University of Wisconsin-Madison
Policy and Procedure

Policy Number: 8.1
Policy Title: HIPAA Security Risk Management
Effective Date: December 22, 2014
Last Revision Date: December 8, 2014

I. Policy

A. It is the policy of the University of Wisconsin-Madison for each unit of the UW-Madison Health Care Component and each individual or unit within UW-Madison that is a Business Associate of a covered entity (hereafter collectively referred to as "units") to conduct thorough and timely risk assessments of the potential threats and vulnerabilities to the confidentiality, integrity, and availability of its electronic protected health information (ePHI) (and other confidential and proprietary electronic information) and to develop strategies to efficiently and effectively reduce the risks identified in the assessment process.

B. Risk analysis and risk management are integral components of each unit's compliance program and Information Technology (IT) security program in accordance with the Risk Analysis and Risk Management implementation specifications within the Security Management standard and the Evaluation standard set forth in the HIPAA Security Rule, 45 CFR §164.308(a)(1)(ii)(A) Risk Analysis, §164.308(a)(1)(ii)(B) Risk Management, §164.308(a)(1)(i) Security Management Process, and §164.308(a)(8) Evaluation.

1. Risk assessments are done throughout IT system life cycle:

   a. Before the purchase or integration of new technologies and Changes are made to physical safeguards;

   b. While integrating technology and making physical security changes; and

   c. While sustaining and monitoring appropriate security controls.

2. Each unit performs periodic technical and non-technical assessments of compliance with the security rule requirements, with additional assessments in response to environmental or operational changes affecting the security of ePHI.

C. Each unit implements security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to:

1. Ensure the confidentiality, integrity, and availability of all ePHI the unit creates, receives, maintains, and/or transmits;
2. Protect against any reasonably anticipated threats or hazards to the security or integrity of ePHI;
3. Protect against any reasonably anticipated uses or disclosures of ePHI that are not permitted or required; and
4. Ensure compliance by workforce.

D. All unit workforce members are expected to fully cooperate with all persons charged with doing risk management work. Any workforce member that violates this policy will be subject to disciplinary action based on the severity of the violation according to Policy # 9.2 "Responding to Employee Noncompliance with Policies and Procedures Relating to the HIPAA Privacy and Security Rules".

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. 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.

E. Risk Assessment: (referred to as *Risk Analysis* in the HIPAA Security Rule) The process that:

- Identifies the risks to information system security and determines the probability of occurrence and the resulting impact for each threat / vulnerability pair identified given the security controls in place;
- Prioritizes risks; and
- Results in recommended possible actions/controls that could reduce or offset the determined risk.

F. Risk Management: Within this policy, it refers to two major process components, risk assessment and risk mitigation. This differs from the HIPAA Security Rule, which defines it as a risk mitigation process only. The definition used in this policy is consistent with the one used in documents published by the National Institute of Standards and Technology (NIST).

G. Risk Management Team: Individuals who are knowledgeable about the Organization's HIPAA Privacy, Security and HITECH policies, procedures, training program, computer system set up, and technical security controls, and who are responsible for the risk management process and procedures outlined below. For each unit, the members of the Risk Management Team will include:

- The HIPAA Privacy Coordinator of the unit (chair);
- The HIPAA Security Coordinator of the unit;
- The Information Security Officer (or the equivalent) of the unit, (if different);
- The Chief Information Officer (CIO) or IT Director (or the equivalent) of the unit, (if different);
- The Business Manager (or the equivalent) of the unit;
- The UW-Madison HIPAA Security Officer or delegate;
- Representative members of the faculty and staff of the unit; and
- Designated subject matter experts.

H. Risk Mitigation: **(**referred to as *Risk Management* in the HIPAA Security Rule,) A process that prioritizes, evaluates, and implements security controls that will reduce or offset the risks determined in the risk

assessment process to satisfactory levels within an organization given its mission and available resources.

