POLICY AND GUIDELINE

TOMAH HEALTH

Tomah, Wisconsin 54660

EFFECTIVE DATE: 07/14/2023
DIVISION: Administration
P.G: 100-GEN-001
TITLE: Confidentiality, Security of Information
ORIGINATION DATE: 03/79

_____ DATE: _____
Author

Approved By: _____ DATE: _____
Author

_____ DATE: _____
Author

_____ DATE: _____
Administrative Team Leader

INVOLVES

Hospital Wide

PURPOSE

To provide awareness of the importance of information security and confidentiality and to authorize and require agreements with individuals and external entities to protect Company information resources, including confidential patient, employment, and operational information.

POLICY

Tomah Health (TH) respects each individual's right to confidentiality in communications and records concerning their care, treatment or employment. (This includes communication in person, written, oral, e-mail, etc.) This policy applies to the use of all information, electronic and computing devices, and network resources used by TH to conduct business or interact with networks and business systems, whether owned, leased by, or otherwise in the custody or control of TH, the employee, business associate, or a third party.

GUIDELINES

Definitions:

Protected Health Information (PHI): "any information, whether oral or recorded in any form or medium" that

- " created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse"; and

- "relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual."

Confidential Information: Information whose unauthorized disclosure could be prejudicial or harmful to the interest of the patient, employee, provider or to TH. Examples include, but are not limited to, patient-identifiable clinical information, peer review, financial, and administrative data.

Computer Resources: This term refers to TH's entire computer network. Specifically, computer resources includes, but not limited to: host computers, file servers, application servers, communication servers, mail servers, fax servers, Web servers, workstations, stand-alone computers, laptops, mobile devices, software, data files, and all internal and external computer and communication networks (for example, Internet, commercial online services, e-mail systems) that may be accessed directly or indirectly from our computer network.
Users: This term refers to all employees, independent contractors, consultants, volunteers, temporary workers, medical staff, and other persons or entities that use our computer healthcare resources for hospital approved access.

Because all information must be held in strict confidence, violation will result in disciplinary action up to and including termination.

A. Confidentiality of health care, employment, personal, and operational information.

1. Each employee, member of the medical staff, allied health professional staff, volunteer, independent contractor, vendor, student, or instructor is responsible to maintain the confidentiality of each individual's health care, employment, personal and operational information protecting that information against loss, defacement, tampering, or use by unauthorized individuals.
2. The patient is assured confidential treatment of his/her healthcare information. Information concerning a patient's condition is confidential, and may be disclosed by staff specifically authorized to do so. This applies also to communication with the patient himself. Refer to "Release of Patient Information" policy and in compliance with HIPAA Guidelines. Patients will be asked upon admission their privacy wishes in accordance with HIPAA guidelines. Their privacy wishes will be entered into the Information system. The patient will also be issued a Notice of Privacy Practices, if required.
3. Confidential information is defined as verbal communications, written records, observations, or computerized information (including, but not limited to: e-mail, faxing, medical records, billing information, etc.).
4. Emphasis must be placed on protection from damage by fire or water. General and specific safety precautions must be followed in all areas in which records are kept.

5. Each employee is responsible to maintain the confidentiality of health care, employment, personal and operational information. Unauthorized access, use, or release, including inappropriate handling of confidential information by a hospital employee, student, member of the professional staff, volunteer, or vendor could lead to disciplinary measures up to and including termination of employment or business relationship.

6. State, Federal, and HIPAA laws protect health care information. Employees, who inappropriately access, use, or release confidential information, may also face civil and/or criminal penalties.

7. All written or computer-based material containing confidential information is to be kept in a secure location within the organization's jurisdiction. This material may not be removed from the facility, except by authorized persons acting in accordance with a court order or with Administration's approval on a case-by-case basis.

8. Confidential information is only available to authorized users, based on a job-related need to know basis.

9. All employees, volunteers, students and clinical students, and job-shadowing are required to attend HIPAA General Awareness Training during the orientation process or a designated alternative activity.

B. Confidentiality of information when employees are patients.

1. Employees and members of the medical or professional staff are on occasion our patients. It is imperative that they are afforded the same right of confidentiality as all other patients. Access is limited to authorized users, based on their job-related need to know basis.

