PATIENT PRIVACY: DE-IDENTIFICATION OF PROTECTED HEALTH INFORMATION (PHI) POLICY

PURPOSE

The purpose of this policy is to instruct Workforce Members how to properly De-Identify Protected Health Information (PHI) under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

POLICY STATEMENT

Safeguarding PHI is among the highest priorities of The University of Texas MD Anderson Cancer Center (MD Anderson). It is the policy of MD Anderson to De-Identify health information in accordance with 45 C.F.R. § 164.514 and this policy. This policy sets out how to properly De-Identify health information; it does not state when Workforce Members should De-Identify health information, as this is a fact-specific determination.

Information that has been De-Identified in accordance with this Policy may be Used or Disclosed without first obtaining an individual’s HIPAA Authorization. See Patient Privacy: Authorization for Use and Disclosure of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0396).

SCOPE

Compliance with this policy is the responsibility of all faculty, trainees/students, and other members of MD Anderson’s workforce.

TARGET AUDIENCE

The target audience for this policy includes, but is not limited to, all MD Anderson Workforce Members who use or disclose health information.

DEFINITIONS

Authorization: A written document signed by an individual granting someone else the ability to use or disclose the individual’s PHI. It is also referred to as a “HIPAA Authorization” or “Authorization for the Use and Disclosure of PHI.” To be valid, an Authorization must meet the requirements specified by 45 C.F.R. § 164.508 and MD Anderson’s Patient Privacy: Authorization for Use and Disclosure of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0396).

Breach: See HIPAA Definitions Plan.
**De-Identification**: Removal of identifying information in accordance with [45 C.F.R. § 164.514(b)](https://www.hhs.gov/). Information which does not identify an individual and which there is no reasonable basis to believe that the information can be used to identify an individual is De-Identified.

**Disclosure**: See [HIPAA Definitions Plan](https://www.hhs.gov/).

**Health Care Operations**: See [HIPAA Definitions Plan](https://www.hhs.gov/).

**Individually Identifiable Health Information**: See [HIPAA Definitions Plan](https://www.hhs.gov/).

**Payment**: See [HIPAA Definitions Plan](https://www.hhs.gov/).

**Protected Health Information (PHI)**: See [HIPAA Definitions Plan](https://www.hhs.gov/).

**Research**: See [HIPAA Definitions Plan](https://www.hhs.gov/).

**Treatment**: See [HIPAA Definitions Plan](https://www.hhs.gov/).

**Use**: See [HIPAA Definitions Plan](https://www.hhs.gov/).

**Workforce Member**: See [HIPAA Definitions Plan](https://www.hhs.gov/).

---

**PROCEDURE**

1.0 Procedure for De-Identifying PHI

PHI may be De-Identified in one of two ways: (1) the Safe Harbor method, or (2) the Expert Determination method.

1.1 Safe Harbor method:

To De-Identify PHI using the Safe Harbor method, eighteen (18) specific identifiers of the individual or the individual’s relatives, employers, or household members must be removed from the health information. These identifiers are:

A. Names (including initials or partial names).

B. All geographic subdivisions smaller than a state (including street address, city, county, precinct, Zip Code, and their equivalent geocodes), except for the first three digits of a Zip Code.

  *Note*: For the following 17 partial Zip Codes, even the first three digits are considered an “identifier” and must be instead changed to “000” in order for it to meet the De-Identification standard: 036, 059, 063, 102, 203, 556, 692, 790, 821, 823, 830, 831, 878, 879, 884, 890, and 893.

C. All elements of dates, except year, directly related to an individual (for example, birth date, admission date, discharge date, treatment dates, date of death).

  *Note*:
  - Ages 89 and less may be used, but ages 90 and greater must be changed to “90 or older.”
It is permissible to convert dates to time periods using years (for example, “years between diagnosis and death: 3”).

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 numbers.
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 or other identifying images (for more information in identifying images, see section 3.0).
R. Any other unique identifying number, characteristic or code (for example, study ID numbers), except as permitted under section 4.0 below.

1.2 Expert Determination method:

To De-Identify PHI using the Expert Determination method, a person with appropriate knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable must:

A. Applying generally accepted statistical and scientific principles, 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; and

B. Document the methods and results of the analysis that justify such determination.

1.3 Written approval must be obtained from the MD Anderson Institutional Compliance Office prior to using the Expert Determination method outlined in Section 1.2 above.

1.4 For questions regarding the Safe Harbor method or the Expert Determination method, please contact the Institutional Compliance Office at 713-745-6636 for assistance.

