| | | |
|---|---|---|
| **ProTeam Management (PTM)**<br><br>***Policy Manual*** | Section: | Information Technology |
| | Policy #: | IT CWI 12-2024 V1 |
| | Subject: | **CMS Web Interface IT Security and HIPAA Compliance Policy** |

| **CROSS-REFERENCES:** |
|---|
| CWI Electronic Communications Policy |

## PURPOSE & OVERVIEW

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) was enacted to improve the efficiency and effectiveness of the nation's health care system.

The law includes provisions to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. It also defines requirements for the privacy and security of protected health information (PHI). The Patient Protection and Affordable Care Act (ACA) expanded on the HIPAA provisions.

As a healthcare services business, PTM must comply with multiple parts of HIPAA especially the requirements for privacy and security of PHI. In addition, PTM is a Business Associate with responsibilities under the terms of Business Associate Agreements (BAAs) signed with our customers (Clients), who are subject to HIPAA (Covered Entities)

Those requirements fall into four main areas of standards:

- Privacy - for the protection of PHI,
- Security - for protecting the confidentiality, integrity, and availability of electronic protected health information (ePHI),
- Breach – for notification of a breach of PHI or ePHI, and
- Enforcement – for the enforcement of HIPAA.

These requirements are met through a mix of administrative, physical and technical safeguards. This policy describes how PTM uses these safeguards to comply with applicable obligations of the HIPAA requirements for delivery of services related to the CMS Web Interface quality measure abstraction and submission program (CWI).

**The Privacy Rule** define standards addressing the use and disclosure of individuals' health information - PHI - by organizations subject to the Privacy as well as standards for individuals' privacy rights to understand and control how their health information is used. Under the privacy

rule and the terms of BAAs signed with Clients, PTM is subject to the Privacy Rule to the extent that it receives and processes patient information. (per 45 CFR Part 160 and Subparts A and E of Part 164)

**The Security Rule** sets national standards for protecting the confidentiality, integrity, and availability of electronic Protected Health Information (ePHI). Any information identifying a patient or offering a reasonable basis for identification is considered PHI. In addition, PTM may be subject to other privacy and confidentiality requirements such as federal requirements for Quality Improvement Organizations or Networks (QIOs or QINs). (per 45 CFR Part 160 and Subparts A and C of Part 164)

**The Breach Rule** requires HIPAA Covered Entities and their Business Associates to provide notification following a breach of unsecured protected health information (per 45 CFR §§ 164.400-414). Similar breach notification provisions implemented and enforced by the Federal Trade Commission (FTC), apply to vendors of personal health records and their third party service providers, pursuant to section 13407 of the HITECH Act.

**The Enforcement Rule** contains provisions relating to compliance and investigations, the imposition of civil money penalties for violations of the HIPAA Administrative Simplification Rules, and procedures for hearings. The HIPAA Enforcement Rule is codified at 45 CFR Part 160, Subparts C, D, and E. (per 45 CFR Part 160, Subparts C, D, and E).

Additional details of the requirements can at this time be found at:

- https://www.cms.gov/Regulations-and-Guidance/Administrative-Simplification/HIPAA-ACA/PrivacyandSecurityInformation.html
- https://www.hhs.gov/hipaa/for-professionals/index.html
- https://https://www.healthit.gov/sites/default/files/pdf/privacy/privacy-and-security-guide.pdf.

## POLICY GUIDELINES - PRIVACY

The HIPAA Privacy Rule requires appropriate safeguards to protect the privacy of PHI and sets limits and conditions on the uses and disclosures that may be made of such information without patient authorization. The Rule also gives patient's rights over their health information, including rights to examine and obtain a copy of their health records and to request corrections.

PHI, also referred to as individually identifiable health information, is information, including demographic information that relates to:

- the individual's past, present, or future physical or mental health or condition,
- the provision of health care to the individual, or
- the past, present, or future payment for the provision of health care to the individual.

In addition, individually identifiable health information identifies the individual or there is a reasonable basis to believe it can be used to identify the individual.

PTM' responsibilities under the Privacy Rule fall into several areas.

**Required Disclosures** require us to disclose PHI in only two situations: (a) to individuals (or their personal representatives) specifically when they request access to, or an accounting of disclosures of, their PHI; and (b) to U.S. Department of Health and Human Services (HHS) when it is undertaking a compliance investigation, review or enforcement action.

**Permitted Uses and Disclosures** define other ways in which we can use or disclose PHI. Our policy is that we use PHI only to fulfill the work we have contracted for with our clients, including government entities. The Privacy Rule defines other permitted uses and disclosures and any other requests or needs for use or disclosure are not allowed without the express written permission of the Chief Executive Officer, Chief Operating Officer or Chief Compliance Officer. In general, our response to other possible permitted uses and disclosures will be to refer the request to our Clients under the terms of the applicable BAA or regulations.

