Policy Summary

UW-Madison strives to ensure the privacy and security of all patient/clients’ protected health information in the maintenance, retention, and eventual destruction/disposal of such information. Destruction/disposal of this information in whatever format shall be carried out as described in this document, but always in a manner that leaves no possibility for reconstruction of information.

This policy and procedure describes how records shall be disposed of/destroyed. When records may be disposed of/destroyed is outlined in applicable records’ retention schedules of the UW Health Care Component.

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. All destruction/disposal of PHI will be done in accordance with applicable federal and state law and any applicable records’ retention schedule of the UW HCC unit. Records that have satisfied the period of retention may be destroyed/disposed of by an appropriate method as described in III.G. below.
2. Records involved in any open investigation, public records request, audit or litigation must not be destroyed/disposed of. If the UW HCC unit receives notification that any of the above situations have occurred or there is the potential for such, the record retention schedule shall be suspended for these records until such time as the situation has been resolved.

3. Records containing PHI that are not originals and that have no retention of record requirements (i.e. provider copies, shadow charts, etc.) will be destroyed/disposed by shredding or other comparable method determined by each UW HCC unit. Certification of destruction of non-origina is not required.

4. Records containing PHI scheduled for destruction/disposal will be secured against unauthorized or inappropriate access until the destruction/disposal of PHI is complete.

5. A record of all destruction/disposal of original medical/client records or other original documents containing PHI will be made and retained permanently. Permanent retention is required because the records of destruction/disposal may be needed to demonstrate that the records containing PHI were destroyed/disposed of in the regular course of business. Records of destruction/disposal should include:

   5.1 Date of destruction/disposal.
   5.2 Method of destruction/disposal.
   5.3 Description of the destroyed/disposed record series or medium.
   5.4 Inclusive dates covered.
   5.5 A statement that the records containing PHI were destroyed/disposed of in the normal course of business.
   5.6 The signatures of the individuals supervising and witnessing the destruction/disposal (when appropriate).

A sample certificate of destruction is available at the hipaa.wisc.edu webpage in the “Forms” tab.

6. If destruction/disposal services are contracted, the contract shall:

   6.1 Specify the method of destruction/disposal (such method must be consistent with those set forth in III.G. below).
   6.2 Specify the time that will elapse between acquisition and destruction/disposal of data/media.
   6.3 Establish safeguards against breaches in confidentiality.
   6.4 Provide proof of destruction/disposal.

See Privacy Policy # 6.1 “Managing Arrangements with Business Associates of the University of Wisconsin-Madison” for more details concerning the requirements of a business associate agreement.

7. PHI will be destroyed/disposed of using a method that ensures the PHI cannot be recovered or reconstructed. Appropriate methods for destruction/disposal are outlined in the following table.
<table>
<thead>
<tr>
<th>Medium</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Audiotapes</td>
<td>Methods for destroying/disposing audiotapes include recycling (tape over) or pulverizing</td>
</tr>
<tr>
<td>Computerized Data/ Computers &amp; Hard Disk Drives (including within some fax machines and copiers)</td>
<td>Methods of destruction/disposal should destroy/dispose of data permanently and irreversibly. Methods may include overwriting data with a series of characters or reformatting the disk (destroying everything on it). Deleting a file on a disk does not destroy/dispose of the data, but merely deletes the filename from the directory, preventing easy access and making the sector available on the disk so it may not be overwritten. Total data destruction/disposal does not occur until the back-up tapes have been overwritten.</td>
</tr>
<tr>
<td>Computer Data/ Magnetic Media</td>
<td>Methods may include overwriting data with a series of characters or reformatting the tape (destroying everything on it). Total data destruction does not occur until the back-up tapes have been overwritten. Magnetic degaussing will leave the sectors in random patterns with no preference to orientation, rendering previous data unrecoverable.</td>
</tr>
<tr>
<td>Computer Diskettes</td>
<td>Methods for destroying/disposing of diskettes include reformatting, pulverizing, or magnetic degaussing.</td>
</tr>
<tr>
<td>Laser Disks</td>
<td>Disks used in &quot;write once-read many&quot; (WORM) document imaging cannot be altered or reused, making pulverization an appropriate means of destruction/disposal.</td>
</tr>
<tr>
<td>Microfilm/ Microfiche</td>
<td>Methods for destroying/disposing of microfilm or microfiche include recycling and pulverizing.</td>
</tr>
<tr>
<td>Paper Records</td>
<td>Paper records should be destroyed/disposed of in a manner that leaves no possibility for reconstruction of information. Appropriate methods for destroying/disposing of paper records include: burning, shredding, pulping, and pulverizing.</td>
</tr>
<tr>
<td>Videotapes</td>
<td>Methods for destroying/disposing of videotapes include recycling (tape over) or pulverizing.</td>
</tr>
</tbody>
</table>

8. **Additional Information on Disposal of Discarded Paper Containing PHI.** On occasion, when copying or faxing documents containing PHI, additional copies are made which are not subject to a retention schedule (because they are copies, not originals) and which may be disposed of immediately after the purpose for which they were made has been fulfilled. Such paper copies may be disposed of in recycle bins or waste receptacles only as described below:

8.1 Unsecured recycle bins/waste receptacles should be located in areas where the public will not be able to access them.

8.2 When possible, dispose of paper waste containing PHI in receptacles that are secured by locking mechanisms or that are located behind locked doors after regular business hours. Locked containers must be used with copy machines located in insecure or unattended areas.
8.3 Paper documents containing PHI may be placed in recycle bins/waste receptacles as described above only if the paper in such bins or receptacles will be disposed of in a manner that leaves no possibility for reconstruction of the information as described in the chart in III.G. above.

9. The methods of destruction/disposal will be reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction/disposal services.

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

Definitions

1. **Protected Health Information** (“PHI”): Health information, or healthcare payment information, including demographic information, 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.

2. **UW-Madison Health Care Component** (“UW HCC”): Those units of the University of Wisconsin-Madison that have been designated by the University as part of its health care component under HIPAA. See HIPAA Policy 1.1 “Designation of UW-Madison Health Care Component” for a listing of these units.

Responsibilities

HIPAA Privacy Officer
HIPAA Security Officer

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