Safeguarding the Privacy and Security of Protected Health Information (PHI)

COMP.102

TABLE OF CONTENTS

Applicability: UW Medicine Affiliated Covered Entity

Policy Title: Safeguarding the Privacy and Security of Protected Health Information (PHI)

Policy Number: COMP.102

Superseded Policy: PP-11, PP-20, PP-20a, PP-30, SP-01 (Privacy portion), SP-02 (Privacy portion), SP-03 (Privacy portion)

Date Established: October 11, 2017

Date Effective: December 15, 2023

Next Review Date: December 15, 2026

PURPOSE

This policy establishes UW Medicine safeguards for protecting the confidentiality, integrity and availability of protected health information (PHI).

DEFINITIONS

See UW Medicine Compliance Glossary.

POLICY

All UW Medicine workforce members and business associates are required to safeguard PHI (in all forms) and at all times (onsite, offsite and in transit).

Workforce members are personally and professionally responsible for reasonably and appropriately protecting the privacy, security and confidentiality of any information to which they are given access.

I. Safeguarding Verbal PHI

Verbal PHI may be safeguarded in the following manners:

- Discuss PHI only with those who have a need-to-know and are authorized to receive the information.
- Discuss PHI only in ways and places where those who are not involved in the patient's care are not likely to overhear. Public areas, such as elevators and cafeterias, may not be appropriate for such discussions.
- Speak quietly and with awareness that PHI could be overheard.
- Use the minimum amount of information necessary for patient safety when calling out patient names in reception areas (for example, if feasible use only patient's first name, or a title and last name).
- Minimize the amount of PHI disclosed when leaving appointment reminders or other types of messages for patients.

II. Safeguarding Paper and Electronic PHI

Paper and electronic PHI may be safeguarded in the following manners:

- Keep paper and electronic-based PHI out of view of anyone who is not involved in the patient's care.
- Ensure that patients and visitors are not able to access paper and electronic-based PHI in the work areas where it is processed.
- Never leave PHI unattended in exam rooms or in unlocked work areas such as desks, patient care units or portable equipment.
- Dispose of PHI in a secure and confidential manner. For example, if PHI is no longer needed, it should be disposed of in appropriate locked shredding bins, or otherwise destroyed according to published standards.
- Maintain the confidentiality and integrity of PHI when it is removed from its originating computing system.
- Workforce members shall minimize the PHI displayed in patient care areas (for example, white boards, patient sign-in sheets), applying the following rules:
  - If names are displayed, use only patients' initials or first initial with the last name unless using abbreviated names may compromise patient safety.
  - Never associate medical conditions with patient names in public areas.
- Manage electronic PHI in transit (e.g., email, "cloud" services, copying to removable media, text messaging, etc.) in a manner that prevents inappropriate access, data loss or alteration, regardless of the method employed to transfer the PHI from one place to another. This includes computing system to computing system communications via shared internal and public networks. All PHI in transit must be encrypted or otherwise physically secured in a manner that prevents its theft or inappropriate use. For guidance on how to securely use UW Medicine email systems to transmit PHI, please see IT Services – Security Guidence (VMC workforce, see VMC IT Security page).
- Workforce members who must take PHI offsite to perform an authorized activity or duty shall execute appropriate safeguards. The same requirements for protecting PHI onsite in the workplace apply when the information is offsite. Additional requirements apply to PHI taken offsite:
  - Workforce members who take PHI offsite shall keep the PHI fully secured and in their physical possession during transit. Workforce members shall never leave PHI unattended in any mode of transport, even if the mode of transport is locked. This does not apply to couriers who transport laboratory specimens from multiple client sites to the reference laboratory, as long as the specimens are transported in locked containers.
  - PHI taken offsite shall be secured at that location, stored in a suitable locked receptacle when not in use or unattended and removed from printers and fax machines immediately.
  - PHI shall not be taken out of UW Medicine facilities without the workforce member's manager's approval.

III. Incidental Uses and Disclosures

An incidental use or disclosure is a secondary use or disclosure that cannot reasonably be prevented, is limited in nature and that occurs as a result of another use or disclosure that is permitted by policy. Incidental uses and disclosures are permitted so long as workforce members use reasonable safeguards to limit such secondary uses and disclosures and abide by the minimum

necessary standard. Examples of incidental uses and disclosures include a patient seeing other patient names on a sign-in sheet or white board.

IV. Verification Requirements for Disclosures of PHI

Workforce members shall verify the identity and authority of individuals who request PHI from UW Medicine before releasing the requested information. Prior to any disclosure of PHI, workforce members shall:

- Verify the identity of any requester who is not already known and determine the requester's authority for access to the PHI.
- Obtain any required verbal/written documentation, statements or representations from the requester.

