Weill Cornell Medicine	**Policy Title**	De-Identification of PHI
	Policy Number	CPO-P-410.11
	Department	Compliance and Privacy
	Effective Date	March 21, 2024
	Last Reviewed	N/A
	Approved By	Information Security and Privacy Advisory Committee (ISPAC)
	Approval Date	March 21, 2024

Policy

Weill Cornell Medicine ("WCM") shall de-identify protected health information (PHI) in accordance with Health Insurance Portability and Accountability Act of 1996 (HIPAA) by use of the (i) Safe Harbor Method or (ii) Expert Determination. De-identified data is achieved by removing all individual identifiers from the record to ensure the individual's identity is anonymous. A record that is properly de-identified no longer qualifies as PHI under HIPAA and is classified as de-identified data. This allows WCM to share health for research purposes in accordance with HIPAA requlations while safeguarding patient privacy.

WCM has established an Honest Broker service to oversee the provide the de-identification of PHI. This service provides an Honest Broker, a neutral third-party designated to manage the process of collecting PHI, using the Safe Harbor method for de-identification, and prepare the de-identified data for various use, including research.

To maintian integrity, WCM prohibits its workforce members from self-certifying de-identified data. All requests for de-identification of PHI must be processed through the Honest Broker service to ensure compliance and proper de-identification procedures. De-identified data created through either the Safe Harbor or Expert Determination method falls outside the scope of this Policy as it no longer qualifies as PHI. However, such data may still be subject to other policies and regulations, including but not limited to WCM ITS Policy 11.03 – *Data Classification*.

Purpose

De-identified data plays a vital role for WCM and its Business Associates (BAs) in sharing and using information for research and other covered entity activities, as permitted by WCM, without requiring authorization. Failure to properly de-identify data sets may lead to unauthorized disclosure or use of PHI under HIPAA. To mitigate these risks, WCM has established a process for de-identifying data in compliance with HIPAA, as outlined in this policy.

Scope

This policy applies to all WCM workforce members, including its Business Associates, and any other individuals involved in handling PHI.

Definitions

Business Associate: a person or entity that performs certain functions or activities, or provides services that creates, receives, maintains, processes or transmits PHI on behalf of, or to WCM and is an external person or entity. *Examples of BA functions or activities include claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, and software hosting of PHI.*

De-Identified Data: Health information that does not identify an individual and with respect to which there is no reasonable basis to believe that the information can be used to identify an individual is not individually identifiable health information.

Electronic Protected Health Information: Protected Health Information that is transmitted or maintained in electronic media that is included in Weill Cornell Medicine's Designated Record Set, excluding (i) psychotherapy

notes, and (ii) information compiled in reasonable anticipation of, or for use in, a civil, criminal, or administrative action or proceeding. *Prior to October 6, 2022, EHI only includes electronic information represented by the data elements of the United States Core Data for Interoperability ("USCDI")*, which include, but are not limited to, patient demographics, allergies, immunizations, procedures, laboratory test results and values, medications, and clinical notes. A list of the USCDI data elements may be found at https://www.healthit.gov/isa/united-states-core-data-interoperability-uscdi.

Electronic Medical Record: An electronic record of health-related information on an individual that can be created, gathered, managed, and consulted by authorized clinicians and staff within a single organization.

Honest Broker: An honest broker is a neutral third-party with no affiliation to the requestor.

Protected Health Information (PHI) - Under HIPAA, PHI is "individually identifiable health information" held, created, or transmitted by a covered entity, or its business associate, in any form or media, whether electronic, paper, or verbal.

A. PHI is information, including demographic data, related to:
    a. The provision of health care to an individual; **or**
    b. An individual's past, present, or future:
        i. physical or mental health condition; or
        ii. payment for the provision of health care to an individual; **and**

B. The information identifies the individual or there is a reasonable basis to believe the information can be used to identify the individual by the presence of one or more (depending on the context) of the following 18 individual identifiers:

1. Names;
2. Geographic subdivisions smaller than a state, including street address, city, county, precinct, ZIP code, and their equivalent geocodes, except for the initial three digits of a ZIP code in certain situations;
3. All elements of date (except year) for dates directly related to an individual, including birth date, discharge date, date of death; and all ages over 89 and all elements of dates indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
4. Telephone numbers;
5. Fax numbers;
6. Electronic mail addresses;
7. Social Security numbers;
8. Medical record numbers;
9. Health plan beneficiary numbers;
10. Account numbers;
11. Certificate/license numbers;
12. Vehicle identifiers and serial numbers, including license plate numbers;
13. Medical device identifiers and serial numbers;
14. Web Universal Resource Locators (URLs);
15. Internet Protocol (IP) address numbers;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code unless otherwise permitted by this Policy for re-identification (§164.514(b)(2)).

Re-identification: The assignment of a unique code to the set of de-identified health information to permit the information identifiable again by the covered entity. Any other unique identifying number, characteristic or code, unless otherwise permitted by this Policy for re-identification (§164.514(b)(2)).

