

The University of Iowa
HIPAA Privacy Rule
Policies and Procedures

DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION (PHI)

Purposes: To define the guidelines and procedures necessary for the de-identification of Protected Health Information (PHI) contained in university records, to provide direction to staff regarding the use of de-identified PHI.

Policy: Protected Health Information is confidential, except when disclosure is authorized or compelled and the university has a duty to protect the privacy of records.

PHI can be de-identified by removing identifying characteristics. De-identified health information is no longer considered to be individually identifiable health information and the requirements of the Privacy Rule do not apply.

Procedure:

For PHI to be de-identified, one of the following must occur:

- 1) **Statistical De-identification:** A person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable determines the PHI is de-identified. This person must determine 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. This person must document the methods and results of the analysis that justify such determination. This process must be approved by the UI Privacy Officer.
- 2) **Alternative Method of De-identification Prescribed by Privacy Rule:**
 - a) De-identification requires the elimination not only of primary or obvious identifiers, such as name, address, date of birth, but also of secondary identifiers through which a user could deduce the individual's identity. For PHI to be de-identified the following identifiers of the individual or of relatives, employers, or household member of the individual, must be removed:
 - 1) Names
 - 2) Address information smaller than a state, including street address, city, county, zip code (except if by combining all zip codes with the same initial three digits, there are more than 20,000 people)
 - 3) Names of relatives and employers
 - 4) All elements of dates (except year), including date of birth, date of medical or health care, date of death; all ages over

89 and all elements of dates including year indicative of such age except that such age elements may be aggregated into a single category of age 90 or older

- 5) Telephone numbers
 - 6) Fax numbers
 - 7) Email addresses
 - 8) Social Security Number
 - 9) Medical or other record number
 - 10) Health beneficiary plan number
 - 11) Account numbers
 - 12) Certificate/License Number
 - 13) Vehicle identifiers, including license plate numbers
 - 14) Device ID and serial number
 - 15) Uniform Resource Locator (URL)
 - 16) Identifier Protocol (IP) addresses
 - 17) Biometric identifiers, including finger and voice print
 - 18) Full face photographic images and other comparable images
 - 19) Any other unique identifying number characteristic, or code;
- b) In addition, the university does not have actual knowledge that the information could be used alone or in combination with other information to identify an individual who is a subject of the information.

***Definitions:**

Protected Health Information (PHI):

Individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic. Individually identifiable health information relates to an individual's health status or condition, furnishing health services to an individual or paying or administering health care benefits to an individual. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual.

Reference: 45 C.F.R. §164.514