A. Conditioned Disclosures

If a disclosure of PHI is conditioned on documentation, statements or representations from the requester, workforce members may rely on the documentation, statements or representations received or provided.

1. For disclosures for law enforcement purposes, workforce members may rely upon a judicial or administrative request, including subpoena or summons, a civil or authorized investigative demand or similar process as authorized by law demonstrating:

    a. The information sought is relevant and material to a legitimate law enforcement inquiry;
    b. The request is specific and limited in scope to the purpose for which it is being sought; *and*
    c. It is unreasonable or infeasible to use de-identified information.
    (See COMP.103 Use and Disclosure of PHI for information related to use and disclosure of PHI to law enforcement and for judicial and administrative proceedings.)

2. For disclosures for research purposes, the requester must provide a valid Institutional Review Board (IRB) waiver. (See information related to research in COMP.103 Use and Disclosure of PHI.)

B. Identity of Public Officials

Workforce members shall verify the identity of public officials requesting PHI. The following are appropriate methods to verify the identity of a public official or person acting on behalf of a public official:

1. In-person presentation of an agency identification badge, other official credentials or proof of government status;
2. Appropriate government letterhead for written requests; *or*
3. A written statement on appropriate government letterhead if the person presenting is acting under the government's authority or some other evidence or agency documentation (for example a contract for services, Memorandum of Understanding or Protective Order) that establishes that the person is acting on behalf of the public official.

C. Authority of Public Officials

Workforce members shall verify that the public official, or a person acting on the behalf of a public official, has the authority to request PHI. The following documentation is accepted for this purpose:

1. A written statement of legal authority or if a written statement is impracticable, an oral statement of such authority; *or*
2. A request pursuant to a warrant, subpoena, order or other legal process issued by a grand jury or a judicial or administrative tribunal.

D. Professional Judgment

Verification requirements are met when workforce members exercise professional judgment to determine appropriate authority.

V. Access Management: Authorizing Users for Access to UW Medicine Information Systems Containing PHI

UW Medicine identifies those persons or classes of persons in its workforce who require access to PHI to carry out their job responsibilities, the category(ies) of PHI to which access is needed and any conditions appropriate to such access. Furthermore, UW Medicine manages access to systems containing PHI for all potential users whether internal or external to UW Medicine. UW Medicine makes reasonable efforts to limit access and uses a role-based model to identify appropriate levels of access to PHI. Where possible, UW Medicine utilizes technology to assist in restricting the flow of information, to account for how information is used and shared and to monitor the effectiveness of these practices. UW Medicine strives to reach an appropriate balance between access required for treatment, payment and healthcare operations, and the patient's privacy.

A. UW Medicine Workforce

1. Managers shall authorize role-based access to UW Medicine information systems containing PHI for the workforce members they supervise as required for the performance of the workforce members' official job responsibilities; while managers may execute this through a delegate, they still retain the authorization responsibility.

2. Workforce members shall complete the workforce member 002.F1 Privacy, Confidentiality and Information Security Agreement (PCISA) upon hire or engagement and at each evaluation or provider credentialing.

3. Managers shall maintain documentation of the systems to which each workforce member has access. 102.F2 Workforce Member Documentation of IT System Access may be used for this purpose.

B. Non-UW Medicine Workforce

UW Medicine may provide individuals who are not part of its workforce with role-based access to UW Medicine information systems containing PHI when a business relationship

or continuity of patient care creates the need for access. These circumstances are categorized as follows:

- Entities in an Organized Healthcare Arrangement (OHCA) with UW Medicine.
- Business associates.
- External healthcare facilities or professionals.
- Other non-UW Medicine workforce (for example, auditors, regulators, insurers, external researchers).
- Limited account access.

The following requirements for specific categories must be met and the processes followed in order to obtain access.

1. OHCA members: UW Medicine may provide individuals from organizations that have entered into an OHCA with UW Medicine with access to UW Medicine information systems containing PHI for the purposes of joint treatment, payment and healthcare operations activities. Non-UW Medicine workforce members must request access from the applicable HIM Director or designated official to UW Medicine information systems containing PHI for research purposes. Each individual shall follow his or her own entity-specific process regarding access authorization and confidentiality agreements.

2. Business associates: The UW Medicine leader (for purposes of this policy, defined as manager or higher) that oversees the work of the business associate must assure that a Business Associate Agreement has been executed and must authorize the access to information systems containing PHI. Each individual must sign the 102.F3 Non-UW Medicine Workforce Member PCISA before access is granted. (The completed form is retained by the non-UW Medicine access coordinator.)