1.5 For help determining when De-Identification should occur, contact the Institutional Compliance Office (ICO) at 713-745-6636.
2.0 PHI and De-Identification Generally

2.1 PHI is created by pairing two elements: identifying information and health information. Health information is defined as any information, including genetic information that:

A. Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse, and

B. Relates to the past, present or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present or future payment for provision of health care to an individual.

2.2 Examples of health information include: diagnosis, prognosis, physical or mental health history, family history, medications, and genomic sequence. Because of the unique nature of the services we provide, the mere inference that an individual is receiving treatment and MD Anderson, without further specifics, may be considered health information.

2.3 When all identifying information defined above in section 1.0 is removed from health information, the information is De-Identified and no longer constitutes PHI under HIPAA. Because it is no longer PHI, the Use or Disclosure of De-Identified health information is not restricted by HIPAA, and the HIPAA Authorization requirement no longer applies. Additionally, because De-Identified health information is not PHI, unauthorized Disclosure of De-Identified health information cannot result in a “Breach.”

2.4 Because De-Identification protects individuals’ identities, whenever it is possible and appropriate to do so, information should be De-Identified. Situations in which it may be appropriate to De-Identify information include, but are not limited to:

A. For Research purposes (as defined under HIPAA), unless the Authorization portion of the informed consent permits PHI to be Used and Disclosed;

B. When sharing information with people outside of MD Anderson;

C. When storing information outside of MD Anderson (for example, in internet-based “cloud” storage);

D. When presenting at a meeting or conference, whether internal or external;

E. For case reports;

F. For use in articles and publications; and

G. For other situations in which you do not have the individual’s Authorization to Use or Disclose his/her PHI and no exception to the HIPAA Authorization rule applies. See Patient Privacy: Authorization for the Use and Disclosure of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0396).

2.5 Workforce Members should contact the Institutional Compliance Office at 713-745-6636 with questions about whether PHI should be De-Identified prior to a particular Use or Disclosure.

2.6 Although it is generally not necessary to De-Identify PHI when the PHI is being Used or Disclosed for Treatment, Payment, or Health Care Operations purposes (or other purposes specifically permitted by law), Workforce Members should always limit Uses and Disclosures of PHI to the minimum amount necessary to accomplish the intended purpose, unless the Use or Disclosure is for Treatment purposes.
2.7 If PHI has not been De-Identified, the general rules governing the Use and Disclosure of PHI, including the need to obtain a HIPAA Authorization, apply. See Patient Privacy: Uses and Disclosures of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0401) and Patient Privacy: Authorization for the Use and Disclosure of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0396).

Although it is not necessary to obtain an individual’s Authorization prior to disclosing De-Identified information to someone outside of MD Anderson, there may be situations in which it is appropriate to enter into a written agreement with the recipient of De-Identified information that is going to be used for Research or commercial purposes. Any questions as to whether a written agreement would be necessary or appropriate should be directed to Legal Services at 713-745-6633 prior to disclosing De-Identified PHI to outside researchers or entities.

3.0 De-Identifying Images

3.1 An image is De-Identified when it is not possible for someone who knows the person (including the individual who is the subject of the image) to identify the person in the image.

3.2 To De-Identify a photograph of an individual, you must ensure that the person’s face and all identifying markings (for example, tattoos, birth marks, scars, and fingerprints) are not recognizable. Blacking out the eyes is not enough. Even if the entire face has been blurred, if the individual’s body is unique enough that the individual or someone who knows the individual would be able to identify the photograph, the photograph should not be considered “De-Identified,” and the subject’s Authorization should be obtained prior to Use or Disclosure. Please refer to MD Anderson’s Policy Regarding Use of Institutional Images (UTMDACC Institutional Policy # ADM1050) for more information about Use of images.

3.3 To De-Identify diagnostic or similar images (for example, MRIs, CT scans, X-rays), remove all identifying writing from the image, including name, MRN, date and time that the image was taken, and any other numbers assigned to the image for identification purposes.

3.4 Electronic image files may not be De-Identified if the image file is easily restorable to its identifiable state. Common practices such as layering shapes over identifiable portions of the image are insufficient to De-identify the file. For assistance with De-Identifying electronic images, contact the Institutional Compliance Office at 713-745-6636.

4.0 Assigning Unique Codes for De-Identification Purposes

4.1 Health information remains De-Identified when a unique code which permits the information to be re-identified is assigned to the information if the following requirements are met:

A. The code is not derived from or related to information about the individual and is not otherwise capable of being translated so as to identify the individual; and

B. MD Anderson does not use or disclose the code for any other purpose and does not disclose the mechanism for re-identification.

