EPHI and to locations where sensitive data such as EPHI may be accessed will be cleared prior to beginning their assigned duties.

Procedure - The Security Officer will determine the level of workforce clearance needed for the organization. The Security Officer may elect to utilize existing procedures from the organization's personnel policy manual or new hire procedures to accomplish the process of checking references and/or obtaining background information on prospective employees. The Security Officer will also perform a search for prospective employees in the Office of Inspector General {OIG) Exclusions Database. Finally, the Security Officer will periodically revalidate a workforce member's clearance by performing another search for the individual in the OIG Exclusions Database. Revalidation should be performed at least annually. Documentation of initial workforce clearance and revalidation shall be maintained in the employee's personnel file.

5.14 WORKFORCE / EMPLOYEE TERMINATION

Policy - The Security Officer will implement procedures for terminating access to sensitive data such as EPHI when the employment or contract with a workforce member ends or their assigned duties change their need to access sensitive data such as EPHI. The same will be performed if a business associate or subcontractor relationship is terminated.

The objective is to prevent access to sensitive data such as EPHI by those who ore no longer authorized to access the data (i.e., they may have left the organization or have been reassigned to another position). The organization will document and provide communication of each termination to the Security Officer who will ensure that termination procedures are followed. It is important to clearly define and then document the responsibilities of designated staff members to ensure that termination procedures ore carried out completely and in a timely manner.

Procedure - The Security Officer will ensure that there is timely communication from supervisors, the personnel deportment, and others, regarding the termination of workforce members and entities with access to the organization's sensitive data such as EPHI.

For example, when a staff member's employment is terminated, their unique identification or other means of access will be disabled so that they or someone else cannot gain access to sensitive data such as EPHI with that user ID and password. The Security Officer will also coordinate with management to ensure the termination of an individual's ability to access the physical location where sensitive date such as EPHI is stored (i.e., through the use of keys, key codes, access badges or alarm codes).

6 Protocols for Devices and Media

6.1 WIRELESS USAGE STANDARDS AND POLICY

Extreme care should be taken when connecting to shared wireless networks (public waiting spaces, hotels, coffee shops, etc.) Use of these networks should be limited and should never should be used to connect to TTHM's network resources, without the use of VPN.

6.2 USE OF TRANSPORTABLE MEDIA

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

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

The use of transportable media in various formats is common practice within TTHM/BA. All users must be aware that ***sensitive data*** could potentially be lost or compromised when moved outside of TTHM/BA networks. Transportable media received from an external source could potentially pose a threat to TTHM/BA networks. ***Sensitive data*** includes all human resource data, financial data, TTHM/BA proprietary information, Personally Identifiable Information ("PII"), and personal health information ("PHI").

USB key devices are handy devices which allow the transfer of data in an easy to carry format. They provide a much-improved format for data transfer when compared to previous media formats, like diskettes, CD-ROMs, or

DVDs. The software drivers necessary to utilize a USB key are normally included within the device and install automatically when connected. They now come in a rugged titanium format which connects to any key ring. These factors make them easy to use and to carry, but unfortunately easy to lose.

Rules governing the use of transportable media include:

> No ***sensitive data*** should ever be stored on transportable media unless the data is maintained in an encrypted/secure format.

TTHM 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 transportable media.

When no longer in productive use, all TTHM laptops, workstation, or servers must be wiped of data in a manner which conforms to applicable regulations and in accordance with the "**DISPOSAL OF EXTERNAL MEDIA / HARDWARE**" policy identified in Section 6.3. All transportable media must be wiped according to the same standards. Thus, all transportable media must be returned to the Security and Privacy Officer or appropriate personnel for data erasure when no longer in use.

6.3 DISPOSAL OF PAPER AND EXTERNAL MEDIA

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.

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

Disposal of Electronic Media: All external media must be sanitized or destroyed in accordance with compliance procedures, as outlined in Section 6.3.1 of this document. Do not throw any media containing sensitive, protected information in the trash.

6.3.1 Disposal of Electronic Media

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.

7 Security Management Process

7.1 SECURITY RULE

This section of the HIPAA Compliance Manual addresses requirements of the Security Rule, as published in the Federal Register February 20, 2003, and the Omnibus Rule, as published in the Federal Register January 25, 2013.

7.2 APPLICABILITY

The Security Rule applies to all covered entities and business associates that transmit protected health information in electronic form in connection with a transaction under the Rule. The Security Rule is consistent with the Privacy Rule, in that its purpose is to safeguard sensitive data such as protected health information (PHI). However, the scope of the Security Rule is limited to electronic protected health information (EPHI), whereas the reach of the Privacy Rule policies also extends to written and other forms of patient information.

7.3 SECURITY MANAGEMENT PROCESS

Policy - The Security Management Process is comprised of four required implementation specifications. The documentation from the organization's risk analysis will provide an initial record of the security status of the organization, and corrective actions that will minimize identified risks to sensitive data such as EPHI. Subsequent or repeat risk analyses will evaluate the effectiveness of security measures and identify any necessary corrective actions.

