Use and Disclosure of De-Identified Data and Limited Data Sets
HIPAA-P06

About This Policy

Effective Dates:
07-01-2014

Last Updated:
08-01-2016

Responsible University Administrator:
Vice President for University Clinical Affairs

Policy Contact:
University HIPAA Privacy Officer

Scope

This policy applies to all personnel, regardless of affiliation, who have access to Protected Health Information ("PHI") under the auspices of Indiana University, designated for purposes of complying with the final provisions of the security and privacy rules regulated by the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act. Please refer to the HIPAA Affected Areas document for a full list of units impacted within Indiana University.

This policy addresses the uses and disclosures of PHI, including determination of required authorization and verification, for research, health plans, health services, business associates and affiliates.

Policy Statement

Indiana University respects the privacy of all members of the IU community, and strives to implement measures to protect privacy consistent with the university mission and environment, applicable legal requirements and professional standards, generally accepted privacy norms, and available resources.

While HIPAA imposes many restrictions on the use and disclosure of protected health information, HIPAA does not regulate the use or disclosure of de-identified information and imposes lesser restrictions on the use and disclosure of Limited Data Sets. It is therefore the policy of Indiana University to use and/or disclose de-identified information or Limited Data Sets where appropriate, in accordance with the policy set forth below. De-identified information and/or limited data sets may still be subject to other confidentiality requirements (e.g., because the information is proprietary) and should be marked confidential when appropriate.

DE-IDENTIFIED INFORMATION POLICY

Health Information is not subject to the HIPAA Privacy Rule if it is de-Identified in accordance with the HIPAA Privacy Rule. No authorization from an Individual is required to use or disclose Health Information that is de-Identified. Health Information is considered de-Identified if: (a) it does not identify an Individual; and (b) there is no reasonable basis to believe it can be used to identify an Individual.

The Department of Health and Human Services published a guidance document in January, 2013, Guidance Regarding Methods for De-Identification of Protected Health Information in Accordance with the Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule. A link to the guidance document is provided under RELATED INFORMATION.

Methods for De-Identification
A covered entity covered entity may determinethathealth information is not individually identifiable health information only if one of two methods is used to de-identify Health Information; expert determination or the Safe Harbor of removing identifiers.

1. **Method 1- Expert Determination:** A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable.

   a. Applying such principles and methods, 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 an individual who is a subject of the information; and

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

2. **Method 2 – Removing Identifiers:** Removal of all of the following identifiers as they pertain to the Individual or to his/her relatives, employers or household members (collectively referred to below as “Individuals”):

   a. Names

   b. All geographic subdivisions smaller than a State, including:

      1. Street address of P.O. Box Number
      2. City
      3. County
      4. Precinct
      5. Town

      6. Zip codes and their equivalent geocodes, except for the initial three digits of a zip code if, according to current publicly-available date from the Bureau of the Census:

         a. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and

         b. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000

   c. All elements of dates (except year) for dates related to an individual including: dates of birth and death, and admission and discharge dates and all ages over 89, in which case the Individuals’ ages must be categorized as 90 or older.

   d. Telephone numbers

   e. Fax numbers

   f. E-mail addresses

   g. Social Security numbers

   h. Medical record numbers

   i. Health plan beneficiary numbers

   j. Account numbers

   k. Certificate/license numbers

   l. Vehicle identifiers and serial numbers, including license plate number

   m. Device identifiers and serial numbers

   n. Web Universal Resource Locators (URLs)

   o. Internet Protocol (IP) address numbers

   p. Biometric identifiers (including finger and voice prints).

   q. Full-face photographic images.

   r. Any other unique identifying number, characteristic or code
Exception: Any code used by the Indiana University to re-identify the information; provided, however, that any such code must not be related in any way to the identifiers that must be removed in order for the information to be de-identified and only the Indiana University can have access to the code and/or use the code for re-identification.

AND

After removing the identifiers, no one has actual knowledge that the remaining information could be used alone, or in combination with other information available to the recipient, to identify an Individual.