2. Employee's employment health care information is available through the Employee Health. Employers will only have access to the employee’s worker’s compensation information in regards to the portion of the medical record that directly relates to the claim.

C. Confidentiality of verbal information.

1. Verbal discussion of confidential information should not take place outside the work area. The greatest risk of unauthorized disclosure occurs with verbal exchanges. Gossip is not professional. It gives the appearance of treating confidential information casually, can damage a personal reputation and that of the hospital, and can result in disciplinary action up to and including termination of employment.

2. Patient information will not be discussed among staff members unless consultation regarding patient care is necessary. Patient information will not be discussed with the public. Under HIPAA regulations the wrongful use or disclosure of any PHI could result in Civil or Criminal penalties that include fines and/or imprisonment.

D. Unauthorized release or handling of confidential information.

1. Peer correction is encouraged and expected. It can be an effective way to educate and to curtail inappropriate handling of confidential information. Incidents should be referred to the supervisor and/or an incident report should be completed using our incident reporting system.
2. Individuals who are aware of unauthorized release of inappropriate handling of confidential information should contact their Supervisor, Corporate Compliance Officer, Administration, Privacy Officer, Security Officer or the Compliance Hotline and/or an incident report should be completed using our incident reporting system.
3. An individual who believes that their personal confidential information has been released inappropriately should be referred to the Privacy Officer, Corporate Compliance Officer, Administration, or the Security Officer.
4. Do not release patient information to anyone not directly involved in the patient's care. Any information released to the patient, and his/her family, will be by the provider or his/her designee.

E. Office/File security

1. All offices and files containing confidential patient information are to be kept locked at all times when personnel are not present. Only authorized personnel can have access to these areas.

HIPPA during an emergency or disaster

HIPAA is not generally waived during an emergency or disaster. Tomah Health proactively protects patient information at all times. However, certain information can be shared during emergency events if the protected health information is disclosed for public health emergency preparedness purposes. Review the HIPPA disclosure flow chart for consideration.

HEALTH INFORMATION SERVICES (H.I.S.)

A. Health Information Services Office is to be kept locked. Only authorized personnel will have access to those areas.

B. Your name badge will be activated to access HIS if it is determined that an employee would need this function in order to perform his/her duties. The activation of your name badge will be determined by HIS Director.

HOSPICE AND PALLIATIVE CARE

A. Patient care records will be secured and confidentiality will be maintained at office sites and in transport. (e.g. in a locked computer, laptop, or file) Computers will be locked when unattended. Laptops will be locked and secured when unattended and locked in the car or trunk of vehicles for transport.

B. Members of the Hospice and Palliative Care teams have access to patient information and the electronic medical record and strict confidentiality will be maintained.

C. Members of the Hospice or Palliative care teams may make and take copies of a portion of the electronic medical record from the office or site to the location of care, if necessary to provide care. .i.e. for use on admission. Copies must be secured in a locked car, positioned to maintain confidentiality at all times, (face down, no wording visible to passerby), and returned after use for disposal.

D. Staff need to be sensitive to the potential for a break in confidentiality with telephone calls, answering machines, and the use of cellular phone, and also any names on reports, work sheets, or materials left unattended at their stations.

PHARMACY SERVICES

A. A patient's record from the pharmacy may be used for educational purposes and research programs. The use of patient protected health information should be approved purposes of research prior to usage. There are four ways to perform HIPAA – compliant research. They are:
   1. Obtain patient authorization.
   2. Obtain a waiver of authorization from the IRB or Privacy Board.
   3. Use de-identified information.
   4. Use a limited data set.

B. A record shall be maintained identifying which profiles were examined, and the personnel outside of pharmacy personnel who have had access to these profiles.

Please review our E-mail and Internet policy for specific guidelines and recommendations.

COMPUTERIZED SYSTEMS

There are major security and confidentiality concerns resulting from the computerization of TH **and/or patient information.** They are as follows:

Access:

Access/role change/termination to computer-based information systems is based on notification by Human Resources (HR) upon employment based on role based which is approved by Department Director to Information Technology Services (IS). Access is based on the role of the employee in our facility as determined by the Department Director and should be limited to meet job functions.

Department Director may request temporary/permanent access to resources based on individual need by generating a help desk ticket to IS. IS will maintain an electronic document tracking access to resources which is forwarded to HR upon termination.