Procedure - The Security Officer shall ensure that the procedures for annual risk assessment are completed and repeated, if necessary, with the frequency noted in individual procedures.

7.4 RISK ANALYSIS

Policy - An initial and periodic or subsequent risk analyses of the organization's security processes shall be performed to identify the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information collected and maintained by the organization.

The risk analysis is not a one-time process. An initial security risk analysis will be completed and then periodically repeated to determine if security measures ore adequate or need improvement. The risk analysis requires consideration of all potential risks to any sensitive data including EPHI and "relevant losses" that might be encountered if security measures are not in place. The risk analysis is an item-by- item review of the Security Rule's implementation specifications to determine how best to protect the confidentiality, integrity, and availability of sensitive data including EPHI that is created, received, maintained, or transmitted by the organization.

In order to effectively address risk to sensitive data such as EPHI, the organization must create on inventory or asset listing that includes:

- All components of the information system, including hardware and software;
- All electronic devices that store sensitive data such as EPHI, such as desktop computers, laptops, tablets, smart phones, cameras, copiers: and
- All portable media, such as thumb drives, mobile hard drives, magnetic tape disks, digital memory cords, etc.

The elements of a risk analysis include:

(a) a listing of the specifications that were addressed;

(b) findings (what measures in place to eliminate or minimize potential risk, and is the item considered a current risk to sensitive data such as EPHI);

(c) a reference to current applicable policies and procedures: and

(d) a reference (if applicable) to corrective actions, assignments and/or deadlines for developing appropriate policies and procedures (this information should be recorded in the "Corrective Actions" section of the Security Risk Analysis document).

Periodic or repeat risk analyses are conducted to identify whether policies and procedures continue to adequately protect sensitive data such as EPHI and meet current regulatory requirements. The analyses will identify any corrective actions or policy modifications that ore necessary.

Procedure - The Security Officer will conduct an accurate and thorough initial assessment or risk analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information collected and maintained by the organization. An asset listing or inventory will be established to ensure that all systems, devices and media that receive, transmit or store sensitive data including sensitive data such as EPHI are considered during the analysis.

Periodic analyses (to be conducted at least annually) will be completed to monitor the current status of compliance and identify the need for modification of security measures due to changes in regulations, the organization's environment and/or technology employed to handle and maintain sensitive data such as EPHI. The Security Officer shall maintain a copy of all risk analyses and supporting documentation for a minimum of six years.

7.5 RISK MANAGEMENT – RISK REGISTER

Policy - Potential security risks to sensitive data such as EPHI shall be identified by the initial and periodic risk analyses. The risk analyses shall be the primary tool to manage the overall security of the organization's sensitive data such as EPHI. The Security Officer is responsible for risk management by ensuring the implementation of security measures sufficient to reduce risks and vulnerabilities that were identified during the analysis to a reasonable and appropriate level (based upon the size and complexity of the organization) to comply with the General Rules of the Security Rule.

Ongoing risk management is achieved by enforcement of current policies and procedures and their modification due to changes in the organization or regulatory requirements. The need for modification will be identified through periodic risk analyses.

Procedure - Security risks to sensitive data such as EPHI maintained by the organization are managed and minimized through the use of the initial and periodic risk analyses, including periodic technical assessments of the organization's information system and implementation of security policies and procedures. The Security Officer shall utilize the results of the periodic risk analyses to determine if security policies and procedures are effective or require modification. Necessary modifications will be made to ensure the continued security of sensitive data such as EPHI that is collected and maintained by the organization. Corrective actions, if any are identified during a given risk analysis, will be noted in the "Corrective Actions" portion of the risk analysis document.

7.6 ANNUAL RISK ASSESSMENT

Statement of Policy

To ensure TTHM conducts an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of ***sensitive data*** held by TTHM.

TTHM shall conduct an accurate and thorough risk analysis to serve as the basis for TTHM compliance efforts. TTHM shall re-assess the security risks to its ***sensitive data*** 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 Officer shall be responsible for coordinating TTHM risk analysis. The Security Officer shall identify appropriate persons within the organization to assist with the risk analysis.

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

   i. Document TTHM current information systems.

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

b) List of all system users with remote access capabilities including VPN, email, and application.

c) Identify and document threats to the confidentiality, integrity, and availability (referred to as "threat agents") of ***sensitive data*** created, received, maintained, or transmitted by TTHM/BA. 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 TTHM/BA'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 ***sensitive data***, modification of ***sensitive data***, 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.

c. Determine and document probability and criticality of identified risks.

