Deidentification

Effective Date: April 3, 2003
Last Updated: March 26, 2020
Previously Updated: July 13, 2014
Last Reviewed: Next Review:

<table>
<thead>
<tr>
<th>Functional Owner</th>
<th>UW-Madison HIPAA Privacy Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executive Sponsor</td>
<td>UW-Madison Chancellor</td>
</tr>
<tr>
<td>Policy Contact</td>
<td>UW-Madison HIPAA Privacy Officer</td>
</tr>
</tbody>
</table>

Policy Summary

Health information that is de-identified, i.e., does not identify a patient and with respect to which there is no reasonable basis to believe that the information can be used to identify a patient, does not constitute protected health information and therefore is not subject to the requirements for the use and disclosure of protected health information in the Privacy Rule. This document describes how protected health information may be de-identified under the Privacy Rule of HIPAA.

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. Use or Disclosure of PHI for Creating a De-identified Data Set
   
   1.1 A UW HCC unit may use PHI to create de-identified information, whether or not the de-identified information is to be used by the UW HCC unit or disclosed to another entity or individual, without patient authorization.
   
   1.2 A UW HCC unit may disclose PHI to a business associate in order to create de-identified information, whether or not the de-identified information is to be used by the UW HCC unit or...
disclosed to another entity or individual, without patient authorization. Additional requirements apply before disclosing PHI to a business associate. (See Privacy Policy # 6.1 “Managing Arrangements of Business Associates with the University of Wisconsin-Madison”).

2. Procedures for De-identification of PHI

A UW HCC unit may determine that health information is de-identified only if the requirements set forth in sections 1 or 2 below are met.

2.1 The following identifiers of the patient or of relatives, employers, or household members of the patient, are removed:

2.1.1 Name

2.1.2 Geographic subdivisions smaller than a state (i.e., county, town or city, street address, and zip code) (note: in some cases, the initial three digits of a zip code may be used)

2.1.3 All elements of dates (except year) for dates directly related to an individual (including birth date, admission date, discharge date, date of death, all ages over 89 and dates indicative of age over 89) (note: ages and elements may be aggregated into a single category of age 90 or older)

2.1.4 Phone numbers

2.1.5 Fax numbers

2.1.6 E-mail addresses

2.1.7 Social security number

2.1.8 Medical record number

2.1.9 Health plan beneficiary number

2.1.10 Account numbers

2.1.11 Certificate/license numbers

2.1.12 Vehicle identifiers and serial numbers

2.1.13 Device identifiers and serial numbers

2.1.14 URLs

2.1.15 Internet protocol (IP) address numbers

2.1.16 Biometric identifiers (e.g., fingerprints)

2.1.17 Full face photographic and any comparable images

2.1.18 Any other unique identifying number, characteristic, or code
2.1.19 Any other information about which the UW HCC unit has actual knowledge that it could be used alone or in combination with other information to identify the individual

2.2 A person with appropriate expertise in statistics and other relevant scientific principles and methods does both of the following:

2.2.1 Determines that the risk is very small that the information could be used, alone or in combination with other reasonably available information, by an anticipated recipient to identify a patient who is the subject of the information.

2.2.2 Documents the methods and results of the analysis that justify such determination.

3. Re-Identification

3.1 The UW HCC unit may assign a code or other means of record identification to allow information de-identified to be re-identified by that UW HCC unit provided that both of the following are true:

3.1.1 The code or other means of record identification is not derived from or related to information about the patient and is not otherwise capable of being translated so as to identify the patient.

3.1.2 The UW HCC unit does not use or disclose the code or other means of record identification for any other purpose (other than re-identification) and does not disclose the mechanism for re-identification.

3.2 Disclosure of a code or other means of record identification, designed to enable coded or otherwise de-identified information to be re-identified, constitutes disclosure of PHI.

3.3 If de-identified information is re-identified, such re-identified information is PHI and the UW HCC unit may use or disclose such re-identified information only as permitted for PHI under the Privacy Rule.

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. **Business Associate**: A person or entity not affiliated with UW-Madison that performs or assists in performing, for or on behalf of any unit in the UW-Madison Health Care Component, business support functions/services that involve the use of Protected Health Information.

2. **Protected Health Information** ("PHI"): Health information or health care payment information, including demographic information, which identifies the patient or can be used to identify the patient. PHI does not include student records held by educational institutions or employment records held by employers.

3. **University of Wisconsin-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 Current Policy

[TBD]

Link to Related Policies

[https://compliance.wisc.edu/policies-and-forms/](https://compliance.wisc.edu/policies-and-forms/)

Link to Policy History

N/A

Review / Approval

- HIPAA Executive Board, March 26, 2020