



POLICY TITLE: De-Identification of Protected Health Information	SYSTEM POLICY AND PROCEDURE MANUAL
POLICY #: 800.64	CATEGORY: Compliance and Ethics
System Approval Date: 5/22/2024	Effective Date: 10/19/2017
Site Implementation Date: 7/08/2024	Last Reviewed/Approved: 04/2023
Prepared by: Office of Corporate Compliance	Notations: N/A

GENERAL STATEMENT of PURPOSE

The purpose of this document is to establish general requirements to achieve de-identification in accordance with the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”) to protect the confidentiality of Protected Health Information (“PHI”) while allowing its necessary use, access and disclosure for purposes of providing high quality care to the patients of Northwell Health.

This policy will establish a standard to understand what de-identification is, and the general process by which de-identified health information is created.

POLICY STATEMENT

It is the policy of Northwell Health that when all characteristics that constitute PHI are completely removed from health information and the resulting information does not identify an individual, it is considered de-identified. Information that has been de-identified pursuant to this policy is no longer considered PHI and is not subject to the same requirements as PHI.

SCOPE

This policy applies to all Northwell Health employees, as well as medical staff, volunteers, students, trainees, physician office staff, contractors, trustees and other persons performing work for or at Northwell Health; faculty and students of the Donald and Barbara Zucker School of Medicine at Hofstra/Northwell or the Hofstra Northwell School of Nursing and Physician Assistant Studies conducting research on behalf of the Zucker School of Medicine on or at any Northwell Health facility.

DEFINITIONS

Authorization: An individual's signed permission that allows a covered entity to use or disclose the individual's PHI for the purpose(s), and to the recipient(s), as stated in the Authorization. See Authorization for Release of Health Information (VD001).

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 Northwell Health and is an external person or entity.

Examples of BA functions or activities can include, but are not limited to claims processing or administration, data analysis, utilization review, quality assurance, billing, benefit management, practice management, and software hosting of PHI. Examples of BA services include legal, actuarial, accounting, consulting, data aggregation, management, administrative, accreditation and financial.

If you have any questions regarding whether a person or entity's function qualifies as a BA, contact the Office of Procurement.

Business Associate Agreement (BAA): a legally binding agreement entered into by a Covered Entity and BA that establishes permitted and required uses and disclosures of PHI, provides obligations for the BA to safeguard the information and to report any uses or disclosures not provided for in the agreement, and requires the termination of the agreement if there is a material violation.

Covered Entity: A facility that conducts Health Care Operations involving the creation and transmission of PHI. Each facility in Northwell Health which conducts Health Care Operations is its own Covered Entity. These Covered Entities are collectively considered an Organized Health Care Arrangement which allows each of the included Covered Entities to share PHI for treatment, payment and Health Care Operations without the requirement of a BAA between Covered Entities.

De-Identification: The process by which identifiers are removed from the health information to mitigate privacy risks to individuals and thereby support the secondary use of data for comparative effectiveness studies, policy assessment, life science research, and other uses. De-identified health information is not protected by the Privacy Rule because it does not fall within the definition of PHI.

Department Manager: The person with managerial responsibility for an identified Northwell Health Department.

Disclosure: The release, transfer, access to, or divulging of information in any other manner outside the entity holding the information.

Electronic Protected Health Information or "ePHI": Any electronic information that is created, received, maintained, stored or transmitted by the Health System via electronic digital or computerized systems.

Health Care Operations: Activities of a Northwell Health facility as they relate to covered functions, including, but not limited to, quality assessment and improvement activities, reviewing the competence or qualifications of health care professionals, activities related to contracting for health insurance or health benefits, conducting or arranging for medical review, legal review, or auditing functions, business planning and development, and business management and administrative activities.

Identifying Code: A code or other means of record identification that may be assigned, to allow information that has been de-identified to be re-identified by the Covered entity - Northwell facility. The identifying code or other means must not be otherwise capable of being translated so as to identify the individual. In addition, the code or other means of record identification must not be used for any other purpose and must not disclose the mechanism for re-identification.

Institutional Review Board (IRB): A committee constituted in compliance with the Department of Health and Human Services (DHHS) regulations at 45CFR46 and FDA regulations at 21CFR50 that has been formally designated by an institution to review and monitor biomedical and behavioral research involving human subjects. In accordance with regulations, an IRB has the authority to approve, require modifications in, or disapprove research. The purpose of IRB review is to ensure, both in advance and by periodic continuing review, that appropriate steps are taken to protect the rights and welfare of humans participating as subjects in the research. To accomplish this purpose, IRBs use a group process to review research protocols and related materials (e.g., informed consent documents and investigator brochures) to ensure protection of the rights and welfare of human subjects of research.