Confidentiality:

The Information systems at TH make available a large amount of confidential information including patient health information. As a result, our obligation to maintain and assure the utmost in confidentiality has been magnified.

Employees must regard computers as tools that are to be used for direct execution of the employee's job and not for personal or curiosity use. Each user authorized for computer access is allowed to seek information only as it relates to the user's normal duties. Solicitation of information from the system when it does not directly relate to the user's normal duties will be regarded as a violation of the TH's confidentiality policies.

It is important to note that the information systems may maintain an audit trail of accesses to information by user. This audit trail could be examined on a regular basis through authorized TH personnel for breaches in confidentiality and security.

Security:

Individual security codes are issued to authorize users by IS for each computer system. These codes give an individual user access to the data contained within the system(s). The information that is in the systems must be kept secure in order to maintain the integrity of the databases.

The computer systems may monitor access to the various components of the system according to these individual security codes. Each authorized computer user will be held responsible for the use or misuse of his/her own security code(s).

Examples: Letting an employee use your security code to perform work is an example of inappropriate use. Leaving a computer workstation unlocked and still logged into an application.

When finished with a function, you must log out of (i.e. exit) the computer system so that another person cannot perform any functions using your security code. If you find the system in the middle of a function, attempt to locate the user and have that person log out of the system before you log in. If the user cannot be found, secure the system until the user returns or, if it can be done safely, terminate the function and then log into the system using your own security code. Using another person's security code to perform system functions is considered a breach of system security.

Passwords: Strong passwords (eight to ten characters, both alpha & numeric characters and a special character) are recommended for users. The user should not use understandable words (i.e. dictionary or activity, or information, etc) as their complete password (append a meaningless number to it. The information system will prompt users to change passwords regularly and the Information system will automatically log users out after defined inactivity.

Security code(s) should be kept in a safe place. Specifically, this means not attached to your computer terminal. Do not list a code with any other information that identifies the system to which the code allows access. Report any loss of a document containing your code(s) or any breach of security immediately to your Supervisor or IS Department. The security of your code(s) is the employee's responsibility.

Screen saver passwords: Users are encouraged to log out all systems and applications when they are going to be away from their computer for an indefinite amount of time. Network group policy will activate the screen saver due to inactivity unless exemption has been granted due to patient care/department needs. **Mobile Storage:** PHI information will not be stored on mobile storage such as laptops, USB drives, smart phones unless properly encrypted.

Responsibility of Users When Using Computer(s) and Computer Software

Users may not deliberately perform acts that waste computer resources or unfairly monopolize resources to the exclusion of others. These acts include, but not limited to, sending mass mailings or chain letters, spending excessive amounts of time on the Internet, playing games, engaging in online chat groups, printing multiple copies of documents, or otherwise creating unnecessary network traffic.

Every user of a computer system is to utilize only licensed software, purchased and owned by this institution. This means absolutely no unauthorized software is to be used on any TH computer system. These acts include, but not limited to, a user should not copy software for use on their home computers, provide copies of software to any independent contractors or customers, and/or download any software from the Internet or other online service to any TH computers/servers. Users who become aware of any misuse of software or violation of copyright law should immediately report the incident to their supervisor and/or IS Department.

In addition, each user is responsible for making sure their data is properly backed up according to departmental policy. Contact the IS Department for further assistance in formulating a secure data backup policy.

Responsibility after Termination of Employment

After a user has terminated employment with TH, all information, materials, software, and/or equipment related to the use of TH computer systems must be returned, if applicable, to the department supervisor. HR Department will send termination notification to IS Department within one business day. If HR department is unavailable, the department supervisor must directly contact IS Department.

Some Examples of Breaches of Confidentiality:

1. "Carelessness or Unintentional"
    - Leaving a computer workstation unsecured before going to lunch.
    - Carelessly access the wrong patient's information.
    - Carelessly discussing confidential information in a public area and it's overheard by someone.
    - Accidentally faxing information to the wrong location.
    - Accidentally leaving a laptop/hospital issued smartphone containing hospital information unattended in a public setting.
    - Throwing patient information in the regular trash can.
2. "Curiosity, Concern, Intentional"
    - Accessing PHI of a friend, family member, co-worker, acquaintance, VIP or other individual out of curiosity or concern or because someone asked you to.
    - Looking up an address so you can send a get well card.
    - Looking up appointment information for you and/or family.
    - Removing confidential information from the facility without proper authorization.
    - Talking/posting information on a social media site about an unusual patient or case that you dealt with or heard about at work with your family, friends, etc.
3. "Personal Gain or Malice"
    - Using TH business or patient information for personal benefit
    - Selling patient or business information for media story.