I. Threat: The potential for a particular threat source to cause loss or to successfully exploit a particular vulnerability. Threats are commonly categorized as:

- Environmental – internal fires, HVAC failure/temperature inadequacy, water pipe burst, power failure/fluctuation; etc.
- Human – hackers, data entry, workforce/ex-workforce members, impersonation, insertion of malicious code, theft, viruses, SPAM, vandalism; etc.
- Natural – fires, floods, electrical storms, tornados; etc.
- Technological – server failure, software failure, ancillary equipment failure, etc.; and
- Other – explosions, medical emergencies, misuse or resources, etc.

J. Threat Source: Any person, circumstance or event with the potential to cause harm (intentional or unintentional) to an IT system. Common threat sources can be natural, human or environmental which can impact the organization's ability to protect ePHI.

K. 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".

L. Vulnerability: A weakness or flaw in an information system that can be accidentally triggered or intentionally exploited by a threat and lead to a compromise in the integrity of that system, (i.e., resulting in a security breach or violation of policy.)

III. Procedures

A. The implementation, execution, and maintenance of the information security Risk Analysis and Risk Management processes is the responsibility of the UW-Madison HIPAA Security Officer, assisted by each unit's Risk Management Team.

B. **Risk Assessment:** The intent of completing a risk assessment is to determine potential threats and vulnerabilities, and the likelihood and impact should they occur. The output of this process helps to identify appropriate security controls for reducing or eliminating risk. There are a variety of methods that are suitable for HIPAA risk assessment. The following is one such method. Consistency of risk assessment methods among units and over time is helpful and encouraged.

1. System Characterization

   a. The first step in assessing risk is to define the scope of the effort. To do this, identify where ePHI is created, received, maintained, processed, or transmitted. Using information-gathering techniques, the IT system boundaries are identified, as well as the resources and the information that constitute the system. Take into consideration policies, laws, the remote work force and telecommuters, and removable media and portable computing devices (e.g., laptops, removable media, and backup media). (To assist with these efforts, see the HIPAA Collaborative of Wisconsin "Risk Analysis & Risk Management Toolkit – Network Diagram Example and Inventory Asset List".)

   b. *Output* – Characterization of the IT system assessed, a good picture of the IT system environment, and delineation of system boundaries.

2. Threat Identification

   a. In this step, potential threats are identified and documented. Consider all potential threat sources through the review of historical incidents and data from intelligence agencies, the government, etc., to help generate a list of potential threats. The list should be based on the individual organization and its processing environment. (See the HIPAA Collaborative of Wisconsin "Risk Analysis & Risk Management Toolkit –Threat Overview" for definitions and the " Threat Source List" in the Risk Assessment for examples of threat sources.)

b. *Output* – A threat statement containing a list of potential threat sources that could exploit system vulnerabilities.

3. Vulnerability Identification

   a. The goal of this step is to develop a list of technical and non-technical system vulnerabilities that could be exploited or triggered by the potential threat sources. Vulnerabilities can range from incomplete or conflicting policies that govern an organization's computer usage to insufficient security controls to protect facilities that house computer equipment to any number of software, hardware, or other deficiencies that comprise an organization's computer network. (See the HIPAA Collaborative of Wisconsin "Risk Analysis & Risk Management Toolkit – Risk Assessment Template – Security Questions and Threat Source List".)

   b. *Output* – A list of system vulnerabilities that could be exploited by the potential threat sources.

4. Control Analysis

   a. The goal of this step is to document and assess the effectiveness of technical and non-technical security controls that have been or will be implemented by the organization to reduce the likelihood of a threat source exploiting a system vulnerability.

   b. *Output* – A list of current or planned security controls used for the IT system to reduce the likelihood of a vulnerability being exploited by a threat source and to reduce the impact of such an adverse event.

5. Likelihood Determination

   a. The goal of this step is to determine the overall likelihood rating that indicates the probability that a vulnerability could be exploited by a threat source given the existing or planned security controls. (See the HIPAA Collaborative of Wisconsin "Risk Analysis & Risk Management Toolkit

– Risk Likelihood, Risk Impact, and Risk Level Definitions".)

b. *Output* – A likelihood rating for each threat source / vulnerability pair of low (.1), medium (.5), or high (1). Refer to the NIST SP 800-30 definitions of low, medium, and high.

