North Shore-LIJ Health System is now **Northwell Health**

POLICY TITLE: Data Encryption and Integrity Policy	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.25	**CATEGORY:** Information Services
System Approval Date: 4/20/17 **Site Implementation Date:** 5/23/17	**Effective Date:** 10/25/12 **Last Reviewed/Approved:** 12/13/12
Prepared by: Office of the CIO – IS Policy and Procedure Committee	**Superseded Policy(s)/#/Notations:** N/A

GENERAL STATEMENT of PURPOSE

This document establishes the encryption requirements for Northwell Health ("Northwell"), and use of cryptography to ensure that protected health information (PHI), personally identifiable information (PII), and other sensitive and highly sensitive information are protected during transmission and while at rest.

POLICY

Northwell shall use encryption safeguards and integrity controls to protect sensitive and highly sensitive information from unauthorized access or changes. Data types such as PII and PHI are defined in the *900.12 Data Classification and Handling Policy* and are subject to this policy.

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 Hofstra Northwell School of Medicine conducting research on behalf of the School of Medicine on or at any Northwell Health facility; and the faculty and students of the Hofstra Northwell School of Graduate Nursing and Physician Assistant Studies.

DEFINITIONS

Cryptographic Key: The information required to encrypt and decrypt data.

Cryptographic Key Custodian: The person or department responsible for managing the cryptographic key software.

Cryptography or Encryption: A method of converting an original message of regular text into encoded text. The text is encrypted by means of an algorithm (such as a type of procedure or formula). If information is encrypted, there is a low probability that anyone other than the receiving party who has the key to the code, or access to another confidential process, would be able to decrypt (translate) the text and convert it into plain, comprehensible text.

Decrypt: The process of reversing encryption to make data readable again.

Electronic Protected Health Information (ePHI): Any protected health information (PHI) that is created, received, maintained, stored, or transmitted by Northwell via electronic, digital, or computerized systems.

Encrypt: The process of making data unreadable in order to protect the information.

Federal Information Processing Standard (FIPS): A U.S. government computer standard used to accredit cryptographic modules.

Hardware and Electronic Media: All stationary and portable hardware, devices, and storage that access or contain sensitive or highly sensitive information from Northwell's network. This includes, but is not limited to:

- Servers, workstations, and laptops
- Hard disk drives (fixed or removable)
- Implantable and wearable devices
- Smartphones and tablets
- mp3 players (in data mode)
- USB portable drives (for example, flash drives)
- SD cards and other removable memory cards
- CDs and DVDs
- Backup tapes and related media

Highly Sensitive Information: Protected health information or any information that, if lost, corrupted, disclosed to, or accessed by an unauthorized person, or disclosed or accessed by unauthorized means, may (i) violate federal, state, and/or local law, (ii) cause significant harm, injury, or damage to another person or entity, or (iii) cause financial loss to another person or entity. Examples include, but are not limited to, Social Security numbers, credit card data, and driver's license information. Refer to the *900.12 Data Classification and Handling Policy*.

Integrity Controls: Technical safeguards designed to detect and/or prevent unauthorized alteration or deletion of data.

Legacy System: An older computer, system, or application in which either vendor support or updates are no longer available, or Northwell has retired and no longer actively uses for production.

Mobile Device: A small portable device, including tablets and smartphones, used for computing and/or communication.

Non-Northwell Equipment: Any computing device not purchased by Northwell that connects to the Northwell Network, but is not a member of the enterprise domain. This includes, but is not limited to:

- Personal laptops
- Smartphones
- Vendor supplied servers
- Tablets (iPads, Kindles, etc.)

Personally Identifiable Information (PII): Any information about an individual maintained by an agency, including (1) 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 (2) any other 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. 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).

Private Key: An encryption/decryption key known only to the party or parties that exchange the encrypted messages.

Protected Health Information (PHI): Any oral, written, or electronic individually identifiable health information. PHI may relate to the past, present, or future physical or mental health or condition of an individual; the provision of healthcare to an individual; or the payment for the provision of healthcare to an individual. The Health Insurance Portability and Accountability Act (HIPAA) further defines PHI as 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 the year) 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) addresses;
16. Biometric identifiers, including finger and voice prints;
17. Full face photographic images and any comparable images;
18. Any other unique identifying number, characteristic, or code.

Removable Media: Any removable storage device (e.g., CDs, DVDs, portable hard drives, tapes, and USB drives).

Sensitive Information: Any information that, if lost, corrupted, disclosed to, or accessed by an unauthorized person, or disclosed or accessed by unauthorized means, may cause harm, injury, or damage to another person or entity. Examples include, but are not limited to, a number of personally identifiable information data elements that are not highly sensitive. Refer to the *900.12 Data Classification and Handling Policy*.

