University of Wisconsin-Madison
Policy and Procedure

Policy Number: 8.12
Policy Title: HIPAA Security Facilities Management
Effective Date: September 1, 2015
Last Revision Date: August 21, 2015

I. Policy

It is the policy of the University of Wisconsin-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.

A. Implement procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. The following components must be included in order to form a complete facility security plan.

1. Implement procedures to limit a person's physical access to restricted or sensitive areas based on their role.

2. The procedures must permit access to ePHI for contingency operations in accordance with the unit's Continuity of Operations plan, as described in Policy # 8.4 "HIPAA Security Contingency Planning".

3. Physical access to restricted areas is limited to only those authorized in accordance with those procedures.

4. All workforce members are responsible for reporting an incident of unauthorized access to restricted areas as described in Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information".

B. Implement procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, walls, doors, locks and other hardware intended to limit physical access.) In managing and monitoring the security of the facilities and in planning and performing such maintenance, repairs or modifications, the unit will:

1. Identify material increases in security risks to PHI;

2. Reduce those increased risks to the extent feasible;

3. Monitor for additional material increases in security risks; and

4. Properly document the project.

C. Responsibility for compliance with specific aspects of this policy in specific circumstances will be assigned in the unit's Safeguard Implementation Plan (or the equivalent) as described in Policy # 8.1 "HIPAA Security Risk Management".

II. Definitions

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

B. Facilities/Building Services/Security Manager: The person responsible for managing a facility, or the person designated as responsible for a facility's physical HIPAA security.

C. Lead Project Coordinator: The person responsible for leading a project that involves repair, modification, or scheduled maintenance of facilities or systems covered by HIPAA.

D. Non-sensitive Areas: Those areas of the facilities where PHI and/or sensitive organizational information is not stored or is not utilized there on a regular basis. These areas include, for example, the following:

1. Lunch rooms;
2. Conference rooms;
3. Facility parking lots;
4. Facility entry ways;
5. Main hallways;
6. Restrooms; and
7. Other public areas.

E. 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.

F. Restricted and Sensitive Areas: Those areas of the facilities where PHI and/or sensitive organizational information is stored or utilized on a regular basis.

Restricted Areas contain PHI which is easily visible or obtained, and must be locked or otherwise secured when unattended to assure that access is limited to those specifically authorized. Restricted Areas include but are not limited to the following examples:

- Medical record storage;
- Information services equipment rooms;
- Designated storage closets and cabinets; and
- Unattended areas where PHI is easily visible or obtained.

Sensitive Areas are those which contain PHI which is locked or otherwise adequately secured to limit access to those who are authorized. Sensitive areas may be unlocked and unattended for periods of time. These areas include, but are not limited to the following examples:

- HIS control desks;
- Check-in desks/stations;
- Nursing/patient care stations/desks;
- Patient care hallways;
- Patient care rooms or other designated area;
- Employee meeting rooms/kitchens located in patient care areas;
- Offices;
- Cubicles;
- Business offices;
- Human resources offices; and
- Administration offices.

G. Risk: The likelihood that a threat will exploit a vulnerability, and the impact of that event on the confidentiality, availability, and integrity of ePHI, other confidential or proprietary electronic information, and other system assets. See Policy # 8.1 "HIPAA Security Risk Management" for related definitions.

H. Vendors: persons from other organizations marketing or selling products or services, or providing services. Examples include, but are not limited to the following:

1. Pharmaceutical representatives;
2. Equipment repair service personnel;

3. Food services; and
4. Independent contractors.

I. 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.

III. Procedures

A. Security of Restricted Areas

1. Restricted areas and facilities are locked or otherwise secured when unattended.
2. Only authorized workforce members and vendors receive keys, card access, or access codes to access restricted areas, as authorized by the unit's HIPAA Security Coordinator, or designee.
3. Workforce members or vendors are required to return the key(s) to the designated office or individual, (such as the Human Resources department or supervisor,) on their last day of employment/last day of contracted work or services being provided.
4. Workforce members and vendors must report a lost or stolen key or access card as described in Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information".
5. When a key is reported lost or stolen the Facilities/Building Services/Security Manager facilitates the changing of the lock(s) within one business day. Access codes and card access are adjusted as soon as possible when an access card is reported lost or stolen or there are changes to those authorized to access the area.