6. Impact Analysis

a. The goal of this step is to determine the level of adverse impact that would result from a threat source successfully exploiting a vulnerability. Factors of the data and systems to consider should include the importance to the organization's mission; sensitivity and criticality (value or importance); and associated costs that could result from the loss of confidentiality, integrity, and availability of systems and data. (See the HIPAA Collaborative of Wisconsin "Risk Analysis & Risk Management Toolkit – NIST Risk Likelihood, Risk Impact, and Risk Level Definitions".)

b. *Output* – Magnitude of impact rating for each threat source / vulnerability pair of low (10), medium (50), or high (100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

7. Risk Determination

a. This step is intended to establish a risk level. By multiplying the ratings from the likelihood determination and impact analysis, a risk level is determined. This represents the degree or level of risk to which an IT system, facility, or procedure might be exposed if a given vulnerability were exploited. The risk rating also presents actions that senior management (the mission owners) might take for each risk level. (See the HIPAA Collaborative of Wisconsin "Risk Analysis & Risk Management Toolkit – NIST Risk Likelihood, Risk Impact, and Risk Level Definitions".)

b. *Output* – Risk level for each threat source / vulnerability pair of low (1-10), medium (>10-50) or high (>50-100). Refer to the NIST SP 800-30 definitions of low, medium, and high.

8. Control Recommendations

a. The purpose of this step is to identify security controls that could reduce the identified risks to an acceptable level. Factors to consider when developing security controls may include effectiveness of recommended options, legislation and regulation, organizational policy, operational impact, safety, and reliability. Security control recommendations provide input to the risk mitigation process, during which the recommended technical and non-technical security controls are evaluated, prioritized, and implemented. (See the HIPAA Collaborative of Wisconsin "Risk Analysis & Risk Management Toolkit – NIST - Risk Mitigation Activities".)

b. *Output* – Recommendation of security controls and alternative solutions to reduce risk.

9. Results Documentation

a. Results of the risk assessment are documented in an official report or briefing and provided to senior management of the unit, the UW-Madison HIPAA Privacy and Security Operations Committee, and the UW-Madison HIPAA Privacy and Security Executive Board, so they can make decisions on policy, procedure, budget, and system operational and management changes. (See the HIPAA Collaborative of Wisconsin "Risk Analysis & Risk Management Toolkit –Risk Analysis Report Template".)

b. *Output* – A risk assessment report that describes the threats and vulnerabilities, measures the risk, and provides recommendations for security control implementation.

C. **Risk Mitigation:** Risk mitigation involves prioritizing, evaluating, and implementing the appropriate risk-reducing security controls

recommended from the risk assessment process to ensure the confidentiality, integrity and availability of ePHI. Determination of appropriate security controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission. There are a variety of methods that are suitable for HIPAA risk mitigation. The following is one such method. Consistency of risk mitigation methods among units and over time is helpful and encouraged.

1. Prioritize Actions

    a. Using results from Step 7 of the Risk Assessment, sort the threat source / vulnerability pairs according to their risk-levels in descending order. This establishes a prioritized list of actions that need to be taken, with the pairs at the top of the list getting/requiring the most immediate attention and top priority in allocating resources.

    b. *Output* – Actions ranked from high to low priority.

2. Evaluate Recommended Control Options

    a. Although possible security controls for each threat source / vulnerability pair are listed in Step 8 of the Risk Assessment, review the recommended security controls and alternative solutions for reasonableness and appropriateness. The feasibility, (e.g. compatibility, user acceptance, etc.,) and the effectiveness, (e.g. degree of protection and level of risk reduction,) of the recommended security controls should be analyzed.

    b. *Output* – A list of the "most appropriate" security control option for each threat source / vulnerability pair..

