HIPAA Security System Access

Policy Summary

It is the policy of the University of Wisconsin-Madison (UW-Madison) that the units of the UW-Madison Health Care Component and each unit within UW-Madison that is a Business Associate of a covered entity, (hereafter collectively referred to as “units,””) ensure the confidentiality, integrity, and availability of all protected health information (PHI) by establishing the following documentation and procedural requirements.

1. Access to information systems and applications by all users, including but not limited to workforce members, volunteers, business associates, contracted providers, consultants, and any other person or entity, is only authorized as described in HIPAA Policy 3.8 “The Minimum Necessary Standard.”

2. The same levels of confidentiality that exist for hard copy PHI, business, and proprietary information apply to digital and/or electronic protected health information (ePHI) within the organization’s information systems and applications, and are extended even after termination or other conclusion of access.

3. Additional restrictions on system access are included in HIPAA Policy 8.10 “HIPAA Security Remote Access” and HIPAA Policy 8.13 HIPAA “Security System Configuration and Use.”

Who This Policy Applies To

Applies to all members of the UW-Madison Health Care Component.

Rationale

In enacting HIPAA, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. Under the patchwork of laws existing prior to adoption of HIPAA and the Privacy Rule, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient’s medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient’s permission, be passed on to a lender who could then deny the patient’s application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions. The Privacy Rule
establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections apply over and above the new Federal privacy standards.

**Policy Detail**

1. **Access Authorization**
   1.1 Role based access authorization categories must be based on the criteria described in HIPAA Policy 3.8 “The Minimum Necessary Standard.”
   1.2 The user is granted access based on these pre-determined roles. When there is not a suitable pre-defined role, the Business Data Custodian may authorize access.
   1.3 Access authorization, revocation of authorization, or other authorization decisions must be documented. See sections (7) Documentation Requirements, and (8) Forms.

2. **Workforce Clearance Procedure**
   2.1 The level of access assigned to a user of the organization’s information systems and applications is based on the criteria described in HIPAA Policy 3.8 “The Minimum Necessary Standard”.
   2.2 Any access not specifically authorized is prohibited. When possible, technical means will be used to prevent unauthorized access.

3. **Access Establishment and Modification**
   3.1 Access to any of the organization’s information systems and applications will not be granted until:
      3.1.1 Training, as described in HIPAA Policy 9.1 “HIPAA Privacy and Security Training,” is completed.
      3.1.2 A signed “Confidentiality and Information Access Agreement” is on file. Forms and signatures may be electronic. See sections (7) Documentation Requirements, and (8) Forms.
   3.2 Whenever new or expanded access to specific resources is requested:
      3.2.1 Access will not be granted until a “System Access Request” form is received, reviewed, and any additional approval is obtained.
      3.2.2 When reviewing a request for new access, the requestor’s current access should also be reviewed and modified to conform with the criteria described in HIPAA Policy 3.8 “The Minimum Necessary Standard.”
   3.3 Each user’s access must be periodically reviewed and modified to conform with the criteria described in HIPAA Policy 3.8 “The Minimum Necessary Standard.”
   3.4 The person who authorizes access should be different from the person who grants access.

4. **Unique User Identification and Person or Entity Authentication**
4.1 Multi-factor authentication should be used when available.

4.2 Access to the organization’s information systems and applications is controlled by requiring unique User Login ID’s and password for each individual user or entity.

4.3 Users may not allow anyone for any reason to have access to any information system or application using another user’s unique User Login ID and password.

4.4 If a user believes their User Login ID has been compromised, they are required to immediately report the incident as described in HIPAA Policy 8.8 “Reporting of HIPAA Incidents and Notifications in the Case of Breaches of Unsecured PHI.”

5. Password Management

5.1 When User Login IDs and passwords are used to control access to the organization’s information systems and applications, the passwords must not be disclosed.

5.2 Passwords are not displayed at any time, nor should they be stored in clear text in programming scripts.

5.3 A User Login ID and generic password is initially assigned for each user. The User Login ID and password are forwarded to the user securely. Users are required to change the password upon first-time use.

5.4 Minimum password requirements are described in the UW-Madison Password Standard. Units and information systems may require stronger passwords.

5.5 Users are required to change passwords periodically.

5.6 The information systems or applications are programmed to deny a user’s ability to use up to a pre-determined number of prior passwords whenever possible.

6. Change/Termination Procedures

6.1 The Human Resources Department (or other designated department), and a workforce member’s supervisor must ensure that the “Change/Termination Checklist” is processed upon completion and/or termination of the workforce member’s employment or other workforce relationship, or upon a change in job assignment or employment status. See sections (7) Documentation Requirements, and (8) Forms.

6.2 Each person responsible for a portion of the off-boarding or change process must complete their portion of the “Change/Termination Checklist.”

6.3 A workforce member’s access rights must be terminated immediately upon notification, or if the change is scheduled, on the effective date of the change.

7. Documentation Requirements

7.1 The unit must document and maintain all of the following records for a period of at least six years, from the date of its creation or the date when it last was in effect, whichever is later.

7.1.1 Records of authorization decisions. (See 1. above)
7.1.2 System Access Request Forms. (See 3. above)

7.1.3 Confidentiality and Information Access Agreement. (See 3. above)

7.1.4 Change/Termination Checklists. (See 6. above.)

7.1.5 A description of the workforce members who are able to add, remove, or modify the access to some or all of the organization’s information systems.

8. Forms

Forms and signatures may be paper or electronic.

8.1 Confidentiality and Information Access Agreement (template)

8.2 System Access Request (template)

8.3 Change/Termination Checklist (template)

Consequences for Non-Compliance

Failing to comply with this policy may result in discipline for the individual(s) responsible for such non-compliance.

Further, the US Department Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules, and an individual’s non-compliance may result in institutional non-compliance and/or an investigation by OCR. OCR attempts to resolve investigations by obtaining voluntary compliance and entering into Corrective Action Plans and Resolution Agreements. Failures to comply with HIPAA or cooperate with OCR in an investigation may result in civil and/or criminal penalties.

Supporting Tools

Additional information may be found at www.compliance.wisc.edu/hipaa

Definitions

1. **Business Data Custodian**: A university official having direct operational-level responsibility for the management of one or more types of data. They are charged with providing authorization for access to institutional data.

2. **Electronic Protected Health Information** (ePHI): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.

3. **Minimum Necessary Information**: Protected health information that is the minimum necessary to accomplish the intended purpose of the access, acquisition, use, disclosure, or request. The “minimum necessary information” principle applies to all protected health information in any form.

4. **Protected Health Information** (“PHI”): Health information or health care payment information, including demographic information collected from an individual, which identifies the individual or can be used to identify the individual. PHI does not include student records held by educational institutions or employment records held by employers.
5. **Role:** The category or class of person or persons doing a type of job, defined by a set of similar or identical responsibilities.

6. **User:** A person or entity who has access to the organization’s information systems. This includes workforce members, business associates, external research collaborators, and other external persons or entities of all kinds.

7. **Workforce:** Employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity, is under the direct control of such entity, whether or not they are paid by the covered entity.

---

**Responsibilities**

- HIPAA Privacy Officer
- HIPAA Security Officer

**Link to Current Policy**

[TBD]

**Link to Related Policies**

[https://compliance.wisc.edu/policies-and-forms/](https://compliance.wisc.edu/policies-and-forms/)

**Link to Policy History**

N/A

**Review / Approval**

- HIPAA Executive Board, March 26, 2020
- HIPAA Privacy and Security Operations Committee, January 11, 2018