Elements that do not need to be removed

The following data elements do not need to be removed from health information in order for the data to be considered de-identified:

1. Age (except over 89, as specified above)
2. Gender
3. Race
4. Ethnicity
5. Marital status
6. State of residence
7. Parts of Zip Code numbers in certain circumstances (as explained above)

LIMITED DATA SET POLICY

A covered entity can use and disclose information in the form of a limited data set without the individual’s authorization for purposes of research, public health or healthcare operations if the data are released in conjunction with a Data Use Agreement.

Limited Data Set

A limited set is information from which “facial” identifiers have been removed. Specifically, as it relates to the individual or his or her relative, employers or household members, all of the following identifiers must be removed in order for health information to be a “limited data set”:

1. Names.
2. Street addresses or RR numbers (other than town, city, state and zip code)
3. Telephone numbers
4. Fax numbers
5. E-mail addresses
6. Social Security numbers
7. Medical record numbers
8. Health plan beneficiary numbers
9. Account numbers
10. Certificate/license numbers
11. Vehicle identifiers and serial numbers, including license plate number
12. Device identifiers and serial numbers
13. Web Universal Resource Locators (URLs)
14. Internet Protocol (IP) address numbers
15. Biometric identifiers (including finger and voice prints).
16. Full-face photographic images.
Health information that may remain in the information disclosed

1. Dates such as date of birth, date of death, admission, discharge, service;
2. City, state, five digit zip code;
3. Ages in years, months or days or hours; and
4. Unique identifying numbers, characteristics or codes provided the unique identifiers cannot reasonable be used to identify an individual

Data Use Agreement

The Data Use Agreement must contain the following elements:

1. A description of the permitted uses and disclosures of the Limited Data Set, which must be limited to and consistent with public health, research or health care operations purposes;
2. A description of those persons who are permitted to use or receive the Limited Data Set;
3. A statement requiring that the Limited Data Set recipient will:
   a. Not use or further disclose the information other than as permitted in the Data Use Agreement or as required by law;
   b. Use appropriate safeguards to prevent the use or disclosure of the information other than as permitted in the Data Use Agreement;
   c. Report to the Indiana University any use or disclosure of the information that is not permitted by the Data Use Agreement of which it becomes aware;
   d. Ensure that any of its agents or subcontractors to whom it provides the Limited Data Set agrees to the same restrictions and conditions that apply to the Limited Data Set recipient; and
   e. Not identify the information or contact the Individuals who are the subject of the information.

AUTHORIZED INDIVIDUAL TO DE-IDENTIFY DATA OR CREATE LIMITED DATA SETS

Only Indiana University Workforce and third-party Business Associates with whom Indiana University has contracted may de-identify health information or use the Health Information to create Limited Data Sets. If a third-party Business Associate is used for this purpose, then there must be a Business Associate Agreement in place with such third-party.

NON-COMPLIANT LIMITED DATA SET RECIPIENTS

If at any time Indiana University becomes aware that a recipient of a Limited Data Set has violated his/her/its Data Use Agreement, then Indiana University must:

A. Take reasonable steps to end the breach of the agreement or cause the breach to be cured; or
B. If the breach cannot be ended or cured, then stop disclosing the Limited Data Set or other PHI to the recipient and report the problem to the Secretary of Health and Human Services.

Reason For Policy

This policy has two purposes, which are as follows:

1. To specify the requirements for de-identifying Protected Health Information (PHI) in accordance with the HIPAA regulations so that the information will no longer be considered PHI and no longer subject to HIPAA.
2. To specify the requirements for removing certain identifying information from PHI in order to create a Limited Data Set that may be disclosed for research, public health, or health care operations purposes once the recipient of the PHI enters into a Data Use Agreement. Data in the form of a Limited Data Set is still considered PHI and protected under HIPAA.
Definitions

See Glossary of HIPAA Related Terms for a complete list of terms.

Sanctions

See HIPAA-G01 HIPAA Sanctions Guidance.

History

07/01/2014  Effective Date

Related Information

HIPAA-A02 General Administrative Requirements
HIPAA-G04 Limited Data Set and Data Use Agreement Guidance
HIPAA-P01 Uses & Disclosures of Protected Health Information Policy
HIPAA-P02 Minimum Necessary
HIPAA-P03 HIPAA Authorizations
HHS De-Identification Guidance
HIPAA Privacy and Security Compliance

Related Forms

Appendix 1 – De-Identification Checklist
Appendix 2 – Limited Data Set Checklist