PROCEDURE/GUIDELINES

1. Encryption Requirements

a. Where reasonable and appropriate, encryption controls that meet Northwell standards (e.g., FIPS validated cryptography and encryption algorithms) must be used to secure electronic information classified by the *900.12 Data Classification and Handling Policy* as sensitive or highly sensitive, whether the data is being transmitted (data in transit) or stored (data at rest). The reasonableness and appropriateness of implementing encryption controls are determined based on:
   i. Level of risk for data disclosure.
   ii. Ability of the system to encrypt data in transit and data at rest.
   iii. Availability of third party solutions for encryption.

iv. Impact to operations and user experience (e.g., performance, ease of use, latency, and hardware requirements).
v. Cost to implement and support.

b. If reasonable and appropriate encryption controls are determined not to be available, Northwell shall document the decision to store and/or transmit unencrypted data by exception, as well as any compensating controls. Northwell shall review such exceptions periodically.
c. Legacy systems that do not support encryption must have alternate safeguards in place to protect against malicious or unauthorized access.

2. Cryptographic Keys

a. All cryptographic keys must be protected against modification, loss, or destruction.
b. Encryption key length must meet Northwell standards.
c. All encryption keys used to secure Northwell data are the property of Northwell and managed by approved key management software.
d. Northwell Information Services team members designated as cryptographic key custodians are responsible for managing the application or software that manages the keys.
e. Where possible, the cryptographic key custodians should have procedures in place to recover encrypted information in the event that a cryptographic key is lost, compromised, or damaged.
f. Service level agreements or contracts with external suppliers of cryptographic services must cover issues of liability, reliability of services, and response times for the provision of services.
g. All regulations and federal restrictions that apply to the use of cryptographic techniques and restrictions for exporting encrypted information across international borders must be adhered to.

3. Hardware and Electronic Media Encryption

a. Northwell hardware and electronic media that store sensitive and highly sensitive information must be encrypted using approved standard encryption software. This includes, but is not limited to, laptops, mobile devices, USB flash drives, and system backups.
b. Sensitive and highly sensitive information must not be stored on personally-owned or third party laptops, workstations, or portable devices without a valid business need. If there is an approved business need (as determined by the local leadership) the device must be encrypted using Northwell's approved standards, with the exception of information in electronic format provided to a patient or patient's representative, as indicated in the *800.02 Release of Protected Health Information for Living Patients Policy*.

4. Integrity Controls

a. The storage or transmission of sensitive or highly sensitive information must use encryption that meets Northwell standards.

b. When reasonable and appropriate, and when the technology is available, data integrity controls that meet Northwell standards (e.g., FIPS validated cyptography and encryption algorithms) must be employed to protect sensitive and highly sensitive information from

being stored or transmitted or from improper or unauthorized alteration, tampering, corruption, or falsification.

c. If reasonable and appropriate integrity controls are determined not to be available, Northwell shall document the decision to store or transmit unencrypted data by exception, as well as any compensating controls. Northwell shall review such exceptions periodically.

ENFORCEMENT

Users should report any violations of this policy immediately to their respective managers. If appropriate, the violation should be escalated and reported to the IS Service Desk or the Office of Corporate Compliance HelpLine. Anyone found in violation of this policy may be subject to disciplinary action, up to and including termination of employment or engagement, as applicable, in consultation with Human Resources.

CONTACT INFORMATION

What	Where
Northwell Health Service Desk	(516) (718) (631) 470-7272
Northwell Health Service Desk Email	servicedesk@northwell.edu
IT Security Hotline Email	ITSecurity@northwell.edu
Office of Corporate Compliance HelpLine	(800) 894-3226
Office of Corporate Compliance Website	www.northwell.ethicspoint.com

REFERENCES TO REGULATIONS AND/OR OTHER RELATED POLICIES

- #800.02 Release of Protected Health Information for Living Patients Policy
- #800.42 Confidentiality, Use, Access and Disclosure of Protected Health Information Policy
- #900.06 Anti-Virus Policy
- #900.11 Electronic Mail (E-Mail) Acceptable Use
- #900.12 Data Classification and Handling Policy
- S900.25.01 Encryption Standards
- S900.25.02 Data Integrity Check Standards
- Health Information Technology for Economic and Clinical Health (HITECH) Act
- Health Information Trust Alliance (HITRUST) Common Security Framework (CSF) Control Objective Names: 6.03 Information System Audit Considerations, 09.08 Exchange of Information, 10.03 Cryptographic Controls
- Health Insurance Portability and Accountability Act (HIPAA), Security Final Rule, 45 CFR 164.312(a)(2)(iv) Access Controls – Encryption and Decryption, 164.312(a)(2)(ii) Transmission Controls - Encryption
- Payment Card Industry Data Security Standards (PCI DSS) v2 3.5.2 and v2.3.6.6
- The Joint Commission IM.02.01.03, EP 2, EP 6

CLINICAL REFERENCES/PROFESSIONAL SOCIETY GUIDELINES
N/A

ATTACHMENTS
N/A

FORMS
N/A

APPROVAL:	
System Administrative P&P Committee	3/30/17
System PICG/Clinical Operations Committee	4/20/17

Standardized Versioning History:
*=Policy Committee Approval; ** =PICG/Clinical Operations Committee Approval

10/25/12	Provisional Approval
*11/29/12	Final Approval
	**12/13/12