Our policy also covers other aspects of the Privacy Rule:

- Minimum necessary use and disclosure of PHI - Our policy is to make reasonable efforts to use, disclose, and request only the minimum amount of PHI needed to accomplish our contractual commitments.
- Restrict access and use of PHI – Our policy is to make reasonable efforts to only allow access and use of PHI to those that must have access to meet our contractual or regulatory requirements. Any other uses require the express written permission of the Chief Executive Officer, Chief Operating Officer or Chief Compliance Officer.
- Disclosure Accounting - Individuals have a right to an accounting of the disclosures of their PHI. Our policy is to make reasonable efforts to track and maintain records of our use of PHI based on the Client contract. If not specified, PTM will make reasonable efforts to maintain this information for ten (10) years.
- Complaints, Retaliation and Waiver - A Covered Entity must provide procedures to complain about our compliance with the Privacy Rule and PTM may not retaliate against a person for exercising rights provided by the Privacy Rule, for assisting in an investigation by HHS or another appropriate authority, or for opposing an act or practice that the person believes in good faith violates the Privacy Rule. PTM' policy is to make reasonable efforts to meet these requirements. Complaints should be brought to the Chief Executive Officer, Chief Operating Officer or Chief Compliance Officer. Concerns about retaliation or waiver should also be brought to one of these people.

## POLICY GUIDELINES - SECURITY

The HIPAA Security Rule requires PTM to take steps aimed at:

1) Preventing unauthorized disclosure of PHI and confidential information,
2) Ensuring integrity of PHI and confidential data,
3) Implementing appropriate retention and disposal of PHI and confidential information, and
4) Providing employees with training about HIPAA and their responsivities.

These goals are met through three types of safeguards: administrative, technical and physical.

PTM utilizes state-of-the art information systems and technology infrastructure incorporating proprietary and user-owned hardware, networks and software as well as vended and cloud-based systems.

In all cases, PTM' policy is to comply with the HIPAA Security Rule implemented appropriately for the different information system configurations. PTM policies, procedures and technology to be compliant in these areas follow.

1. **Prevent unauthorized disclosure of PHI and confidential information:**

   **User Devices**
   CWI work should only be done using PTM issued and owned laptops. These devices are required to be encrypted using at least 256-bit encryption and appropriate authentication such as a user ID and a password or PIN to access the device.

   **Corporate Storage, Servers, and Information Systems**
   PTM utilizes different types of storage, servers and information systems for CWI work. The following policies and procedures are required and enforced.

   - **Vendors:** PHI can only be stored or used on company designated corporate information technology or information systems. All storage must be configured to meet HIPAA compliance and, if cloud-based, the vendor must execute a BAA. Signed copies of BAAs are maintained by the Corporate Contract Manager.
   - **User Authentication**: Either a combination of user ID and password or multi-factor authentication is required to gain access to all PTM utilized information systems and corporate IT infrastructure.
   - **Password management:** Where applicable, rules are implemented for a minimum length and complexity of passwords and passwords must be changed on a regular basis. Users are required to keep their passwords private and not share them with anyone.
   - **Log-in Management:** Users are locked out of PTM information systems which contain PHI after five failed login attempts.
   - **Automatic Logoff:** PTM information systems holding PHI lock after fifteen minutes of inactivity and require the user to log back into the system. This helps prevent unauthorized users from gaining access to PHI in the absence of an authorized user.
   - **Storage Encryption:** All devices that are used in the processing or storage of PHI have encrypted storage using at least 256-bit encryption.
   - **Physical Storage Security:** PHI should not be stored on any other devices. Nonetheless, if PHI is on a CD, thumb drive or other physical storage media, these

media must be marked as confidential and stored securely under lock and key.

- **Access rights:** Access rights to PHI is assigned by the Information Technology (IT) Department based on a profile filled by the individual's supervisor or the HR/recruiting departments based on instructions in writing from supervisors. Instructions to establish or change access rights must be transmitted in writing using PTM designated forms or electronic communication. It is the supervisor's responsibility to ensure assignment of access rights to appropriate staff at the point of hiring and update the rights throughout the period of employment.
- **Procedure for termination of accounts assigned to former employees:** A procedure is in place to lock out user accounts upon staff termination. The Human Resources Department submits requests to the IT department. Requests must be in writing using PTM designated forms or electronic communication to discontinue a staff's account when a staff member is no longer with the company.