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

a. "Very Likely" (3) is defined as having a probable chance of occurrence.

b. "Likely" (2) is defined as having a significant chance of occurrence.

c. "Not Likely" (1) is defined as a modest or insignificant chance of occurrence.

ii) Assign criticality level.

a. "High" (Tier 1) is defined as having a catastrophic impact on business operations

b. "Medium" (Tier 2) is defined as having a significant impact on business operations

c. "Low" (Tier 3) is defined as a modest or insignificant impact on business operations

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

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.

ii) Determine timeline for implementation.

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

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

v) Make necessary adjustments based on implementation experiences.

vi) Document actual completion dates.

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

C. The Security Officer shall be responsible for identifying appropriate times to conduct follow-up evaluations and coordinating such evaluations. The Security Officer shall identify appropriate persons within the organization to assist with such evaluations. Such evaluations shall be conducted upon the occurrence of one or more of the following events: changes in regulations; new federal, state, or local laws or regulations affecting the security of ***sensitive data***; changes in technology, environmental

processes, or business processes that may affect security policies or procedures; or the occurrence of a serious security incident.

7.7 EVALUATION

Policy - The organization shall conduct a periodic technical and nontechnical evaluation of its security policies and procedures to determine their effectiveness and whether modifications are necessary.

The organization will review its security policies and procedures whenever major changes occur (in the organization or regulatory requirements) and not less than at one-year intervals. The evaluation process will include a review of all components of the safeguards: administrative, physical, and technical.

The purpose of the evaluation is to periodically review the organization's security policies and procedures to determine

a. if the organization mode any changes that would require security modifications, such as major technology or environmental changes which affected the security of sensitive data such as EPHI,

b. if there have there been any changes to the regulatory requirements that would necessitate revisions,

c. if there have been any known security problems

Procedure - The Security Officer shall schedule a periodic evaluation of the organization's security policies and procedures to determine their effectiveness and the need for modifications. The nontechnical evaluation shall be conducted on an annual basis, as part of the organization's security risk analysis. The technical evaluation of workstation/network security should be repeated as needed to address environmental, technical or operational changes affecting the security of sensitive data such as EPHI. Required modifications to policies and procedures will be implemented as soon as possible following the review.

7.8 SANCTION POLICY

Policy - Appropriate sanctions will be applied when workforce members (including management and officers) fail to comply with the security policies and procedures established by the organization.

Sanction policies are the penalties that would be imposed on individuals for failure to comply with the organization's security policies and procedures. The severity of a penalty is based upon the potential risk to the organization's sensitive data such as EPHI. Other considerations such as repeat offenses, intent, and actual impact of the violation are also considered when determining the penalties to be imposed.
Sanctions or penalties can range from verbal correction, to written reprimand, to suspension from work (for a period of time), to dismissal from the organization.

Notice of the organization's sanction policy is provided to all workforce members to ensure their understanding of consequences for non-compliance with the organization's policies. Notice is included in the confidentiality

statement that each workforce member is asked to sign, as well as the Workforce Member HIPAA Training Handbook.

Procedure - Specific sanctions or penalties shall be imposed for security incidents that place sensitive data such as EPHI at risk and/or are identified as a violation of the organization's HIPAA policies and procedures. Specific sanctions are listed in section 13.8.1 of this manual. Sanctions shall be reviewed and updated, as necessary.

7.8.1 HIPAA Sanctions

Appropriate sanctions must be applied when workforce members (including management and officers) fail to comply with the organization's privacy and security policies. The severity of a penalty is based upon the potential risk posed to protected health information (PHI). Other considerations such as repeat offenses, intent, and actual impact on PHI will also help determine the appropriate penalty to be imposed.
Sanctions can range from verbal correction (or retraining), written reprimand, suspension of information system/PHI access (for a period of time), to dismissal from the organization. The actual sanction to be imposed for a specific incident shall be determined by the Security Officer, Compliance Manager or other management personnel.

A standard set of sanctions is provided in the following section (7.8.2). The Compliance Manager and Security Officer shall review the set of sanctions on an annual basis, and update the list if necessary.

Notice of the sanction policy shall be provided to all officers, employees, and contractors to ensure their understanding of actions that may be taken for failure to comply with the organization's privacy and security policies.

7.8.2 HIPAA Sanction Examples

The Security Officer, Compliance Manager and other management personnel shall impose the sanction(s) that they determine to be appropriate, considering the severity of the incident, the intent of the workforce member, and the number of prior incidents in which the individual has been involved.

- A verbal reprimand shall be imposed for incidents that are deemed to be minor, and for first occurrence of an incident by an individual.
- A written reprimand shall be imposed for incidents that are a repetition of an incident, or a different incident that involves the same individual.
- A workforce member may be temporarily suspended from work to prevent him/her from accessing protected health information, for a length of time to be determined by the Security Officer or Compliance Manager. The length of the suspension will be dependent upon the type and the severity of the incident and/or the repetition of offenses by the individual.
- A workforce member may be terminated from the organization for malicious or other serious failure to follow HIPAA policies and procedures implemented by the organization.