University of Wisconsin-Madison
Policy and Procedure

Policy Number: 8.11
Policy Title: HIPAA Security Data Management and Backup
Effective Date: June 9, 2015
Last Revision Date: February 12, 2015

I. Policy

A. It is the policy of the University of Wisconsin-Madison that 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"), will protect the confidentiality, integrity and availability of electronic Protected Health Information (ePHI), by implementing sound data management and backup practices that include, but are not limited to, the activities described in this policy below.

B. The unit establishes and implements procedures to create and maintain retrievable exact backup copies of electronic protected health information as required by 45 CFR § 164.308(a)(7)(ii)(A) (HIPAA Security Rule – Contingency Plan – Data Backup Plan). The procedures will assure that complete, accurate, retrievable, and tested back-ups are available for all ePHI on all information systems used by the unit, with the following exceptions.

1. Additional copies of ePHI created for convenience do not need to be backed up, provided that the original copy is properly backed up and available as required by the HIPAA Security Rule.

2. Data sets containing ePHI which were generated from other data sets do not need to be backed up, provided that the original data sets containing ePHI are properly backed up and available as required by the HIPAA Security Rule, and it is possible to recreate enough of the generated data set in a timely manner so that ePHI in the generated data set is available as required by the HIPAA Security Rule.

C. The unit creates a retrievable exact backup copy of electronic protected health information (ePHI) before movement of equipment as required by 45 CFR § 164.310(d)(2)(iv) (HIPAA Security Rule – Device and Media Controls – Data Backup and Storage). The same exceptions listed in section I.B. apply.

D. The unit maintains a record of movements of hardware and electronic media containing ePHI and any person responsible therefore, as required

by 45 CFR § 164.310(d)(2)(iii) (HIPAA Security Rule – Device and Media Controls – Accountability).

E. The unit creates and stores backup copies in accordance with their Safeguard Implementation Plan (or the equivalent) as described in Policy # 8.1 "HIPAA Security Risk Management". The unit creates backup copies at a sufficient frequency and retains them in safe locations for a sufficient length of time to accomplish all of the following:

1. Data backups that enable the restoration of ePHI that is lost or corrupted.
2. Data backups that support the unit's Disaster Recovery Plan (or the equivalent) as required by 45 CFR § 164.308(a)(7)(ii)(B) (HIPAA Security Rule – Contingency Plan – Disaster Recovery Plan) and as described in Policy # 8.4 "HIPAA Security Contingency Planning".
3. Data backups that support the unit's Emergency Mode Operations Plan (or the equivalent) as required by 45 CFR § 164.308(a)(7)(ii)(C) (HIPAA Security Rule – Contingency Plan – Emergency Mode Operations Plan) and as described in Policy # 8.4 "HIPAA Security Contingency Planning".
4. Data backups that support the unit's mechanisms to authenticate ePHI, as required by 45 CFR § 164.312(c)(2) (HIPAA Security Rule – Integrity – Mechanism to Authenticate Electronic Protected Health Information) and as described in Policy # 8.3 "HIPAA Security Auditing".

F. Data backups will be tested according to the requirements of 45 CFR § 164.308(a)(7)(ii)(D) (HIPAA Security Rule – Contingency Plan – Testing and Revision Procedures) as described in Policy # 8.4 "HIPAA Security Contingency Planning".

G. Responsibility for compliance with 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. Backup: The process of making an electronic copy of data stored in a computer system. Examples of backups include:

1. Full/Complete Backup - a backup/image of all (selected) data, programs, files on the system;
2. Incremental Backup - a backup that only contains the files that have changed since the most recent backup (either full or incremental);
3. Snap-shot back-up (image backup) - a process to restore/recover the system at a particular state, at a particular point in time;
4. In the event a system does not allow for an electronic backup, the unit will develop an alternative method to create a copy of the ePHI contained on that system.

B. Business Associate: A person or entity that performs or assists in performing, for or on behalf of a covered entity, business support functions/services that involve the use of Protected Health Information.

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

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.

III. Procedures

A. Data Backup

1. The UW-Madison HIPAA Security Officer has oversight responsibility and the Security Officer or delegate will work with each unit's HIPAA Security Coordinator to ensure that responsibility is further assigned within the unit.