3. External healthcare facilities or professionals: Individuals from external healthcare facilities or external healthcare professionals may be granted electronic access to information systems containing PHI if all of the following criteria have been met:

    a. A UW Medicine leader (manager or higher) must sponsor the access.
    b. The information need cannot be met through standard entity Release of Information processes, Epic Care Everywhere, EpicCare Link or U-link access.
    c. The request for electronic access to information systems containing PHI is made to the applicable ERHI/HIM Director or designated official.
    d. There is an ongoing relationship with the external facility or professional, which includes sharing PHI for ongoing patient care or mandated reporting at a high frequency and/or volume, where:

        - Efficiency, utilization and quality of patient care is improved by allowing electronic access; *and*
        - Waiting for an individual disclosure would negatively impact patient care delivery.

    e. Providing access to the external healthcare facility or professional will improve patient or public safety.

f. There is a contract, affiliation, legal obligation or agreement in place that reflects the need to provide access to the external facility or professional, and a copy of this document is maintained by the applicable ERHI/HIM Director or designated official. (See 102.F1 Agreement for Electronic Access to PHI.)

If the above criteria are met, the applicable ERHI/HIM Director or designated official may approve the access request. Each individual must sign the 102.F3 Non-UW Medicine Workforce Member PCISA before access is granted. The completed form is retained by the non-UW Medicine access coordinator.

4. Other non-UW Medicine workforce: Other non-UW Medicine workforce members' (for example, auditors, insurers or external researchers) access to information systems containing PHI must be authorized by a UW Medicine leader (manager or higher). Each of these individuals must sign the 102.F3 Non-UW Medicine Workforce Member PCISA before access is granted. The completed form is retained by the non-UW Medicine access coordinator.

5. Limited account access: The applicable ERHI/HIM director or designee may provide limited electronic access to specific patient account(s) as an alternative to processing Release of Information disclosures through ERHI/HIM.

C. Access Modifications and Terminations

Managers and non-UW Medicine access coordinators must promptly report any changes to end-user duties or employment status to keep system privileges up-to-date and restricted to current job requirements. Examples of reportable changes include promotion, extended leave and separation. In addition to the manager or non-UW Medicine access coordinator, the end-user's Human Resources department and any supervisor in the end-user's chain of command may also authorize termination of the end-user's access.

D. Access Documentation and Records Retention

Managers, other leaders and access coordinators must maintain the documentation required by Section IV of this policy for at least seven years or in accordance with entity-specific retention policies, whichever is longer. (102.F2 Workforce Member Documentation of IT System Access)

PHI must be maintained in accordance with UW Medicine records retention policies.

REGULATORY/LEGISLATION/REFERENCES

- Security Standards for the Protection of Electronic Protected Health Information, 45 C.F.R. § 164, Subpart C.
- Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164, Subpart E.
- Revised Code of Washington (RCW) 19.215 – Disposal of personal information.
- RCW 40.14 Preservation and destruction of public records.
- RCW 70.02 Medical Records — Health Care Information Access and Disclosure.
- RCW 7.70.065 Informed Consent – Persons authorized to provide for patients who are not competent.
- RCW 70.41.190 Medical records of patients — Retention and preservation.

- OCR HIPAA Privacy Incidental Uses and Disclosures Guidance

PROCEDURE ADDENDUM(s) REFERENCES/LINKS

- UW Medicine Compliance Glossary.
- 102.F1 Agreement for Electronic Access to Protected Health Information.
- 102.F2 Workforce Member Documentation of IT System Access.
- 102.F3 Non-UW Medicine Workforce Privacy, Confidentiality and Information Security Agreement.
- 102.G2 Faxing PHI
- 102.G4 Protected Health Information.
- 002.F1 Privacy, Confidentiality, and Information Security Agreement.
- UW Administrative Policy Statement 2.4 Information Security and Privacy Roles, Responsibilities, and Definitions.
- UW Research – Information Privacy and Security.
- EpicCare Link Enrollment and Agreement Form.
- UW Medicine Account Activation, Deactivation, Change Request Forms.
- IT Services – Security Guidance
- VMC IT Security page
- UW Medicine Records Retention Schedule.

ROLES AND RESPONSIBILITIES

Defined within POLICY.

APPROVALS

/s/ Beth DeLair
Beth DeLair,
Chief Compliance Officer, UW Medicine
Associate VP for Medical Affairs, UW

12/21/2023
Date