3. Conduct Cost-Benefit Analysis

    a. Determine the extent to which a security control is cost-effective. Compare the benefit (e.g., risk reduction) of applying a security control with its subsequent cost of application. Security controls that are not cost-effective are also identified during this step. Analyzing each security control or set of controls in this manner, and prioritizing

across all security controls being considered, can greatly aid in the decision-making process.

b. *Output* – Documented cost- benefit analysis of either implementing or not implementing each specific security control.

4. Select Controls

a. Taking into account the information and results from previous steps, the unit's mission, and other important criteria, the Risk Management Team determines the best security controls for reducing risks to the information systems and to the confidentiality, integrity, and availability of ePHI. These security controls may consist of a mix of administrative, physical, and/or technical safeguards, and other technical and non-technical controls.

b. *Output* – Selected security controls, with rationale for selecting the controls and for not selecting other controls that were considered.

5. Assign Responsibility

a. Identify the individual(s) or team with the skills necessary to implement each of the specific security controls listed in the previous step, and assign their responsibilities. Also identify the equipment, training and other resources needed for the successful implementation of security controls. Resources may include time, money, equipment, etc.

b. *Output* – A list of responsible persons, their assignments, and other necessary resources.

6. Develop Safeguard Implementation Plan

a. Develop an overall implementation plan and individual project plans needed to implement the identified security controls. The Implementation Plan should contain the following information:

i. Each risk or threat / vulnerability pair and risk level;

ii. Prioritized actions;

iii. The selected security controls for each identified risk;

iv. Required resources for implementation of the controls;

v. Team member responsible for implementation of each control;

vi. Start date for implementation;

vii. Target date for completion of implementation; and

viii. Maintenance requirements.

b. The overall implementation plan provides a broad overview of the implementation of the security controls, identifying important milestones and timeframes, resource requirements, (e.g. staff and other individuals' time, budget, etc.,) interrelationships between projects, and any other relevant information. Regular status reporting of the plan, along with key metrics and success indicators is reported to the HIPAA Privacy and Security Operations Committee, which further reports such status information to the HIPAA Privacy and Security Executive Board.

c. Individual project plans for implementation of the security controls may be developed and contain detailed steps that assigned resources carry out to meet implementation timeframes and expectations. (This is often referred to as a work breakdown structure). Additionally, consider including items in individual project plans such as a project scope, a list deliverables, key assumptions, objectives, task completion dates, and project requirements.

d. *Output* – Safeguard implementation plan.

7. Implement Selected Controls – as security controls are implemented, monitor the affected system(s) to verify that the implemented controls continue to meet expectations.

a. Continually and consistently communicate expectations to all Risk Management Team members, as well as senior management and to the HIPAA Privacy and Security Operations Committee throughout the risk mitigation process.

b. Additional monitoring is especially crucial during times of major environmental changes, organizational or process changes, or major facilities changes.

c. If risk reduction expectations are not met, then repeat all or a part of the risk management process so that additional controls needed to lower risk to an acceptable level can be identified.

d. Identify when new risks are found and when security controls lower or offset risk rather than eliminate it.

e. *Output* – Safeguard Implementation Plan project documentation, and identified residual risk levels.

8. Residual Risk Acceptance

a. Any residual risk remaining after other risk controls have been applied requires sign off by the:

- HIPAA Security Coordinator of the unit;
- HIPAA Privacy Coordinator of the unit;
- Senior leadership of the unit;
- UW-Madison HIPAA Security Officer; and
- UW-Madison HIPAA Privacy Officer.

b. *Output* – Risk acceptance documentation.

D. **Risk Management Schedule:** The two principle components of the risk management process - risk assessment and risk mitigation - will be carried out according to the following schedule to ensure the continued adequacy and improvement of the unit's information security program.