2. A backup, recovery and testing strategy should be determined based upon the unit's Safeguard Implementation Plan (or the equivalent) as described in Policy # 8.1 "HIPAA Security Risk Management".
3. The following is typical of backup arrangements, and can be used as a template for variation:
    a. A typical arrangement includes a daily backup of data that has changed on all systems that create, receive, maintain, or transmit ePHI.
    b. Data backup systems may be manual or automated. Automated systems electronically capture back up locations, date/time, etc. If the process is manual, documentation of the backup should include:
        i. Site/location name;
        ii. Name of the system;
        iii. Type of data;
        iv. Date & time of backup;
        v. Where backup is stored (or to whom it was provided);
        vi. Signature of individual that completed the back up.
4. Stored backups must be sufficiently accessible and retrievable to meet the specifications of the unit's Continuity of Operations Plan (or the equivalent) as described in Policy # 8.4 "HIPAA Security Contingency Planning".
5. All media used for backing up ePHI must be stored in a physically secure environment, such as a secure, off-site storage facility or, if backup media remains on site, in a physically secure location, different from the location of the computer systems it backed up (i.e., in a location that protects the backups from loss or environmental damage).
6. If an off-site storage facility or backup service is used, a Business Associate Agreement (BAA) must be used to ensure that the

Business Associate will safeguard the ePHI in an appropriate manner. A BAA might not be needed for off-site storage or backup services at certain UW-Madison facilities. This will need to be evaluated on a case-by-case basis by the UW-Madison HIPAA Privacy Officer and the UW-Madison HIPAA Security Officer.

7. When reusable media such as tapes are used as the back up media, refer to Policy # 8.7 "Destruction/Disposal of Protected Health Information" and UW-Madison "Media and Device Disposal and Reuse".

8. Data backups should be tested and data restored, to assure accuracy. Documentation of backup testing, or restore logs, should be maintained and should capture the date and time the data was restored. Operational procedures for backup, recovery, and testing should be documented and periodically reviewed.

9. Proper management of situations concerning data back-up and data recovery, such as emergencies or other occurrences, should be addressed in the unit's Continuity of Operations Plan (or the equivalent) as described in Policy # 8.4 "HIPAA Security Contingency Planning".

B. **Destruction**

1. The unit will determine an appropriate schedule for retention of data backups. This schedule should include a timeline for ultimate destruction of reusable storage media.

2. Refer to Policy # 8.7 "Destruction/Disposal of Protected Health Information" and UW-Madison "Media and Device Disposal and Reuse" when records are disposed of, or storage media containing ePHI is re-used or disposed of.

C. **Media Handling**

It is not possible or economically practical to control all media that enter and leave an organization.

1. The unit will make reasonable and prudent efforts to control media entering and leaving the organization.

2. Media that contains PHI that is no longer useful or useable should be sanitized or disposed of consistent with Policy # 8.7 "Destruction/Disposal of Protected Health Information" and UW-Madison "Media and Device Disposal and Reuse".

D. **Sanctions**

1. Failure to back up a system in the absence of a system failure is a violation of this policy.

2. Violation of this policy and its procedures by workforce members may result in sanctions as described in Policy # 9.2 "Responding to Employee Noncompliance with Polices and Procedures Relating to the HIPAA Privacy and Security Rules".

3. Violation of the policy and procedures by others, including providers, providers' offices, business associates and partners may result in termination of the relationship and/or associated privileges.

IV. Documentation Requirements

The UW-Madison HIPAA Security Officer, the HIPAA Security Coordinator of each unit, and other custodians of records or documentation related to the HIPAA Data Management and Backup policy and procedures will assure 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 § 164.308(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)
- 45 CFR § 164.310(a)(2)(i) (HIPAA Security Rule – Facility Access Controls/Contingency Operations)
- 45 CFR 164.310(d)(2)(iii) (HIPAA Security Rule – Accountability)
- 45 CFR 164.310(d)(2)(iv) (HIPAA Security Rule – Data Backup and Storage)
- 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 "Data Management and Backup" policy template.
- HIPAA Collaborative of Wisconsin "Risk Analysis and Risk Management Toolkit" at http://hipaacow.org/resources/hipaa-cow-documents/risk-toolkit
- 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 # 8.7 "Destruction/Disposal of Protected Health Information"
- Policy # 8.12 "HIPAA Security Facilities Management"
- Policy # 9.2 "Responding to Employee Noncompliance with Polices and Procedures Relating to the HIPAA"
- UW-Madison "Media and Device Disposal and Reuse"

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