University of Wisconsin-Madison
Policy and Procedure

Policy Number: 8.2
Policy Title: HIPAA Security Oversight
Effective Date: December 22, 2014
Last Revision Date: December 8, 2014

I. Policy

A. In accordance with the standards set forth in the HIPAA Security and HITECH Omnibus Rules, the University of Wisconsin-Madison (UW-Madison) is committed to ensuring the confidentiality, integrity, and availability of all electronic protected health information (ePHI) it creates, receives, maintains, or transmits. To that end UW-Madison has a designated HIPAA Security Officer to coordinate the appropriate HIPAA security development, implementation, and oversight of the units of the UW-Madison Health Care Component and each individual or unit at UW-Madison that is a Business Associate of a covered entity (hereafter collectively referred to as "units") The UW-Madison HIPAA Security Officer is responsible for:

1. Advising UW-Madison leadership, including the UW-Madison HIPAA Privacy Officer, the HIPAA Privacy Coordinator of each unit, and the HIPAA Security Coordinator of each unit on all matters related to the HIPAA security;
2. The development, implementation and maintenance of all shared policies, procedures, and documentation related to efforts toward HIPAA security compliance;
3. Security incident reporting and investigation, and participation in incident response; and
4. Facilitation of security audits, maintenance of security documents required by the security rule, assisting in the administration and oversight of business associates, and reporting of HIPAA security compliance efforts to the UW-Madison HIPAA Privacy Officer and university leadership.

B. Each unit has a designated HIPAA Security Coordinator as described in Policy # 10.2 "Designation of Unit Privacy and Security Coordinators." In addition to the duties specified in Policy # 10.2, the HIPAA Security Coordinator of a unit is responsible for the development, implementation and maintenance all local policies, procedures, and documentation related to efforts toward HIPAA security compliance in the unit, and has other

HIPAA security oversight duties described in section (III)(B) and in other related policies.

C. Each unit has a designated HIPAA Privacy Coordinator as described in Policy # 10.2 "Designation of Unit Privacy and Security Coordinators." In addition to the duties specified in Policy # 10.2, the HIPAA Privacy Coordinator of a unit has other HIPAA security oversight duties described in section (III)(C) and in other related policies.

D. In some units there may be privacy or security sub-coordinators who have the same duties within their subunits.

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. HIPAA Privacy Coordinator of a unit: A designated individual who serves in that role for a school, college, division, department or individual, as defined in Policy #10.2 "Designation of Unit Privacy and Security Coordinators" with duties further clarified in Policy # 8.2 "Security Oversight" and other related policies.

C. HIPAA Security Coordinator of a unit: A designated individual who serves in that role for a school, college, division, department or individual, as defined in Policy #10.2 "Designation of Unit Privacy and Security Coordinators" with duties further clarified in Policy # 8.2 "HIPAA Security Oversight" and other related policies.

D. 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.

E. UW-Madison Health Care Component (UW-Madison HCC): Schools, colleges, divisions, departments, and certain individuals as designated in Policy # 1.1 "Designation of the UW-Madison Health Care Component".

F. UW-Madison HIPAA Privacy and Security Program Coordinator: A designated individual who serves in that role for all units, with duties that

include but are not limited to those identified in Policy # 8.2 "HIPAA Security Oversight" and other related policies.

G. 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. **UW-Madison HIPAA Security Officer responsibilities.** The Security Officer, in collaboration with the UW-Madison HIPAA Privacy Officer, is responsible for facilitating the development, implementation, and oversight of all activities pertaining to UW-Madison efforts to be compliant with the HIPAA security regulations. The intent of these oversight activities is to maintain the confidentiality, integrity, and availability of ePHI. The responsibilities of the UW-Madison HIPAA Security Officer include, but are not limited to the following.

1. The UW-Madison HIPAA Security officer is a co-chair of the UW-Madison HIPAA Privacy and Security Operations Committee.
2. Advisory duties – The UW-Madison HIPAA Security Officer provides advice and expertise on all matters related to HIPAA security.
    a. The Security Officer is advisory to:
        i. UW-Madison leadership;
        ii. The UW-Madison HIPAA Privacy and Security Executive Board;
        iii. The UW-Madison HIPAA Privacy Officer;
        iv. The HIPAA Privacy Coordinator of each unit;
        v. The HIPAA Security Coordinator of each unit; and
        vi. Anyone who is supporting the HIPAA-related work of the above, such as Trainers, Developers, Human

Resources staff, Information Technology staff, Facilities Managers, etc.

b. Advice may be solicited or unsolicited. The Security Officer will take the initiative to provide needed advice whenever and to whoever seems appropriate in order to help accomplish HIPAA security compliance at UW-Madison.

c. The Security Officer may arrange for additional expertise or assistance as needed, such as security experts, security auditors, etc.