VOICE MAIL

Voice mail should not be used for transmitting confidential information. Employees will be trained in the limitations of the voice mail system as it pertains to confidentiality.

Be aware that it is possible in some situations that recipients of voice mail may review their messages within hearing distance of other people. Also, verify the voice mail box number carefully before leaving the information.

DISPOSAL OF CONFIDENTIAL INFORMATION

Effective February 1, 2000, Wisconsin Act 9, Section 895.505 (also known as the Dumpster Diving Law), requires "proper" disposal of all records containing confidential information. Confidential information, which includes any patient information, will be disposed of in the appropriate manner. PHI should be disposed in locked containers, which are located in all departments of the hospital. The locked containers are to store confidential material, which is to be disposed of once a month through a contracted company. All confidential material is shredded on-site under the direct eye contact of the contracted company.

Persons who are not staff, employed or volunteers of Tomah Health may on occasion participate in debriefings and care reviews. A Confidentiality/Information Security Agreement Statement For Non-Employee Persons form shall be signed and HIPAA guidelines reviewed prior to discussions or sharing of information.

FORMS

Confidentiality/Information Security Agreement Statement and the Confidentiality/Information Security Agreement Statement For Non-Employee Persons (also located in HR section, Training, Orientation, Non-Employee Orientation, Orientation Documents, HR section Non-Employee Orientation, forms to Complete on HealthConnect)
Information Systems Request form (form reviewed with policy 200-IS-010)

COMPETENCY/REFERENCE DOCUMENTS (RD)

None

REFERENCE

OCR Emergency Prep-HIPPA Discloser
Policy: Release of Patient Information

TOMAH HEALTH
CONFIDENTIALITY AND SECURITY AGREEMENT

I understand that the facility or business entity (the "Company") in which or for whom I work, volunteer or provide services, or with whom the entity (e.g., physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of health information (the "Company"), has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with patient identifiable health information, "Confidential information").

In the course of my employment / assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Policies/Standards of Behavior available on HealthConnect (intranet), P&G Station and/or upon request. I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.

I WILL NOT:

- access, disclose, or discuss any Confidential Information with others, including friends or family
- Divulge copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized
- Discuss Confidential Information where others can overhear the conversation
- Make any unauthorized transmissions, inquiries, modifications, or purging of Confidential Information
- Share/disclose user names, passwords, etc
- Use tools or techniques to break/exploit security measures
- Connect to unauthorized networks through the systems or devices

I AGREE:

- My obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company
- Upon termination, I will immediately return any documents, equipment, or media containing Confidential Information to the Company
- I have received training on how to protect health information/confidentiality as necessary and appropriate to perform my job responsibilities.

I UNDERSTAND:

- I have no right to any ownership interest in any information accessed or created by me during my relationship with the Company
- I will act in the best interest of the Company and in accordance with its Standards of Behavior at all times during my relationship with the Company
- That violation of this Agreement may result in disciplinary action, up to and including termination of employment, suspension and loss of privileges, and/or termination of authorization to work within the Company, in accordance with the Company's policies
- I understand and agree that the computer login and/or electronic signature is equivalent to a legal signature.
- I understand and agree to use hospital issued equipment for business purposes and no expectation of privacy.

I WILL:

- Only access or use systems or devices I am officially authorized to access, and will not demonstrate the operation or function of systems or devices to unauthorized individuals
- Practice good workstation security measures such as logging out when leaving a workstation **unattended, locking** a workstation (CTRL-ALT-DEL) when not being used, position screens away from public view, etc.
- Practice secure electronic communications by transmitting Confidential Information only to authorized entities, in accordance with approved security standards
- Use only my officially assigned User-ID and password
- Use only approved licensed software
- Use a device with virus protection software

- Notify my manager, Administration, or Information Services if my password has been seen, disclosed, or otherwise compromised, and will report activity that violates this agreement, privacy and security policies, or any other incident that could have any adverse impact on Confidential Information.
- I will only access software systems to review patient records when I have a need to know basis. By accessing a patient's record, I am affirmatively representing to the Company at the time of each access that I have the need to do so for patient care, and the Company may rely on that representation in granting such access to me.

