



<b>POLICY TITLE:</b>  Disposal Policy for Protected Health and Confidential Health System Information	<b>SYSTEM POLICY AND PROCEDURE MANUAL</b>
<b>POLICY #:</b> 800.47	<b>CATEGORY:</b> Compliance & Ethics
<b>System Approval Date:</b> 03-21-2024	<b>Effective Date:</b> 01/2013
<b>Site Implementation Date:</b> 05-06-2024	<b>Last Reviewed/Approved:</b> 05/2022
<b>Prepared by:</b> Corporate Compliance	<b>Notations:</b> N/A

## GENERAL STATEMENT of PURPOSE

The purpose of this document is to outline the established requirements for disposal of Northwell Health hard copy documents and electronic media that contain Confidential Information, including, but not limited to, Protected Health Information (“PHI”) and Personally Identifiable Information (“PII”). Confidential information is defined as “sensitive” and “highly sensitive” according to Policy #900.12 - *Data Classification and Handling Policy*. Hard copy documents include, but are not limited to, paper documents, photographs, imaging films, addressograph cards, and wrist bands. Electronic media include, but are not limited to, hard drives, flash drives and CDs.

## POLICY STATEMENT

It is the policy of Northwell Health that all Northwell Health information and information entrusted to Northwell Health from third parties will be disposed of in a manner that ensures confidentiality in accordance with federal and state laws including the Health Insurance Portability and Accountability Act (“HIPAA”). All applicable documents will be discarded using the appropriately identified trash receptacles.

## 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

**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 a 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.

**Personally Identifiable Information (PII):** Any information about an individual maintained by an agency, including (i) any information that can be used to distinguish or trace an individual’s identity, such as name, Social Security number, date and place of birth, mother’s maiden name, or biometric records; and (ii) any information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

The following list contains examples of information that may be considered PII:

1. Name, such as full name, maiden name, mother’s maiden name, or alias
2. Personal identification number, such as Social Security number (SSN), passport number, driver’s license number, taxpayer identification number, patient identification number, and financial account or credit card number

3. Address information, such as street address or email address
4. Asset information, such as Internet Protocol (IP) or Media Access Control (MAC) address or other host-specific persistent static identifier that consistently links to a particular person or small, well-defined group of people
5. Telephone numbers, including mobile, business, and personal numbers
6. Personal characteristics, including photographic image (especially of face or other distinguishing characteristic), x-rays, fingerprints, or other biometric image or template data (e.g., retina scan, voice signature, facial geometry)
7. Information identifying personally owned property, such as vehicle registration number or title number and related information
8. Salary and bonus information
9. Work eligibility
10. Citizenship
11. Criminal records
12. Date of death or death certificate number
13. Dependent information
14. Disability information
15. Other information about an individual that is linked or linkable to one of the above (e.g., date of birth, place of birth, race, religion, weight, activities, geographical indicators, employment information, medical information, education information, financial information)

All PII shall at all times be subject all applicable laws, including, without limitation, the New York State Social Security Number Protection Law, New York State Labor Law, and Fair Credit Reporting Act. This includes all PII relating to members of the Northwell workforce. All PII that is also PHI shall, at all times, also be subject to all applicable laws and Northwell policies regarding PHI, as set out above.

## **PROCEDURE**

1. All waste/trash shall be collected from designated areas (e.g., patient rooms, utility rooms, offices) through the facility on a regular basis as needed, by Environmental Services personnel.
2. All hard copy and electronic waste containing PHI, PII or any other sensitive or highly sensitive information must be properly discarded as follows:
  - a. Paper items must be discarded in confidential document bins or cross-cut shredders.
  - b. Patient information labels, including labels on containers (e.g. IV bag labels, syringes, bottles, vials, etc.), shall be self-shredding or shall be rendered unrecognizable before it is discarded.
  - c. Prescription bottles will be returned to the pharmacy and labels shall be rendered unrecognizable and disposed of appropriately.