3. Policies and procedures – The UW-Madison HIPAA Security Officer develops, implements and maintains the shared HIPAA security policies and procedures that apply to all units. The Security Officer or delegate:

a. Establishes, updates, and maintains the shared policies and procedures written to comply with the Security rule;

b. Retains the policies and procedures for six years from the date of creation or date it was last in effect, whichever is later;

c. Provides copies of the policies and procedures to management, and has them available for review by all other workforce members to which they apply; and

d. Periodically, and as necessary, reviews and updates the shared policies and procedures in order to respond to environmental or operational changes affecting the security of ePHI.

4. Security incident reporting, investigation and follow up – The UW-Madison HIPAA Security Officer facilitates HIPAA security incident reporting, investigation and follow up processes for ePHI. The Security Officer or delegate:

a. Maintains a program promoting workforce members to report possible security breaches or other non-compliance with security policies and procedures.

b. Promptly, properly, and consistently investigates and addresses reports of possible security breaches and takes steps to prevent recurrence. This investigation focuses on determining what unauthorized access or use of ePHI has occurred (if any). It is distinct from, but related to, the investigation facilitated by the UW-Madison HIPAA Privacy Officer that focuses on the involvement of workforce members in a privacy or security breach or violation of privacy and security policies and procedures which could result in notification to affected individuals or the application of sanctions to workforce members. Care must be taken while investigating a possible security breach so that later investigation of workforce member involvement is not compromised.

c. Promptly reports possible security breaches to the UW-Madison HIPAA Privacy Officer and other designated officials.

d. Works with HIPAA Security Coordinators and IT staff to mitigate to the extent practicable, any harmful effects known to UW-Madison of a use or disclosure of ePHI in violation of HIPAA security policies and procedures.

e. Works in consultation with the appropriate dean or division director, the Office of Human Resources, and the UW-Madison HIPAA Privacy Officer to help assure consistent and appropriate sanctions against workforce members who fail to comply with the security policies and procedures.

5. Incident response – The UW-Madison HIPAA Security Officer participates in the incident response process. The Security Officer or delegate:

a. Is immediately informed of a report of a possible privacy or security breach as outlined in Section III.B. of Policy # 8.8 “Notification and Reporting in the Case of Breach of Unsecured Protected Health Information” ;

b. Remains engaged and continues to receive updates on each active privacy or security response until the Security Officer or delegate determines that ePHI was not involved in the breach; and

c. Serves on any administrative or leadership team that recommends the appropriate response to a possible breach involving ePHI.

6. Authorization and access control – In cases where central (UW-Madison level) security authorization and access controls are appropriate, the UW-Madison HIPAA Security Officer or delegate implements procedures for:

   a. Initial authorization and granting of security access rights for workforce members so they can access specific information resources;

   b. Timely modification of access rights as the need for access changes; and

   c. Termination of access rights in a timely manner, including both event-driven termination and periodic assessments to find those authorizations or access rights that are no longer necessary.

7. Auditing, reporting and documentation – The UW-Madison HIPAA Security Officer or delegate:

   a. Facilitates security assessments and audits to validate security compliance efforts among all units,. including both internal assessments and external audits;

   b. Documents or receives a copy of all documents pertaining to all activities and assessments completed to comply with the Security Rule, and maintains those documents for six years from the date of creation or date it was last in effect, whichever is later;

   c. Assists the UW-Madison HIPAA Privacy Officer and the HIPAA Privacy Coordinator of each unit in the administration and oversight of Business Associates and

agreements, including both Business Associates at UW-Madison and those external to UW-Madison; and

d. Provides timely reports of HIPAA security compliance activities to the UW-Madison HIPAA Privacy Officer and university leadership.

B. **Responsibilities of the HIPAA Security Coordinator of a unit.** Some responsibilities of the HIPAA Security Coordinator are specified in Policy # 10.2 "Designation of Unit Privacy and Security Coordinators." The HIPAA Security Coordinator has additional security oversight duties that include but are not limited to:

1. The HIPAA Security Coordinator of a unit is a member of the UW-Madison HIPAA Privacy and Security Operations Committee.

