
**University of Wisconsin-Madison
Policy and Procedure**

Policy Number: 8.4
Policy Title: HIPAA Security Contingency Planning
Effective Date: March 10, 2015
Last Revision Date: February 12, 2015
Page 1 of 5

I. Policy

- A. The units 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”) shall be included in an appropriate Continuity of Operations Plan (COOP) which has been suitably developed or modified to address the standards set forth by the HIPAA Security rule.
- B. The COOP documentation and templates provided by the University of Wisconsin Police Department do not explicitly address the specific needs of a unit that stores or processes ePHI. The following components must be included in a COOP in order to meet the requirements of the HIPAA Security rule. The COOP must:
1. Establish and implement procedures to create and maintain retrievable exact copies of ePHI.
 2. Establish (and implement as needed) procedures to restore any loss of ePHI.
 3. Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.
 4. Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
 5. Establish and implement procedures to preserve (and as needed restore) documentation needed for compliance with the HIPAA Security rule.
 6. Establish and implement procedures that, to the extent practical, preserve (and as needed restore) security audit data needed for compliance with the HIPAA Security rule.
 7. Establish (and implement as needed) procedures that allow facility access in support of the procedures established in items 1. to 6. above.

**University of Wisconsin-Madison
Policy and Procedure**

Policy Number: 8.4
Policy Title: HIPAA Security Contingency Planning
Effective Date: March 10, 2015
Last Revision Date: February 12, 2015
Page 2 of 5

8. Establish and implement procedures for periodic testing and revision of, at a minimum, those components of the COOP that involve or affect items 1. to 7. above.
 9. Incorporate into the COOP procedures the assessment of the relative criticality of specific applications and data that store or process ePHI.
- C. Responsibility for the procedures listed in I.B. is among the duties of the UW-Madison HIPAA Security Officer and the HIPAA Security Coordinator of each unit, as described in Policy # 8.2 “HIPAA Security Oversight”.

II. Definitions

- A. Continuity of Operations Plan (“COOP”): A unit’s COOP is activated if a disaster or emergency severely affects the unit. The plan ensures delivery of essential functions and guides the ‘rebuilding’ of the affected unit.
- B. Electronic Protected Health Information (“ePHI”): Any individually identifiable health information protected by HIPAA that is transmitted by or stored in electronic media.
- C. 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.

III. Procedures

Each unit should already be covered by the COOP of their school, college or division, (or some other parent organizational entity within UW-Madison.)

- A. If the unit is already covered by a COOP, that plan should be modified in order to meet the minimum requirements for a COOP that includes within its scope a unit that stores or processes ePHI, as defined in I.B. above.
- B. If the unit not already covered by a COOP, the unit should be included in an existing COOP, develop its own COOP, or participate in the

**University of Wisconsin-Madison
Policy and Procedure**

Policy Number: 8.4
Policy Title: HIPAA Security Contingency Planning
Effective Date: March 10, 2015
Last Revision Date: February 12, 2015
Page 3 of 5

development of a broader COOP that includes the unit. The instructions and templates for development of a COOP are provided by the University of Wisconsin Police Department at: <http://uwpd.wisc.edu/continuity-of-operations-plans-coop/>.

- C. While the COOP described in A. or B. above is being modified or developed, the unit should implement an interim version of the procedures that meet the minimum requirements for a COOP that includes within its scope a unit that stores or processes ePHI, as defined in I.B. above.

IV. Documentation Requirements

The UW-Madison HIPAA Security Officer, and the HIPAA Security Coordinator of each unit will assure that copies of the COOP or procedures are retained as described in the Documentation Requirements of Policy # 8.2 “HIPAA Security Oversight”.

V. Forms

There are no COOP forms specific to the HIPAA Security rule. Many forms and checklists are part of the COOP documentation and templates at: <http://uwpd.wisc.edu/continuity-of-operations-plans-coop/>. Some or all of these may be incorporated into a particular COOP.

VI. References

- 45 CFR § 164.308(a)(7)(i) (HIPAA Security Rule – Contingency Plan)
- 45 CFR § 164.308(a)(7)(ii)(A) (HIPAA Security Rule – Data Backup Plan)
- 45 CFR § 164.308(a)(7)(ii)(B) (HIPAA Security Rule – Disaster Recovery Plan)
- 45 CFR § 164.308(a)(7)(ii)(C) (HIPAA Security Rule – Emergency Mode Operation Plan)
- 45 CFR § 164.308(a)(7)(ii)(D) (HIPAA Security Rule – Testing and Revision Procedures)

**University of Wisconsin-Madison
Policy and Procedure**

Policy Number: 8.4
Policy Title: HIPAA Security Contingency Planning
Effective Date: March 10, 2015
Last Revision Date: February 12, 2015
Page 4 of 5

- 45 CFR § 164.308(a)(7)(ii)(E) (HIPAA Security Rule – Applications and Data Criticality Analysis)
- 45 CFR § 164.310(a)(2)(i) (HIPAA Security Rule – Facility Access Controls/Contingency Operations)
- 45 CFR § 164.312(a)(2)(ii) (HIPAA Security Rule – Emergency Access Procedure)
- 45 CFR § 164.316(a-b) (HIPAA Security Rule – Documentation)

Resources

- HIPAA Collaborative of Wisconsin “Contingency Planning Whitepaper”
- UW-Madison Police Department “Continuity of Operations Plan”
- 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 Management”
- Policy # 8.2 “HIPAA Security Oversight”
- Policy # 8.11 “HIPAA Security Data Management and Backup”
- Policy # 8.12 “HIPAA Security Facilities Management”

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

**University of Wisconsin-Madison
Policy and Procedure**

Policy Number: 8.4
Policy Title: HIPAA Security Contingency Planning
Effective Date: March 10, 2015
Last Revision Date: February 12, 2015
Page 5 of 5

UW-Madison Office of Legal Affairs

Approved By

Interim HIPAA Privacy and Security Operations Committee