B. Persons Allowed in Restricted Areas

1. Workforce members as approved by their supervisor and as needed to perform their job duties.
2. Vendors who are on a long-term contract once oriented to the areas, without an escort.

3. Other vendors with an escort into and out of the restricted areas.
4. Other visitors (not vendors) with an escort into, out of, and while moving around within restricted areas.

C. Enforcement of Access to Restricted Areas

1. When a workforce member discovers an unauthorized person or persons accessing or attempting to access a Restricted Area, *do not attempt to detain them or to investigate the incident*. Instead, do one of the following.
   a. If you believe it is safe to do so, immediately and politely inquire about where they are intending to go, escort them out of Restricted Areas and escort or direct them to the area they are trying to get to.
   b. If you believe it might be unsafe to approach, interact or continue to interact with them, get to a safe place as quickly as it is safe to do so, and dial 911 to report an intrusion.

   In either case, follow up by reporting the unauthorized access as described in (2) below.
2. Report unauthorized access to Restricted Areas or other violations of this policy as described in Policy # 8.8 “Notification and Reporting in the Case of Breach of Unsecured Protected Health Information”.
3. Workforce members in violation of this policy may be subject to disciplinary action as described in Policy # 9.2 “Responding to Employee Noncompliance with Policies and Procedures Relating to the HIPAA Privacy and Security Rules”.
4. Vendors in violation of this policy may be subject to termination of services.
5. Other visitors in violation of this policy may be subject to loss of visiting privileges.

D. Security of Sensitive Areas

1. When a Sensitive Area is unattended and unlocked/unsecured, all media containing PHI must be either or both of:

a. Locked in storage closets, cabinets or other secure containers that are treated as Restricted Areas; or

b. Encrypted according to Policy # 8.9 "HIPAA Security System Access".

2. All workstations or other devices within Sensitive Areas that store or process ePHI must be secured as described in Policy #8.9 "HIPAA Security System Access".

E. Identifying PHI Security Risk(s) when Changing the Physical Facilities

Prior to approving plans to repair, modify, or schedule maintenance of physical facilities, the Lead Project Coordinator works with the Facilities/Building Services/Security Manager, to determine whether or not the scheduled maintenance, repairs, changes, or the construction process itself, materially increases the security risk to PHI. These security risks include, but are not limited to, work completed on the internal and/or external perimeter of the facilities (entryways, doors, locks, controlled access systems, walls, removing windows, etc.) and may result in:

1. Material potential to limit or remove an authorized user's ability to access workstations or other devices in which PHI is created, received, maintained, or transmitted during regularly scheduled hours and at regularly scheduled locations.

2. Material increases in the potential for unauthorized access to PHI.

3. Other material increases in risk to the confidentiality, integrity, or availability of PHI.

An increase in risk is material if the risk determination changes from "low" to "medium" or from "medium" to "high" as measured by the risk assessment procedure currently in use, (such as the example risk assessment procedure described in Policy # 8.1 "HIPAA Security Risk Management").

F. Reducing PHI Security Risks(s) when Changing the Physical Facilities

If the changes to the physical facilities indicate a material increase in the security risk to PHI as described in in III.G. above, the Lead Project

Coordinator works with the Facilities/Building Services/Security Manager to amend the plans to contain the following conditions:

1. All users that need access to PHI have access to PHI during their regularly scheduled hours. If, however, any user will not have access to PHI during their regularly scheduled hours, the Lead Project Coordinator notifies that user's supervisor prior to the unavailability of the PHI. The Lead Project Coordinator and supervisor develop a plan to accommodate necessary changes. Document all decisions made and followed as required in this policy.
2. If the plans increase the potential for unauthorized access to PHI, the Lead Project Coordinator works with the Facilities/Building Services/Security Manager, unit IT department, and supervisors, to identify ways to secure PHI throughout the project from unauthorized access. Document all decisions made and followed as required in this policy.
3. If the plans otherwise increase risk to the confidentiality, integrity, or availability of the PHI, the Lead Project Coordinator works with Facilities/Building Services/Security Manager, unit IT department, and supervisors, to identify ways to secure PHI throughout the project. Document all decisions made and followed as required in this policy.