2. Advisory duties – The HIPAA Security Coordinator is advisory to:

   a. Leadership of the unit;

   b. The HIPAA Privacy Coordinator of the unit;

   c. The HIPAA Security Sub-Coordinators of the unit (if any); and

   d. Anyone who is supporting the HIPAA-related work of the above, such as Human Resources staff, Information Technology staff, Facilities Managers, etc.

3. Policies and procedures –

   a. The HIPAA Security Coordinator of a unit develops, implements and maintains any HIPAA security policies and procedures that apply specifically to that unit.

   b. When a unit's policy must differ from the shared policies, the unit's policy may not be less restrictive. Local policies must be reported to the UW-Madison HIPAA Security Officer so they can be incorporated as exceptions to the shared policies and procedures.

   c. When a procedure must differ from similar procedures specified in the shared policies and procedures, the unit's procedure must be reported to the UW-Madison HIPAA

Security Officer for possible inclusion as an exception to the shared policies and procedures. The Security Officer will determine if inclusion is warranted.

4. Security incident reporting and investigation – After a possible security incident is reported, the HIPAA Security Coordinator of the unit will immediately be informed if that possible security incident involves the Security Coordinator's unit.

5. Incident investigation and response – The HIPAA Security Coordinator of the unit:

    a. May be asked to serve on a team that investigates or makes recommendations regarding the appropriate response to an incident.

    b. Will be informed of the result of any security incident investigation and the response of the institution.

6. Authorization and access control – In cases where security authorization and access controls decisions are made by the unit, the HIPAA Security Coordinator or designee implements procedures for:

    a. Initial authorization and granting of security access rights for unit workforce members so they can access specific information resources in the unit;

    b. Timely modification of access rights as the need for access changes; and

    c. Termination of security access rights in a timely manner, including both event-driven termination and periodic audits to find those authorizations or access rights that are no longer necessary.

7. Assessment, reporting and documentation – The HIPAA Security Coordinator or designee of a unit:

    a. Facilitates self-assessments to improve Security Rule compliance efforts in the unit;

b. Documents or receives a copy of all documents pertaining to all activities and assessments completed by the unit to comply with the Security Rule, and forwards a copy of all of these to the UW-Madison HIPAA Security Officer (in electronic form if available.)

c. Assists the HIPAA Privacy Coordinator of the unit in the administration and oversight of Business Associates and agreements in place with the unit, including both Business Associates at UW-Madison and those external to UW-Madison;

d. Provides timely reports of HIPAA security compliance activities in the unit to the HIPAA Privacy Coordinator and leadership of the unit.

8. Identifying and assisting in the acquisition of necessary resources – This includes resources for:

a. The security compliance-related activities and facilities of the unit; and

b. The unit's contribution to security compliance-related activities and facilities that are shared with other units.

C. **Security-related duties of the HIPAA Privacy Coordinator of a unit.** Some duties of the HIPAA Privacy Coordinator are specified in Policy #10.2 "Designation of Unit Privacy and Security Coordinators." The Privacy Coordinator has additional security oversight duties that include but are not limited to:

1. The HIPAA Security Coordinator of a unit is a member of the UW-Madison HIPAA Privacy and Security Operations Committee.

2. Facilitating the appropriate supervision of all unit workforce members with respect to HIPAA privacy and security matters – The HIPAA Privacy Coordinator works with leaders to implement the following.

a. It is the responsibility of all leaders (i.e. team leaders, supervisors, managers, directors, senior leaders, etc.) to supervise all workforce members, including third party

vendors, contractors or other users of the unit's systems, applications, servers, workstations, etc. that contain ePHI.

b. Leaders monitor workstations and applications for unauthorized use, tampering, and theft and report non-compliance according to Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information."

c. Leaders assist the UW-Madison HIPAA Security Officer, the unit's HIPAA Privacy Coordinator and HIPAA Security Coordinator to ensure appropriate role-based access is provided to all workforce members.

d. Leaders take all reasonable steps to hire, retain, and promote workforce members and provide access to workforce members who comply with the security policies and procedures.