Minimum Necessary: The minimum necessary standard, a key protection of the HIPAA Privacy Rule, is derived from confidentiality codes and practices in common use today. It is based on sound current practice that protected health information should not be used or disclosed when it is not necessary to satisfy a particular purpose or carry out a function. The Privacy Rule's requirements for minimum necessary are designed to be sufficiently flexible to accommodate the various circumstances of any covered entity.

Payment: The actions taken by a health care provider or health plan to obtain or provide reimbursement for the provision of health care.

Protected Health Information ("PHI"): Any oral, written, or electronic individually identifiable health information. PHI is information created or received by Northwell that (i) may relate 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 payment for the provision of health care to an individual; and (ii) identifies the individual who is the subject or based on which there is a reasonable basis to believe that the individual who is the subject can be identified. The Health Insurance Portability and Accountability Act (HIPAA) further clarifies that PHI includes information that identifies the individual by one or more (depending on context) of the following 18 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;
13. Medical device identifiers;
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.

Treatment: The provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party, consultation between health care providers relating to a patient, or the referral of a patient for health care from one health care provider to another.

PROCEDURE

De-identifying PHI under the Privacy Rule

HIPAA allows a Covered Entity to de-identify data by removing all 18 elements of PHI that could be used to identify the individual or the individual's relatives, employers, or household members. The Covered Entity must ensure that the remaining information could not be used alone or in combination with other information to identify the individual who is the subject of the information.

Minimum Necessary Standard

The minimum necessary standard will generally not apply if the health information has been de-identified.

Sensitive PHI

The Privacy Rule provides heightened protection for special categories of PHI. De-identifying PHI in these categories may require additional authorization and/or consultation with the Department Chair.

The following categories of PHI are treated with heightened privacy protections:

- Psychotherapy notes (See Northwell Health Policy #800.02, *Disclosure, Release, and Use of Protected Health Information*); and

- PHI accessed, used, or disclosed for research purposes (See Northwell Health Policy #GR094, *Access Use and Disclosure of Protected Health Information for Research*).

Methods for De-identification of PHI

PHI can be de-identified by using one of the two methods listed below:

1. **Safe Harbor Method:** This requires deleting the following specified identifiers from PHI of the individual or of relatives, employers, or household members. In addition, the Northwell Health facility or Business Associate must ensure that the information could not be used alone or in combination with other information to identify an individual who is a subject of the information.
 - Names,
 - All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip codes and equivalent geocodes (the population in any zip code must be more than 20,000 people when combining the first three digits),
 - All elements of dates except year that is directly related to an individual, including birthdate, admission date, discharge date, date of death (ages over 89 may be aggregated to a category of 90 or older),
 - Telephone numbers,
 - Fax numbers,
 - Electronic mail addresses,
 - Social Security numbers,
 - Health plan beneficiary numbers,
 - Certificate/license numbers,
 - VIN and serial numbers, including license plate numbers,
 - Device identifiers and serial numbers,
 - URLs,
 - IP addresses,
 - Biometric identifiers, including fingerprints and voice prints,
 - Full face photographs,
 - Any other unique identifying number.
 - The Covered Entity 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.
2. **Expert Determination:** A biostatistician or other qualified person with appropriate knowledge of and experience with statistical and scientific principles and methods for rendering information not individually identifiable can apply such principles and methods and 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.

Methods and results of the analysis that justify an expert determination must be documented. The person making this determination must be an independent third party and the documentation should be filed with the original copies of the information in a secure location.

Re-identification of Health Information

An identifying code may be assigned, or another means of record identification may be used, to allow information de-identified under this policy to be re-identified by Northwell Health provided that:

- 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
- Northwell Health 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.

Refer to HHS.gov for more information regarding what constitutes “any other unique identifying number, characteristic, or code” with respect to the Safe Harbor method of the Privacy Rule.

PHI for Research

PHI may be used or disclosed only for research purposes without an Authorization; if granted a waiver of authorization by a Northwell Health-authorized IRB; or a limited data set pursuant to a data use agreement. Questions regarding access to, or the use or disclosure of, PHI for research purposes should be directed to the Human Research Protection Program or the Office of Research Compliance.

For more information refer to the *Northwell Health Policy #GR094 Access Use and Disclosure of Protected Health Information for Research*. All applicable research policies must be followed.