G. Monitoring for Additional Risks when Changing the Physical Facilities

1. During the course of the project, the Lead Project Coordinator continuously monitors the project and immediately notifies Facilities/Building Services/Security Manager, unit IT department, and supervisors of any material increase in security risks to PHI (including printed media.)
2. If a violation of HIPAA security policies and procedures is identified, it is reported and investigated according to Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information".

IV. Documentation Requirements

A. Documentation of Physical Access Authorization for Restricted Areas and Restricted Devices

The unit's HIPAA Security Coordinator, or designees, maintain a record of workforce members and vendors who are authorized to access Restricted Areas. When authorizing physical access, workforce members may be identified by role, by name, or both, as appropriate.

B. Documentation when Changing the Physical Facilities

The Lead Project Coordinator and/or the Facilities/Building Services/Security Manager facilitates documentation throughout the project.

1. Documentation includes, at a minimum, the following information:
    a. Description of the repair or modification.
    b. Repair or modification start and end dates.
    c. Contact information for the units, contractors or vendors who completed the repair or modification.
    d. Summary of steps taken to reduce any material increase to the security risk(s) to PHI (including those identified before, during, and after the work was completed). At a minimum, this summary includes:
        i. Description of the identified material increase(s) in security risk(s).
        ii. A description of what was done to reduce those security risk(s).
        iii. If a material increase in security risk was due to a "high" risk determination:
            (1) Date the security risk was identified.
            (2) Dates and times steps were taken to reduce the security risk.

(3) Individuals involved in reducing the security risk.

2. Documentation for IV.1.a.-c. may be incorporated by reference to project documentation maintained by others such as the project manager or general contractor, provided that the documentation (or a copy of it,) is available for the required retention period.

3. Documentation for IV.1.d. for routine or repetitive work that results in a similar material increase in security risk(s) can reference prior documentation for similar work, provided that similar steps are taken to reduce the risk.

4. No documentation is required for routine or repetitive work where there is a low risk that exposure of PHI would result in an incident requiring notification.

5. After completion of the project, forward all documentation to the Facilities/Building Services/Security Manager.

C. The custodians of records or documentation related to the HIPAA security facilities management will ensure that those records or documents are retained for six years from the date of creation or date it was last in effect, whichever is later.

V. Forms

None

VI. References

- 45 CFR § 164.310(a)(2)(i) (HIPAA Security Rule – Facility Access Controls/Contingency Operations)
- 45 CFR §164.310(a)(2)(ii) (Facility Security Plan)
- 45 CFR §164.310(a)(2)(iii) (Access Control & Validation Procedures)
- 45 CFR §164.310(a)(2)(iv) (HIPAA Security Rule – Maintenance Records)
- 45 CFR §164.316(a-b) (HIPAA Security Rule – Documentation)

Resources

- HIPAA Collaborative of Wisconsin "Facility Maintenance and Repair" policy template
- HIPAA Collaborative of Wisconsin "Facility Access" policy template
- UW-Madison IT Security "Departmental IT Security Baseline"

VII. Related Policies

- Policy # 1.1 "Designation of UW-Madison Health Care Component"
- Policy # 8.1 "HIPAA Security Risk Assessment"
- Policy # 8.2 "HIPAA Security Oversight"
- Policy # 8.3 "HIPAA Security Auditing"
- Policy # 8.4 "HIPAA Security Contingency Planning"
- Policy # 9.2 "Responding to Employee Noncompliance with Polices and Procedures Relating to the HIPAA"
- Policy # 9.3 "Responding to Student Noncompliance with Polices and Procedures Relating to the HIPAA Privacy and Security Rules".

The HIPAA policies listed above are located at: www.hipaa.wisc.edu. UW-Madison IT policies are at: www.cio.wisc.edu/policies/.

VIII. For Further Information

For further information concerning this policy, please contact the UW-Madison HIPAA Security Officer or the appropriate unit's HIPAA Security Coordinator. Contact information is available within the "Contact" tab at www.hipaa.wisc.edu.

Reviewed By

UW-Madison HIPAA Privacy Officer
UW-Madison HIPAA Security Officer
UW-Madison Office of Legal Affairs

Approved By

Interim HIPAA Privacy and Security Operations Committee