TTHM Security Policy Handbook 2024 v2.3

From: **Ian Cerveny, Operations Director**

TTHM Security & Privacy Officer

To: **All TTHM Employees, Vendors and Subcontractors**

The current members of the TTHM 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

This TTHM Security Policy Handbook includes critical sections of the TTHM Security Policy. For additional details, refer to the Security Policy itself. If you have any questions, concerns or are lacking the requirements detailed in this Handbook and in the Security Policy, reach out to a member of the Compliance Committee immediately for assistance.

Security Policy Basics (TTHM Security Policy Sections 1.1, 1.2, 1.3)

The policy provides sales, executive and production staff within Telephone Town Hall Meeting (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.

Included are definitions of terms and roles, scope of the policy, and applicable regulations.

This handbook should be considered supplemental to the full Security Policy, not a suitable replacement for reading and comprehending that policy in full. It is recommended that TTHM employees familiarize themselves with the Security Policy sections referenced in this Handbook.

Protected, Secure & Confidential Information Handling (TTHM Security Policy Section 2.1)

Access to Confidential Information provided by clients or event participants to facilitate TTHM outreach events and services will be granted to TTHM employees and vendors as-needed. All Confidential Information received directly or cultivated as a result of producing events or providing services must be protected in accordance with the TTHM Security Policy and HIPAA.

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.

Importantly, all Confidential Information must be protected before and during event production and/or as services are rendered. Then all digital and physical copies of that information must be destroyed within one (1) month of completion of the related event or service. Employee and Vendor Non-Disclosure Agreements specify this tenet of our policy.

Notification of Confidential Information (TTHM Security Policy Section 2.1)

TTHM Schedulers will note events and services where Confidential Information will be distributed to TTHM employees and/or vendors. Distribution of that information will be prefaced by the following notice:

Data and documents provided to facilitate this outreach event or service contain Confidential Information. Protection and subsequent destruction of this information in all physical and digital formats is required in accordance with the TTHM Security Policy, section 2.1.2.

Data Access & Removal Notes (TTHM Security Policy Section 2.1)

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.
Data used to facilitate events and services where potential PHI/PII/CUI/PPI is involved must be scrubbed from TTHM systems, computers and devices 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.

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.

Password Guidance (TTHM Security Policy Section 2.4)

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.

TELECOMMUTING (TTHM Security Policy Section 5.1)

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.

General Requirements (TTHM Security Policy Section 5.1.1)

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.

Data Security Protection (TTHM Security Policy Section 5.1.2)

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.

Minimum Hardware Security Protections (TTHM Security Policy Section 5.1.3)

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.

Required Equipment (TTHM Security Policy Section 5.1.4)

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:

(TTHM Security Policy Section 5.1.4.1.1)

TTHM/BA Provided:

Virus Protection

VPN Software

Bitlocker or similar hardware encryption

Bitraser or similar file destruction software

(TTHM Security Policy Section 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.

Sanctions (TTHM Security Policy Section 7.8)

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.

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.