3. Assisting in the appropriate investigation of unit workforce members with respect to HIPAA privacy and security matters – At the direction of the UW-Madison HIPAA Privacy Officer, the HIPAA Privacy Coordinator of a unit assists in the appropriate investigation of any unit workforce member who may be in non-compliance with HIPAA privacy and security policies and procedures. This investigation focuses on the involvement of workforce members in a possible privacy or security breach or violation of privacy and security policies and procedures which could result in notification to affected individuals or the application of sanctions to workforce members. This is distinct from but related to the investigation of a possible security breach which focuses on determining what unauthorized access or use of ePHI has occurred (if any.) While timely investigation of workforce member involvement is important, care must be taken to avoid damaging evidence that might indicate the nature and extent of the possible breach.

a. The HIPAA Privacy Coordinator of a unit works with leaders to foster a culture by which all workforce members and any others with system access report non-compliance

with policies and procedures. Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information" describes the reporting process.

b. At the direction of the UW-Madison HIPAA Privacy Officer, the HIPAA Privacy Coordinator of a unit assists in facilitating a timely and thorough investigation of all reported violations of privacy and security policies and procedures in the unit. The Privacy Coordinator or delegate may request the assistance of others such as Human Resources staff, the workforce member's supervisor, other workforce members, or vendor/contractors as needed. The result is the formation of a team of investigators appropriate to the situation.

c. Investigations are conducted as described in Policy # 9.2 "Responding to Employee Noncompliance with Polices and Procedures Relating to HIPAA Privacy and Security Rules" and Policy # 9.3 "Responding to Student Noncompliance with Policies and Procedures Relating to HIPAA Privacy and Security Rules".

4. Identifying and assisting in the acquisition of necessary resources. This includes resources for:

a. The security compliance-related activities and facilities of the unit; and

b. The unit's contribution to security compliance-related activities and facilities that are shared with other units.

D. Workforce Training. The UW-Madison HIPAA Privacy Officer and UW-Madison HIPAA Security Officer are jointly responsible for development and implementation of privacy and security training that is shared by all units. The HIPAA Privacy Coordinator and HIPAA Security Coordinator of each unit provide assistance, and are also responsible for development and implementation of training that is specific to the unit, (when such is required.) Privacy and security training isdescribed in Policy # 9.1 "HIPAA Privacy and Security Training".

IV. Documentation Requirements

A. The UW-Madison HIPAA Security Officer or delegate documents or receives a copy of all documents pertaining to all HIPAA security oversight activities completed to comply with the Security Rule, and maintains those documents for six years from the date of creation or date it was last in effect, whichever is later.

B. Each HIPAA Security Coordinator or designee documents or receives a copy of all documents pertaining to all HIPAA security oversight activities completed by the unit to comply with the Security rule, and forwards a copy of all of these to the UW-Madison HIPAA Security Officer (in electronic form if available.) The HIPAA Security Coordinator may optionally maintain convenience copies of those documents 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 §164.308(a)(1)(ii)(C) (HIPAA Security Rule – Sanction Policy)
- 45 CFR §164.308(a)(2) (HIPAA Security Rule – Assigned Security Responsibility)
- 45 CFR §164.308(a)(3)(ii)(A) (HIPAA Security Rule – Authorization and/or Supervision)
- 45 CFR §164.308(a)(4) (HIPAA Security Rule – Information Access Management)
- 45 CFR §164.308(a)(4)(ii)(B) (HIPAA Security Rule – Access Authorization)
- 45 CFR §164.308(a)(4)(ii)(C) (HIPAA Security Rule – Access Establishment and Modification)
- 45 CFR §164.308(a)(5)(i) (HIPAA Security Rule – Security Awareness and Training)
- 45 CFR §164.308(a)(5)(ii)(A) (HIPAA Security Rule – Security Reminders)

- 45 CFR §164.308(a)(6)(i-ii) (HIPAA Security Rule – Response and Reporting)
- 45 CFR §164.316(a-b) (HIPAA Security Rule – Documentation)

Resources

- HIPAA Collaborative of Wisconsin Security Oversight Policy
- HIPAA Collaborative of Wisconsin Security Oversight Whitepaper
- UW-Madison IT Security "Departmental IT Security Baseline"

VII. Related Policies

- Policy # 1.1 "Designation of the UW-Madison Health Care Component"
- Policy # 8.1 "HIPAA Security Risk Management"
- Policy # 8.3 "HIPAA Security Auditing"
- Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information"
- Policy # 9.1 "HIPAA Privacy and Security Training"
- Policy # 9.2 "Responding to Employee Noncompliance with Polices and Procedures Relating to HIPAA Privacy and Security Rules"
- Policy # 9.3 "Responding to Student Noncompliance with Policies and Procedures Relating to HIPAA Privacy and Security Rules"
- Policy # 10.2 "Designation of Unit Privacy and Security Coordinators"
- UW-Madison "Information Incident Reporting and Response"

The HIPAA policies listed above are located at: http://www.hipaa.wisc.edu/. The UW-Madison policies are at: http://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 Privacy Coordinator or 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