Policy Summary

1. 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.

2. 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 backups are available for all ePHI on all information systems used by the unit, with the following exceptions.

   2.1 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.

   2.2 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.

3. 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.

4. 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).

5. 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:
5.1 Data backups that enable the restoration of ePHI that is lost or corrupted.

5.2 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”.

5.3 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”.

5.4 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”.

6. 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”.

7. 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”.

Who This Policy Applies To

Applies to all members of the UW-Madison Health Care Component.

Rationale

In enacting HIPAA, Congress mandated the establishment of Federal standards for the privacy of individually identifiable health information. Under the patchwork of laws existing prior to adoption of HIPAA and the Privacy Rule, personal health information could be distributed—without either notice or authorization—for reasons that had nothing to do with a patient’s medical treatment or health care reimbursement. For example, unless otherwise forbidden by State or local law, without the Privacy Rule patient information held by a health plan could, without the patient’s permission, be passed on to a lender who could then deny the patient’s application for a home mortgage or a credit card, or to an employer who could use it in personnel decisions. The Privacy Rule establishes a Federal floor of safeguards to protect the confidentiality of medical information. State laws which provide stronger privacy protections apply over and above the new Federal privacy standards.

Policy Detail

1. Data Backup

1.1 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.

1.2 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”.
1.3 The following is typical of backup arrangements, and can be used as a template for variation:

1.3.1 A typical arrangement includes a daily backup of data that has changed on all systems that create, receive, maintain, or transmit ePHI.

1.3.2 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:

- Site/location name;
- Name of the system;
- Type of data;
- Date & time of backup;
- Where backup is stored (or to whom it was provided);
- Signature of individual that completed the back up.

1.4 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”.

1.5 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).

1.6 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.

1.7 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”.

1.8 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.

1.9 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”.

2. Destruction
2.1 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.

2.2 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.

3. Media Handling

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

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

3.2 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”.

4. Sanctions

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

4.2 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”.

4.3 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.

**Consequences for Non-Compliance**

Failing to comply with this policy may result in discipline for the individual(s) responsible for such non-compliance.

Further, the US Department Health and Human Services (HHS) Office for Civil Rights (OCR) is responsible for enforcing the HIPAA Privacy and Security Rules, and an individual’s non-compliance may result in institutional non-compliance and/or an investigation by OCR. OCR attempts to resolve investigations by obtaining voluntary compliance and entering into Corrective Action Plans and Resolution Agreements. Failures to comply with HIPAA or cooperate with OCR in an investigation may result in civil and/or criminal penalties.

**Supporting Tools**

Additional information may be found at [www.compliance.wisc.edu/hipaa](http://www.compliance.wisc.edu/hipaa)

**Definitions**

1. **Backup**: The process of making an electronic copy of data stored in a computer system. Examples of backups include:

   1.1 Full/Complete Backup - a backup/image of all (selected) data, programs, files on the system;
1.2 Incremental Backup - a backup that only contains the files that have changed since the most recent backup (either full or incremental);

1.3 Snap-shot back-up (image backup) - a process to restore/recover the system at a particular state, at a particular point in time;

1.4 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.

2. **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.

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

4. **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.

**Responsibilities**

HIPAA Privacy Officer
HIPAA Security Officer

**Link to Current Policy**

[TBD]

**Link to Related Policies**

https://compliance.wisc.edu/policies-and-forms/

**Link to Policy History**

N/A

**Review / Approval**

- HIPAA Executive Board, March 26, 2020