Workforce Member: any faculty, staff, students, volunteers, trainees, and other persons whose conduct, in the performance of work for WCM, is under the direction and control of WCM, whether they are paid by WCM.

Procedure

1. De-identification of PHI under HIPAA

De-identification of PHI involves the removal of personal identifiers from a record to create a dataset that cannot identify an individual, with no reasonable basis to re-identify the individual. Under HIPAA, there are two methods by which PHI can be de-identified: (i) the Safe Harbor Method and (ii) the Expert Determination Method.

(i) **Safe Harbor Method:** This method entails removing all 18 personal identifiers related to an individual, their relatives, employers or household members from the PHI. These identifiers include:

a. All geographic subdivisions smaller than a state, including street address, city, county, precinct, zip code and their equivalent geographical codes except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
   i. The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   ii. The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people are changed to 000.

b. All elements of dates (excluding year) directly related to an individual, including birth date, admission date, discharge date, and date of death. Additionally, ages over 89 and all elements of dates indicating such ages may be aggregated into a single category of age 90 or older.

(ii) **Expert Determination Method:** This method involves the engagement of an expert – a person with knowledge of and experience with generally accepted statistical and scientific principles and methods for rendering information not individually identifiable. The expert must:

a. Determine that there is a "very small" risk that the information, alone or combined with other reasonably available data, could be used by an anticipated recipient to identify an individual who is the subject of the information.
b. Document the methods and results of the analysis justifying the determination.

2. De-identification of PHI by Use of the Honest Broker Service

WCM has designated the WCM Information Technologies and Services (ITS) department oversee the Honest Broker service. This service ensures the removal of identifiers from PHI in accordance with the appropriate methods under HIPAA.

WCM Workforce members seeking to de-identify PHI and/or share the resulting de-identified dataset should submit a request for use of the Honest Broker service via email to arch-support@med.cornell.edu. The request will undergo a review to determine if additional supporting documentation, such as the IRB protocol and details about the recipient of the de-identified data, is required.

Upon completion of the request and necessary supporting documentation, the Honest Broker service will process the collected data to create a HIPAA-compliant de-Identified dataset. Each dataset will be assigned a unique code and will contain minimum amount of information necessary for successful sharing or use of the de-identified data for its intended purpose.

3. Re-Identification of a De-Identified Data Set

WCM may assign a code or other means of record identification to allow de-identified information to be re-identified by WCM, provided that:

(i) **Derivation.** The code or other means of record identification 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
(ii) **Security.** The covered entity does not use or disclose the code or other means of record identification for any other purpose, and does not disclose the mechanism for re-identification.

WCM's Honest Broker service facilitates the re-identification process by assigning a unique code to each set of data that will allow de-identified data to be re-identified by WCM. Workforce Members seeking to re-identify a de-identified data set may submit a request to WCM ITS by emailing arch-support@med.cornell.edu.

4. Restrictions on Use of PHI

HIPAA permits patients the right to request restrictions on certain uses and disclosures of their PHI, even for research purposes, regardless of whether it is de-identified. Requests for restrictions on the use of PHI are submitted in writing by patients and are managed by WCM's Privacy Office. To confirm patient preferences regarding information used for research, there must be a review of the patient electronic medical record.

5. Retention

De-identified data intended for research purposes must comply with the document retention requirements outlined in Cornell University Policy 4.21 - *Research Data Retention*. For all other purposes, de-identified data should be retained in accordance with Cornell University Policy 4.7 – *Retention of University Records*.

Compliance with this Policy

All members of the WCM workforce are responsible for adhering to this policy. Failure to comply will be evaluated on a case-by-case basis and could lead to corrective action, up to and including termination. Instances of non-compliance that potentially involve a lapse of professionalism, may lead to the engagement of the Office of Professionalism for evaluation and intervention.

Contact Information

You can direct any questions about this policy to the WCM Compliance and Privacy Office. If you know or suspect a privacy incident may have occurred, promptly notify your supervisor and/or the WCM Compliance and Privacy Office. You can also direct any questions about this policy to:

- Email: privacy@med.cornell.edu
- Phone Number: 646-962-6930

If you need to file an Anonymous Report, contact the Cornell Hotline at the following:

- Website: www.hotline.cornell.edu
- Phone Number: 866-293-3077

References

- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- Health Information Technology for Economic and Clinical Health Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5 (Feb. 17, 2009)
- Final HIPAA Omnibus Rule (78 Fed. Reg. 5566)
- Family Education Rights Privacy Act 20 U.S.C. §1232g
- NYS Stop Hacks and Improve Electronic Data Security ("SHIELDS") Act
- Security Privacy Incident Response Plan (SPIRP).
- WCM ITS Policy 11.05 - *Security and Privacy Incident Response Plan*
- Cornell University Policy 4.21 – *Research Data Retention*
- Cornell University Policy 4.7 - *Retention of University Records Policy*

Policy Approval

This policy was approved by the WCM Information Security and Privacy Advisory Committee (ISPAC).

Version History

Date	Author	Revisions
3/21/2024	WCM Compliance & Privacy Office	Original date of issue.