- d. Hard copy data in non-paper form (e.g., microfilm, microfiche, imaging films) cannot be discarded in confidential document bins designated for paper waste only and thus any PHI, PII or other sensitive or highly sensitive information on such non-paper form must be rendered unrecognizable and properly discarded either internally or through a Northwell Health approved and contracted vendor.
  - e. Electronic media is governed by Northwell Health Policy #900.26 – *Media Reuse and Disposal Policy*. Policy #900.26 handles procedures that address the removal, re-use and disposition of devices and media containing sensitive or highly sensitive information.
  - f. All hard copy and electronic waste containing PHI, PII, or any other sensitive or highly sensitive information, including any such items removed from any Northwell Health campus by applicable Northwell Health employees, shall be disposed of appropriately.
    - 1. Employees working remotely shall dispose of hard copy PHI and PII off-premises using a cross-cut shredder. Employees printing remotely shall do so in accordance with Policy #900.08 – *Remote Access*.
    - 2. Employees shall not use a vendor (including but not limited to UPS, FedEx, local government sponsored shredding events, etc.) to discard of hard copy and electronic waste containing PHI, PII or any other sensitive or highly sensitive information.
    - 3. Electronic media and computing hardware must be disposed of using methodologies consistent with the National Institute of Standards and Technology (NIST) publication 800-88 Guidelines for Media Sanitization.
      - i. Northwell hardware and electronic media waste containing sensitive or highly sensitive information must be properly disposed of in accordance with Policy #900.26 - *Media Reuse and Disposal Policy*.
  - g. Hard copy waste must not be “overstuffed” into the container, such that the container’s contents protrude and can be removed from the container. If the container is close to overflowing, Environmental Services must be contacted immediately for assistance.
  - h. For proper disposal of Electronic Media, please refer to *Policy #900.26 – Media Reuse and Disposal Policy*. Employees must contact the Northwell Health Digital IT&S Service Desk to arrange for disposal of electronic media. Northwell Health Digital IT&S Service Desk (516) (718) (631) 470-7272.
3. Employees handling items containing PHI, PII or other sensitive or highly sensitive information are responsible to ensure all such information, whether on or off-site, has been secured or destroyed. It is the office manager/supervisor/director's responsibility to ensure that all employees are adhering to this policy.

4. In accordance with Policy #100.97 -*Records Retention and Destruction*, all documents must be maintained for the appropriate length of time before being disposed of as indicated above.
5. Standard document disposal and destruction policies shall be immediately suspended once there is a notification that the documents are or may be part of a government investigation, audit, subpoena, search warrant, litigation hold, or document sequestration. In case of questions regarding document maintenance, the Office of Legal Affairs must be contacted.
6. Document destruction shall be performed by an authorized vendor. Access to waste containers shall be limited to the vendor and/or an authorized designee at each facility.
7. Compliance Monitoring: the Office of Corporate Compliance shall perform periodic audits to monitor compliance with this policy.

### **Training**

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

### **Sanctions**

In compliance with the HIPAA Privacy Rule, violations of this policy will be subject to disciplinary action as outlined in the Human Resources Policy and Procedure Manual and in the Bylaws, Rules and Regulations of the Medical Staff.

### **Document Retention**

Any documentation generated in compliance with this policy will be retained for a minimum of 6 years from the date of its creation.

## **REPORTING AND ENFORCEMENT**

All violations of this policy 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](http://www.northwell.ethicspoint.com), is accessible to all Affected Individuals 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 in the

Bylaws, Rules and Regulations of the Medical Staff and an Affected Individual's contract with Northwell Health.



## **CONTACT INFORMATION**

Environmental Services	516-734-3001
Information Services	(718, 516, 631) 470-7272
Office of Corporate Compliance	516-465-8097
Office of Legal Affairs	516-465-8100
Compliance Help Line	800-894-3226
	<a href="http://www.northwell.ethicspoint.com">www.northwell.ethicspoint.com</a>

## **REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES**

- Human Resources Part 5-3 Conduct in the Workplace/Progressive Discipline
- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164
- 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)
- Northwell Health Policy #100.97 – Records Retention and Destruction
- Northwell Health Policy #350.25 – Pharmaceutical Waste Management
- Northwell Health Policy #800.02 – Disclosure, Release and Use of Protected Health Information
- Northwell Health Policy #900.12 – Data Classification and Handling Policy
- Northwell Health Policy #900.26 – Media Reuse and Disposal Policy
- Northwell Health Policy #900.08 – Remote Access

## **CLINICAL REFERENCES/PROFESSIONAL SOCIETY GUIDELINES**

N/A

## **ATTACHMENTS**

N/A

## FORMS

N/A

<b><u>APPROVAL:</u></b>	
Northwell Health Policy Committee	02/27/2024
System PICG/Clinical Operations Committee	03-21-2024

### Standardized Versioning History:

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

☒11/29/12

\*12/17/12

\*\*01/24/13

\*03/31/16

\*\*04/21/16

♦06/18/18

♦06/25/20

\*04/28/22

\*\*05/19/22