4.2 The following are examples of situations where information would not be deemed De-Identified:

A. A code based on identifying information about the individual, such as the first three letters of the individual’s last name combined with the individual’s year of birth;

B. A code assigned to individuals based on the order in which they enrolled in a study, because the numbers were derived from information about the individual (the order of enrollment in the study) and someone who has information about the order in which individuals signed up for the study would potentially be able to re-identify the individuals;
C. A code assigned to tissue samples that is also used to identify the samples for Treatment purposes;

D. A code assigned to study participants in order to De-Identify the information in a spreadsheet, but the code is later included on a serious adverse event report to the study's sponsor that also contains the date on which the adverse event occurred. Because the code is now linked to the adverse event date (another HIPAA identifier) in the communication to the sponsor, the assigned code has become an identifier.

4.3 For questions about the assignment of unique numbers for De-Identification purposes, contact the Institutional Compliance Office at 713-745-6636.

5.0 Consequences of Failure to Properly De-Identify

5.1 PHI that has not been properly De-Identified is still PHI, and if it is Used or Disclosed without an individual’s Authorization or for a reason that does not fall under one of the exceptions to the HIPAA Authorization rule, the Institutional Compliance Office will need to determine whether a Breach has occurred, in accordance with MD Anderson’s Patient Privacy: Breach Notification Policy (UTMDACC Institutional Policy # ADM1033).

5.2 Workforce Members must immediately report the following situations to the Institutional Compliance Office at 713-745-6636:

A. Any Use or Disclosure of PHI that has not been properly De-Identified, for which no HIPAA Authorization has been obtained, and the Use or Disclosure was not related to Treatment, Payment, or Health Care Operations purposes;

B. Any Research Use or Disclosure of PHI that is inconsistent with the informed consent document or IRB waiver for a Research study (for example, if the informed consent document promises that information will be de-identified, but some PHI is shared with a study sponsor who is not named in the informed consent and authorization document);

C. Any other instance where information Used or Disclosed was thought to be De-Identified but may not have been properly De-Identified.

5.3 Failure to properly De-Identify information when it is required to be De-Identified (for example, if the protocol and informed consent document for a study require De-Identification) may constitute a HIPAA violation and/or violation of MD Anderson policy subject to disciplinary action pursuant to the Corrective Action Policy (UTMDACC Institutional Policy # ADM0256).

6.0 Partial De-Identification

6.1 If it is not possible to remove all 18 of the identifiers noted above at section 1.1., partial De-Identification is encouraged, because it is a useful means of minimizing the potential for harm to individuals if their PHI is Used or Disclosed to an unauthorized individual.

6.2 Only fully De-Identified information is definitely exempt from the definition of PHI. Partially De-Identified information is still PHI and must be protected under HIPAA. An unauthorized Disclosure of partially De-Identified information must undergo a Breach analysis by the Institutional Compliance Office.

7.0 Limited Data Sets

7.1 A Limited Data Set is PHI that has been partially De-Identified by removing 15 of the 18 identifying elements of an individual or of relatives, employers, or household members of the individual (as discussed above at section 1.1). A Limited Data Set is permitted to keep city/state/Zip Code, dates, and unique characteristics or codes.
7.2 Use or Disclosure of a Limited Data Set may be appropriate in situations where PHI cannot be completely De-Identified and the Use or Disclosure is only allowed for Research, Public Health, or Health Care Operations purposes. For more information on Use and Disclosure of an LDS, see the Limited Data Set and Data Use Agreement Policy (UTMDACC Institutional Policy # ADM0343).
ATTACHMENTS / LINKS

None.

RELATED POLICIES

Corrective Action Policy (UTMDACC Institutional Policy # ADM0256).

Limited Data Set and Data Use Agreement Policy (UTMDACC Institutional Policy # ADM0343).

Patient Privacy: Authorization for the Use and Disclosure of Protected Health Information Policy (MDACC Institutional Policy # ADM0396).

Patient Privacy: Uses and Disclosures of Protected Health Information Policy (UTMDACC Institutional Policy # ADM0401).

Policy Regarding Use of Institutional Images (UTMDACC Institutional Policy # ADM1050).

JOINT COMMISSION STANDARDS / NATIONAL PATIENT SAFETY GOALS

IM.02.01.01:

OTHER RELATED ACCREDITATION / REGULATORY STANDARDS


HIPAA Privacy Rule, 45 C.F.R. §§ 164.506, 164.512, 164.514.

REFERENCES

None.
POLICY APPROVAL

Approved With Revisions Date: 09/14/2017
Approved Without Revisions Date:
Implementation Date: 09/14/2017
Version: 14.0

RESPONSIBLE DEPARTMENT(S)

Institutional Compliance Office