Limited Data Sets of Protected Health Information and Data Use Agreements
Under the HIPAA Privacy Rule

Effective Date: April 14, 2003
Last Updated: November 9, 2020
Previously Updated: March 26, 2020, September 22, 2014

Policy Summary

A limited data set (commonly referred to as a "LDS") is Protected Health Information ("PHI") that excludes certain direct identifiers and can be used or disclosed without an individual’s authorization when other compliance steps are taken. The UW HCC units may use or disclose a limited data set of PHI only for the purposes of public health activities, research, or health care operations. Such use or disclosure requires a data use agreement between the entities sharing and receiving the limited data set. This document describes how a limited data set of PHI may be created, and how it may further be used or disclosed 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 to Create a Limited Data Set of Protected Health Information

1.1 A UW HCC unit may use or disclose a LDS of PHI – without authorization from the individuals whose limited identifiers comprise the LDS – only for the purposes of research, public health activities, or health care operations.

1.2 A UW HCC unit may use PHI to create a LDS of PHI, whether or not it is to be used by the UW HCC unit or disclosed to another entity or individual.

1.3 A UW HCC unit may disclose PHI to a business associate in order to create a LDS of PHI, whether or not it is to be used by the UW HCC unit or disclosed to another entity or individual. 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 Creating a Limited Data Set

2.1 The following limited identifiers may be included in a LDS of PHI:

2.1.1 Dates (such as admission date, discharge date, service date, date of birth, date of death)
2.1.2 Ages (in years, months, days or hours)
2.1.3 Town/City, state, 5-digit zip code (but not street name or number, or 9-digit zip code)*
2.1.4 Other numbers, characteristics, or codes not listed as direct identifiers under HIPAA

*Whether a data set which includes other geocoding or other identifiers not listed above may qualify as a LDS of PHI will depend upon the circumstances. 9-digit zip codes and geocoding information which allow specificity of location to a “street” level may not be included in a LDS of PHI (see Federal Register, Vol. 67, No. 157, at 53235).

2.2 The following direct identifiers of an individual or the individual’s relatives, employers, or household members must be removed in order for a data set to meet HIPAA’s definition of a LDS of PHI:

2.2.1 Name
2.2.2 Address or location information more specific than 5-digit zip code
2.2.3 Phone numbers
2.2.4 Fax numbers
2.2.5 E-mail addresses
2.2.6 Social security number
2.2.7 Medical record number
2.2.8 Health plan beneficiary number
2.2.9 Account numbers
2.2.10 Certificate/license numbers
2.2.11 Vehicle identifiers and serial numbers
2.2.12 Device identifiers and serial numbers
2.2.13 URLs
2.2.14 Internet protocol (IP) address numbers
2.2.15 Biometric identifiers (e.g., fingerprints)
2.2.16 Full face photographic and any comparable images
3. **Data Use Agreements**

3.1 The UW HCC unit may use or disclose a LDS of PHI only if it obtains satisfactory assurance, in the form of a data use agreement, that the data recipient will only use or disclose the LDS of PHI for specified purposes.

Similarly, a UW HCC unit may receive a LDS of PHI from another Covered Entity if it provides satisfactory assurance to the Covered Entity, in the form of a data use agreement, that the Covered Entity’s LDS of PHI will only be used or disclosed for specified purposes.

3.2 In order to comply with the requirements of HIPAA, the data use agreement must:

3.2.1 Establish the permitted uses and disclosures of the LDS of PHI by the recipient, which may be for research, public health activities or health care operations only.

3.2.2 Establish who is permitted to use or receive the LDS of PHI.

3.2.3 Provide that the recipient of the LDS of PHI will:

3.2.3.1 Not use or further disclose the information other than as permitted by the data use agreement or as otherwise required by law;

3.2.3.2 Use appropriate safeguards to prevent use or disclosure of the information other than as provided for by the data use agreement;

3.2.3.3 Report to the UW HCC unit any use or disclosure of the information not provided for by its data use agreement of which it becomes aware;

3.2.3.4 Ensure that any agents, including a subcontractor, to whom it provides the LDS of PHI, agree to the same restrictions and conditions that apply to the recipient with respect to such information; and

3.2.3.5 Not identify the information or contact the individuals.

3.3 **Data Use Agreement Templates**

3.3.1 UW HCC units are encouraged to utilize approved templates to create data use agreements. Templates are available through a number of offices at UW-Madison, including the Office of Compliance and the Office of Research and Sponsored Programs (“RSP”).

3.3.2 When a UW HCC unit receives a LDS of PHI from another institution, that other institution may prefer to use their institutional template to create a data use agreement; using other institutions’ templates is acceptable so long as the resulting data use agreements meet the requirements of HIPAA stated above in Section 3.2 of this policy.

3.4 **Signature Authority for Data Use Agreements at UW-Madison**

3.4.1 Data Use Agreements must be executed by an individual with authority sign contracts on behalf of UW-Madison. Generally, researchers do not have authority to sign contracts on behalf of UW-Madison; researchers should contact their department
administrator or other department leadership with any questions regarding execution of a Data Use Agreement.

4. Compliance

A UW HCC unit is not in compliance with this policy or with HIPAA regulations if the UW HCC unit knows of a pattern of activity or practice of the recipient of a LDS of PHI that constitutes a material breach or violation of the data use agreement, unless the UW HCC unit took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful:

4.1 Discontinues disclosure of the PHI to the recipient; and

4.2 Reports the problem to the UW-Madison HIPAA Privacy Officer, who shall report the problem to the Secretary of the Department of Health and Human 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

UW-Madison Office of Compliance data use agreement templates may be found at: https://compliance.wisc.edu/policies-and-forms/.

RSP Data Use Agreement templates may be found at: https://www.rsp.wisc.edu/contracts/dtua.cfm.

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. Data Use Agreement: An agreement between the entity that shares or discloses protected health information and recipient of the protected health information by which recipient agree only to use or disclose the protected health information for limited purposes as further described below.

3. Health Care Operations: Any of a number of business and administrative activities, including

   3.1 Conducting quality assessment and improvement activities
   3.2 Reviewing the competence or qualifications of health care professionals
   3.3 Conducting training programs
   3.4 Accreditation
   3.5 Credentialing
   3.6 Conducting or arranging for medical review, legal services and auditing functions
3.7 Business planning and development, and
3.8 Business management and general administrative activities

Health care operations do not include research and many fundraising and marketing activities. See Privacy Policies # 3.5 “Uses and Disclosures of Protected Health Information for Marketing” and # 3.6 “Uses and Disclosures of Protected Health Information for Fundraising” for more information.

4. **Protected Health Information** ("PHI"): Is 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.

5. **Public Health Activities**: The activities of public health authorities who are legally authorized to receive protected health information for the purpose of preventing or controlling disease, injury, or disability. This would include, for example, the reporting of a disease or injury; reporting vital events, such as births or deaths; and conducting public health surveillance, investigations, or interventions.

6. **Public Health Authority**: An agency or authority of the United States government, a State, a territory, a political subdivision of a State or territory, or Indian tribe that is responsible for public health matters as part of its official mandate, as well as a person or entity acting under a grant of authority from, or under a contract with, a public health agency.

7. **Research**: A systematic investigation, include research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

8. **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.

**Responsible Parties**

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, November 9, 2020
- HIPAA Privacy and Security Operations Committee, August 13, 2020