**Networks**

Access to PTM and other systems, like customer systems is done over a network which accesses the internet. The configuration of the network depends on the user's location and therefore the security requirements depend on the location.

- **User Device Network Protection:** Per above, all CWI work should only be done on PTM provided and owned laptops. These devices have a software firewall configured per PTM policies.
- **PTM Proprietary:** Networks at PTM facilities have a firewall deployed to protect it and any systems on that network from unauthorized access from the internet. Wireless networks in PTM facilities are password protected.
- **User Proprietary:** If at all possible user facilities, such as a user's home, should have a router or firewall in place. These wireless networks must be password protected.
- **Public:** CWI work should not be done from public facilities.

**Transmission**

PHI should only be transmitted using approved encrypted methods. Email transmissions containing electronic PHI are encrypted and decrypted by the PTM email system using at least 256-bit encryption. Other transmissions are encrypted and decrypted using at least 256-bit encryption, such as HTTPS. When applicable, a Virtual Private Network is utilized to access PHI. If a Client contract requires a different transmission method, that method will be used as long as it is HIPAA compliant.

**Physical Site Security**

**Physical Site Security – PTM Facilities**

- **Site Security:** PTM facilities have appropriate physical site security such as locked doors, cardkeys, and access tracking. Specific site security will vary by site. All PTM staff must use the site-designated physical security and acknowledge that their access to and movement around a site can be logged.
- **Visitor Control:** For visitor control, paper sign-in logs are used identifying the visitor, section or person visited, and sign in/out times. Visitors must adhere to site-specific requirements such as wearing a badge.
- **Multi-day Visitor Control:** Non-PTM staff who have regular need to access a site can be provided with site access, such as a card key. Providing access requires approval from the appropriate manager.

**Physical Site Security – User or Public Facilities**

Most PTM CWI employees and contractors work "virtually" in geographically dispersed locations. All work done for CWI should be done from their homes. These staff have

responsibility to physically protect PHI and PTM assets as follows.

- **Site Security:** All equipment which might have access to PHI should be kept in a location that can be locked when unattended. A lock on the user's home or primary, private work location is sufficient though, if possible, CWI work should be done from a separate, lockable room at that location. When away from the user's home or primary work location, equipment should not be used for CWI work, always be under the supervision of the user, and should never be left at that location.
- **Non-Staff Control:** Obviously there are often others living in employees' homes and visitors cannot be controlled. This is one of the reasons for the device security requirements in this policy. PTM owned equipment for CWI should not be used by anyone other than PTM staff.

**Software Development**

PTM uses vendor supplied information systems and PTM developed software for CWI.

- **Vendor Supplied Information Systems:** As described above, vendors of all vendor supplied information systems which process or store PHI must sign a BAA.
- **PTM Developed Software:** The software development process for information systems which process, or store PHI must include security requirements and testing for the software's compliance with the HIPAA Security Rule. Outsourced vendors developing PTM software which has PHI must sign a BAA.

## 2. Ensure integrity of PHI and confidential data

PTM uses the following processes, controls, and technology to make reasonable efforts to ensure the integrity of PHI and confidential data.

- **Access Controls:** Access controls help ensure the integrity of PHI and confidential data by managing who has access to that information. The Access Controls described above therefore also apply to this area.
- **Physical Site Security:** Controlling physical access to PHI and confidential data also helps ensure its integrity. Therefore the physical site security guidelines above apply to this area as well.
- **Encryption:** PHI and confidential data are encrypted both at motion and at rest. The encryption policies and technical standards are described above.
- **Audit Controls:** Access and changes to ePHI on PTM' propriety systems (e.g. DART) or SaaS systems (e.g. Office 365) storing PHI client are tracked and recorded.
- **Protection from malicious software**: Virus protection software is installed on all PTM laptops used for CWI. Users should not put unauthorized software on that laptop.
- **Backup:** Backup procedures allow reconstruction of PHI. DART and other PTM systems used for CWI are backed up at least daily and backups are stored in a redundant fashion based on the vendors' procedures which must be HIPAA compliant as evidenced by the vendor's BAA.
- **Emergency Mode Operation Plan/Disaster Recovery Plan:** Procedures for accessing electronic PHI in an emergency are defined in the Business Continuity and Contingency Plan.
    - PTM policy is to base all IT infrastructure and systems in either proprietary off-site hosting centers or shared infrastructure (such as for SaaS) accessible from the internet with appropriate access controls. These vendors provide access to PHI from many locations. The vendors provide Emergency Mode Operation and Disaster Recovery Plans which are reviewed by PTM annually.
    - The disaster recovery team meets annually to go over roles and responsibilities and to address any changes to the plan.