Additional TH Resources which may/may not be used based on authorization

Users will comply with all TH policies/procedures applicable along with federal/state regulations. User is responsible for information accessed under issued credentials. Immediately report lost, stolen, and/or security concerns to Information Systems at 608-377-8670 Option # 2.

Laptop/Mobile Devices Reminders: Additional security measures should not be disabled such as encryption, virus protection, power on password, etc. Unauthorized software is prohibited. Do not store passwords/PHI within the laptop, cases, etc. Do not allow non TH staff to use business resources. Be aware of eavesdropping, use of public Wi-Fi, storing PHI on local drive with no backup, securing device at all times, etc.

Remote User/VPN Reminders: Devices used for remote connection should have up to date antivirus/malware protection. Protect business resources from being accessed/viewed by unauthorized persons. User are not allowed to transfer any data from remote connection to non-hospital owned equipment. Users agree to provide a secure location, internet connection adequate to support productivity, and follow organizational policies and procedures.

Encryption: Service obtained thru department manager for setup/orientation to be completed by Information Services. Trigger phase is **zixcrypt** anywhere in the subject line. Phrase **noencrypt** will exclude email from this process and to be used with caution. Users should understand the process of the recipient.

_____ _____

Employee/Consultant/Vendor/Physician Signature Date

_____ _____

Employee/Consultant/Vendor/Physician Printed Name Facility Name (if other than TH)

This document may be electronically signed /historically stored by Human Resources/designee for participants.

TOMAH HEALTH
CONFIDENTIALITY AND SECURITY AGREEMENT

(for Non-Employee Persons participating in care reviews, training exercises, and debriefings)

I understand that the facility or business entity (the "Company") in which or for whom I work, volunteer or provide services, or with whom the entity (e.g., physician practice) for which I work has a relationship (contractual or otherwise) involving the exchange of health information (the "Company"), has a legal and ethical responsibility to safeguard the privacy of all patients and to protect the confidentiality of their patients' health information. Additionally, the Company must assure the confidentiality of its human resources, payroll, fiscal, research, internal reporting, strategic planning, communications, computer systems and management information (collectively, with patient identifiable health information, "Confidential information").

In the course of my employment / assignment at the Company, I understand that I may come into the possession of this type of Confidential Information. I will access and use this information only when it is necessary to perform my job related duties in accordance with the Company's Policies/Standards of Behavior available on HealthConnect (intranet), P&G Station and/or upon request. I further understand that I must sign and comply with this Agreement in order to obtain authorization for access to Confidential Information.

I WILL NOT:

- access, disclose, or discuss any Confidential Information with others, including friends or family
- Divulge copy, release, sell, loan, alter, or destroy any Confidential Information except as properly authorized
- Discuss Confidential Information where others can overhear the conversation
- Make any unauthorized transmissions, inquiries, modifications, or purging of Confidential Information
- Share/disclose user names, passwords, etc
- Use tools or techniques to break/exploit security measures
- Connect to unauthorized networks through the systems or devices

I AGREE:

- My obligations under this Agreement will continue after termination of my employment, expiration of my contract, or my relationship ceases with the Company
- Upon termination, I will immediately return any documents, equipment, or media containing Confidential Information to the Company
- I have received training on how to protect health information/confidentiality as necessary and appropriate to perform my job responsibilities.
- I only receive confidential information on a need to know basis.

I UNDERSTAND:

- I have no right to any ownership interest in any information accessed or created by me during my relationship with the Company
- I will act in the best interest of the Company and in accordance with its Standards of Behavior at all times during my relationship with the Company
- That violation of this Agreement may result or law enforcement involvement based on circumstances and evaluation.
- I understand and agree that the computer login and/or electronic signature is equivalent to a legal signature.
- I understand and agree to use hospital issued equipment for business purposes and no expectation of privacy.

Return to Health Information Services

_____ _____

Signature Date

_____ _____

Printed Name Date

_____

Agency Represented

AT A GLANCE – May I disclose protected health information for public health emergency preparedness purposes?

(From the perspective of the source of the information)