Access and Disclosure Restrictions

Individuals have the right to request restrictions on the access, use or disclosure of their PHI (*See Northwell Health Policy #800.46*).

Obligation of Department Managers

It is the responsibility of each Department Manager to evaluate the PHI generated and received within their Departments. The Department Manager must thereafter work with the appropriate individuals within the Department to develop and implement reasonable procedures to safeguard all PHI as related to this policy.

Obligation of Department Chairs, Directors or Conference Leaders

It is the responsibility of the Department Chair, Department Director, Conference Leader or other appropriate individual, as applicable, to ensure that only those necessary individuals attend internal medical education conferences in which PHI is discussed. At all such medical education conferences, any reference to the identity of patients shall be redacted from the case presentation. The case will be given a fictitious name or de-identified number that will be used throughout the discussion, but will not be associated with the patient’s PHI in any way. In cases where the identity of the patient could potentially be known because the case is unique, a HIPAA authorization form should be obtained from the patient.

Training and Security Reminders

The Office of Corporate Compliance will provide training on HIPAA on, at least, an annual basis.

Document Retention

Any documentation generated in compliance with this policy will be retained for a minimum of 6 years from the date of creation or last revision date, whichever is later in accordance with Northwell Health HIPAA policies and procedures.

Questions related to access to, or the use or disclosure of, PHI should be directed to the facility Privacy Officer.

REPORTING AND ENFORCEMENT

All violations of this policy or questions regarding the access, use, disclosure of PHI shall be reported to the appropriate manager/supervisor/director or to the Office of Corporate Compliance (516-465-8097) for appropriate resolution of the matter. The HelpLine is available 24 hours a day, seven days a week at (800) 894-3226 or online at www.northwell.ethicspoint.com, is accessible and allows for questions regarding compliance issues to be asked and for compliance issues to be reported. Reports of potential fraud, waste and abuse and compliance issues also may be made directly to the Chief Corporate Compliance Officer or designee in person, in writing, via email, mobile device via a QR code, or by telephone.

All reports received by the Office of Corporate Compliance are investigated and resolved to the fullest extent possible. The confidentiality of persons reporting compliance issues shall be maintained unless the matter is subject to a disciplinary proceeding, referred to, or under investigation by Medicaid Fraud Control Unit, Office of Medicaid Inspector General or law enforcement, or disclosure is required during a legal proceeding, and such persons shall be protected under the required provider's policy for non-intimidation and non-retaliation.

Violations of this policy will be subject to disciplinary action as outlined in the Human Resources Policy and Procedure Manual and *Northwell Health Policy #800.73 – Compliance Program Disciplinary Standards for Non-Employees*.



REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- Health Insurance Portability and Accountability Act, 45 CFR Parts 164.502(d) and 164.514(a)-(c)
- Health Information Technology for Economic and Clinical Health (HITECH) 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)

- Protection of Human Subjects, 45 CFR Part 46, and 21 CFR Part 50
- Northwell Health Human Resources Policy and Procedure Manual
- Northwell Health Bylaws, Rules and Regulations of the Medical Staff
- Northwell Health Notice of Privacy Practices
- Northwell Health Policy #100.25 Health Care Proxy, Health Care Agent, Patient Representative, Support Person and Caregiver Designation Policy
- Northwell Health Policy #100.97 - Records Retention and Destruction
- Northwell Health Policy #800.46 – Patients’ Rights to Request Confidential Communications and Disclosure Restrictions of Protected Health Information
- Northwell Health Policy #800.02 – Disclosure, Release and Use of Protected Health Information
- Northwell Health Policy #900.00 – Acceptable Computer Use Policy
- Northwell Health Policy #GR094 – Access, Use and Disclosure of Protected Health Information for Research
- Northwell Health Policy #GR056 – Research with Human Subjects
- Northwell Health Policy #800.73 – Compliance Program Disciplinary Standards for Non-Employees

CLINICAL REFERENCES/PROFESSIONAL SOCIETY GUIDELINES

N/A

ATTACHMENTS

N/A

FORMS

<https://secure.vitaldocs.cexpforms.com/>

- #VD001 – Authorization for Release of Health Information

APPROVALS:	
Northwell Health Policy Committee	4/23/2024
System PICG/Clinical Operations Committee	5/22/2024

Standardized Versioning History:

Approvals: * =Northwell Health Policy Committee; ** = PICG/Clinical Operations Committee; ✖ = Provisional; ♦ = Expedited

*09/28/17

**10/19/17

✖03/28/19

*04/25/19

**05/10/19

*04/22/21

**05/13/21

*03/21/23

**04/20/24