### 3. Appropriate retention and disposal of PHI and Confidential information

- **Retention of PHI**: PTM will make reasonable efforts that PHI will be retained based on the Client contract. If not specified, PTM will make reasonable efforts to retain PHI for ten (10) years.
- **Disposal of ePHI**: After the retention period, PHI will be destroyed using industry standard, secure electronic destruction methods. If PHI is on a CD, thumb drive or other physical storage media, these media must be marked as confidential and turned over to IT to be destroyed after the planned use.
- **Printed, Hard-copy PHI:** PHI should not be printed if at all possible. If necessary, hard-copy PHI, should be stored securely under lock and key. Disposal of hard-copy PHI at all other locations should be done by shredder.

### 4. Employee Training and Responsibility

- **Security Training and Reminders:** Training on confidentiality and security of data is required of each new CWI staff person. Confidentiality statements are signed by all CWI staff. Periodic reminders are also sent by email to CWI staff, as appropriate.
- **Responsibility Acknowledgement**: To help ensure compliance with the HIPAA requirements, this PTM HIPSS Compliance Agreement directs CWI users to meet these HIPAA policies. CWI staff electronically acknowledge that they have reviewed and are responsible to implement this HIPAA Compliance Agreement policy each year.
- **Security Incident Tracking:** Tracking reports are maintained by IT including record of actions taken in response to such incidents.
- **Assigned Security Responsibility:** The Compliance Officer oversees the HIPAA policies and procedures regarding the Privacy, Breach and Enforcement rules. The Security Officer oversees the HIPAA policies and procedures regarding the Security Rule.
- **Sanction policy:** When an unauthorized disclosure of PHI has been identified, the staff proximately responsible for the breach of policy, their supervisor, the Compliance Officer, and the Security Officer will meet as a team to discuss the events that led to the incident. The goal is to put into place such measures throughout PTM that would prevent this problem from recurring. All staff will be notified about the preventive measures put in place. Administrative sanctions up to and including termination may be applied for willful and purposeful violations of this policy.

## POLICY GUIDELINES – BREACH NOTIFICATION

A Breach is generally an impermissible use or disclosure under the Privacy Rule that compromises the security or privacy of PHI that is unsecured, meaning that the PHI is usable, readable or decipherable.

PTM policies in the event of a Breach follow.

- Notify the Covered Entity, usually a PTM Client, without unreasonable delay and no later than 60 days from the discovery of the breach or per the BAA with that client, whichever is sooner.
- Notify affected individuals either directly or per the BAA by notifying the Client.

- If a breach affecting more than 500 residents of a State or jurisdiction occurs, in addition

to notifying the affected individuals, provide notice to prominent media outlets serving the State or jurisdiction.

- Notify the Secretary of HHS. If the breach is more than 500 individuals, without unreasonable delay and within 60 days. If less than 500 individuals, maintain a log of the Breach and submit the log to HHS annually.
- If PTM staff believe a Breach has occurred, they should notify the Chief Executive Officer, the Chief Operating Officer, or the Chief Compliance officer as soon as possible. Those individuals will review the possible breach, and if appropriate will initiate the appropriate notification action.

## POLICY GUIDELINES – ENFORCEMENT RULE

The federal Department of Health & Human Services Office for Civil Rights (OCR) is responsible for enforcing the Privacy and Security Rules. OCR carries out this responsibility by investigating complaints that have been filed against organizations. OCR investigates all breaches of 500 or more records that are reported through the OCR breach portal to determine whether the breach was the result of noncompliance with HIPAA Rules and whether, through HIPAA compliance, the breach could have been prevented. If some evidence of noncompliance is discovered, a more comprehensive compliance review may be initiated. OCR may also conduct compliance audits to determine if Covered Entities have implemented the appropriate policies and procedures demanded by HIPAA.

PTM policy is to cooperate with any OCR enforcement action and to implement applicable compliance improvements and enforcement actions. If PTM staff have reason to believe that an enforcement action that involves PTM could occur, they should notify the Chief Executive Officer, the Chief Operating Officer, or the Chief Compliance officer as soon as possible. Those individuals will initiate the appropriate action.

| | |
|---|---|
| Process Owner | Chief Information Officer |
| Department | Information Technology |
| Effective Date | December 01, 2024 |
| Revision Date(s) | December 01, 2024 |
| Authorities | |

| | |
|---|---|
| **APPROVED BY: CHIEF OPERATING AND INFORMATION OFFICER, MANAGER OF CMS WEB INTERFACE PROGRAMS, MANAGER OF IT OPERATIONS, AND IT SYSTEM ADMINISTRATOR** | **DECEMBER 01, 2024** |