1. Scheduled Basis – an overall risk assessment of each unit's information system infrastructure will be conducted every three years. The assessment process should be completed in a timely fashion so that risk mitigation strategies can be determined and included in the budgeting process.
2. Throughout a System's Development Life Cycle – from the time that a need for a new information system is identified through the time it is disposed of, ongoing assessments of the potential threats to a system and its vulnerabilities should be undertaken as a part of the maintenance of the system.
3. As Needed – the HIPAA Privacy Coordinator of the unit, the HIPAA Security Coordinator of the unit, the UW-Madison HIPAA Privacy Officer, or the UW-Madison HIPAA Security Officer may call for a full or partial risk assessment in response to changes in business strategies, information technology, information sensitivity, threats, legal liabilities, or other significant factors that affect the unit's information systems.

IV. Documentation Requirements

A. The UW-Madison HIPAA Security Officer or delegate documents or receives a copy of all documents pertaining to risk assessments and risk mitigation 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 documents or receives a copy of all documents pertaining to to risk assessments and risk mitigation 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 §164.302-306 (HIPAA Security Rule – General Requirements)
- 45 CFR §164.308(a)(1)(i) (HIPAA Security Rule – Security Management Process)
- 45 CFR §164.308(a)(1)(ii)(A) (HIPAA Security Rule – Risk Analysis)
- 45 CFR §164.308(a)(1)(ii)(B) (HIPAA Security Rule – Risk Management
- 45 CFR §164.308(a)(8) (HIPAA Security Rule – Evaluation)
- 45 CFR §164.316(a-b) (HIPAA Security Rule – Documentation)

Resources

- HIPAA Collaborative of Wisconsin Risk Management Policy
- HIPAA Collaborative of Wisconsin Risk Management Toolkit
- NIST Risk Management Guide for Information Technology Systems, Special Publication 800-30, July 2002.
- NIST Security Self Assessment Guide for Information Technology Systems 800-26

VII. Related Policies

- Policy # 1.1 "Designation of the UW-Madison Health Care Component"
- Policy # 6.1 "Managing Arrangements with Business Associates of University of Wisconsin-Madison"
- Policy # 6.2 "Managing Business Associate Arrangements When the University of Wisconsin-Madison is the Business Associate"
- Policy # 6.3 "Use of and Safeguards for Protected Health Information by UW-Madison Internal Business Support Personnel"
- Policy # 8.2 "HIPAA Security Oversight"
- Policy # 8.3 "HIPAA Security Auditing"
- Policy # 8.4 "HIPAA Security Contingency Planning"
- Policy # 8.6 "E-mail Communication Involving Protected Health Information"
- Policy # 8.7 "Destruction/Disposal of Protected Health Information"
- Policy # 8.8 "Notification and Reporting in the Case of Breach of Unsecured Protected Health Information"
- Policy # 8.9 "HIPAA Security System Access"
- Policy # 8.10 "HIPAA Security Remote Access"

- Policy # 8.11 "HIPAA Security Data Management and Backup"
- Policy # 8.12 "HIPAA Security Facilities Management"
- Policy # 9.1 "HIPAA Privacy and Security Training"
- Policy # 9.2 "Responding to Employee Noncompliance with Polices and Procedures Relating to the HIPAA Privacy and Security Rules"
- Policy # 9.3 "Responding to Student Noncompliance with Policies and Procedures Relating to the HIPAA Privacy and Security Rules"
- Policy # 10.2 "Designation of Unit Privacy and Security Coordinators"
- UW-Madison "Computer Logging Statement"
- UW-Madison "Electronic Devices Connected to the UW-Madison Network"
- UW-Madison "Information Incident Reporting and Response"
- UW-Madison "IT Compliance Agreement"
- UW-Madison "Media and Device Disposal and Reuse"
- UW-Madison "NetID Appropriate Use Standards"
- UW-Madison "Password Standard"
- UW-Madison "Responsible Use of Information Technology"
- UW-Madison "Restricted Data Management"
- UW-Madison "Sensitive Information Definition"
- UW-Madison "Storage and Encryption of Sensitive Information"
- UW-Madison "Storage, Transmission, and Encryption of Sensitive Information" (draft)
- UW-Madison "Use of Institutional Access Control Services"
- UW-Madison "Vulnerability Scanning"

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