Northwell Health

POLICY TITLE: Data Classification and Handling Policy	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.12	**CATEGORY:** Information Services
System Approval Date: 4/21/16 **Site Implementation Date:** 6/3/16	**Effective Date:** 11/09 **Last Reviewed/Revised:** 8/13
Prepared by: Office of Corporate Compliance; Office of the Chief Information Officer; Data Privacy Committee	**Superseded Policy(s)/#:** N/A

GENERAL STATEMENT of PURPOSE

The purpose of this policy is to provide guidelines for classifying and handling various types of data. It provides direction for determining the criticality of information and the assignment of appropriate security guidelines to ensure the confidentiality, integrity, and availability of information to the extent required by Northwell Health ("Northwell") and applicable law. Throughout this policy, the words "data" and "information" shall be used interchangeably.

Data classification encompasses both electronically stored information (ESI) as well as non-electronic information, such as paper files, and hard-copy data. ESI can reside on computers workstations, laptops, smartphones, and storage media such as flash drives, videotape, diskette, CD, DVD, memory cards, and other devices. The foregoing may be used for the creation, receipt, storage, archival, sharing, and deleting of data, and therefore require adequate planning so that issues related to data confidentiality, integrity, and availability can be analyzed and addressed.

Appropriate controls must be in place to protect data from intentional or accidental disclosure, modification, or destruction. Systems that process, store, or forward Northwell information must comply with appropriate levels of security defined for that information.

POLICY

All Northwell data must be categorized into one of two primary classifications, Public or Confidential. In addition, subcategories within the confidential category help further identify appropriate handling and precautions to be taken.

SCOPE

This policy applies to all members of the Northwell Health workforce including, but not limited to: employees, medical staff, volunteers, students, physician office staff, 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 & Physician Assistant Studies.

DEFINITIONS

Protected Health Information (PHI): *Protected Health Information* or PHI is defined as any oral, written or electronic individually identifiable health information collected or stored by a facility. Individually identifiable health information includes demographic information and any information that relates to the past, present or future physical or mental condition of an individual. The *Health Insurance Portability and Accountability Act* (HIPAA) details eighteen items that render PHI identifiable.

- Names
- 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
- 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
- Telephone numbers
- Fax numbers
- Electronic mail addresses
- Social Security numbers
- Medical record numbers
- Health plan beneficiary numbers
- Account numbers
- Certificate/license numbers
- Vehicle identifiers and serial numbers
- Medical Device Identifiers
- Web Universal Resource Locators (URLs)
- Internet Protocol (IP) address numbers
- Biometric identifiers, including finger and voice prints
- Full face photographic images and any comparable images
- Any other unique identifying number, characteristic, or code

All PHI shall at all times be subject to all applicable laws, including, without limitation, HIPAA and the Health Information Technology for Economic and Clinical Health Act (HITECH), and any Northwell policies regarding PHI. This includes all PHI relating to members of Northwell workforce who are also patients of Northwell. All PHI is classified as Highly Sensitive confidential data. PHI is to be handled in accordance with Northwell policies on PHI.

Personally Identifiable Information (PII): *Personally Identifiable Information* or PII is defined as any oral, written or electronic individually identifiable personal information collected or stored by a facility. Examples of PII include the following data elements.

- Bank/Credit Union account numbers
- Biometrics (finger/face print)
- Birth certificate
- Citizenship
- Credit card expiration date
- Credit card number
- Criminal records
- Date of birth
- Date of death
- Death certificate number
- Dependent information
- Disability information
- Driver's license number
- Financial data
- Home address
- Home phone number
- IP address
- Mother's maiden name
- Name
- Other identity verification or authentication data
- Passport number
- Personal phone number
- Personal e-mail address
- Photo
- Race or Ethnicity
- Salary and bonus
- Social Security number
- Vehicle registration plate number
- Work eligibility

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 time, also be subject to all applicable laws and Northwell policies regarding PHI, as set out above.

PROCEDURE/GUIDELINES

A. ROLES & RESPONSIBILITIES

1. All Northwell workforce members who, in the course of their duties, have authorized

access to, or come in contact with, Northwell data are required to be familiar with and abide by the requirements of this policy, and to address any questions they may have about it, or concerns they may have about compliance with it, to his or her supervisor or manager.

2. All Northwell workforce managers are required to report any non-compliance with this policy to the Compliance Director/Privacy Officer for his or her respective facility. Policy violations may also be reported to the Office of Corporate Compliance at (516) 465-8097 or **www.northwell.ethicspoint.com**, or may be reported anonymously to the Office of Corporate Compliance Helpline at (800) 894-3226.

B. DATA CLASSIFICATION REQUIREMENTS

Data Classification is the process of categorizing all Northwell information, based on its sensitivity, business value and context, and determines the level of safeguards that are applied to the information. All such information must be categorized into one of two primary classifications: Public or Confidential. Confidential information will be further classified as *Highly Sensitive*, *Sensitive* or *Internal Information*. All PHI is deemed Highly Sensitive Information. Any information that does not fall under the classifications of Public, Highly Sensitive or Sensitive Information shall be deemed to be Internal Information.

1. Public Information

Public Information is Northwell data that may be released, with appropriate Northwell authorization, to the general public, competitors, and the press (for example, in the public domain). Examples of Public Information include, but are not limited to, the following.

- Press announcements
- Regulatory filings, such as Internal Revenue Service filings
- Certification labels such as NCQ or The Joint Commission Certification
- General public health awareness or regulation awareness publications
- General sales, literature or marketing materials
- Business contact information

If there is ever a question as to whether information is or may be made public, contact Office of Public Affairs at (516) 465-2640. The use and release of any Public Information must at all times comply with applicable copyright laws.

2. Confidential Information

All information that is not *Public* is considered Confidential. Confidential information is further classified by Northwell as *Highly Sensitive*, *Sensitive*, or *Internal*.

a) Highly Sensitive: PHI 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 number, credit card data, and driver's license information.

b) Sensitive: 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 not limited to, a number of PII data elements listed above.

c) Internal: Any confidential information that does not fall under the classifications of Highly Sensitive or Sensitive Information shall be deemed to be Internal Information.

C. IMPLEMENTATION

Implementation of the data classification framework described above encompasses both ESI as well as non-electronic information, such as paper files, and hard-copy data.

D. DATA HANDLING

PHI is to be handled in accordance with Northwell policies on PHI.

Northwell workforce members must distribute or transmit only the minimum amount of Confidential data required to accomplish the intended purpose to only those who need-to-know the information.

Any data subject to a document hold, in accordance with *Policy# 100.97 the Records Retention and Destruction Policy* must be treated as *Highly Sensitive* data and follow the associated requirements.

Additional data handling requirements are described in Addendum A.

ENFORCEMENT

Users should report any violations of this policy immediately to his or her manager. If appropriate, the violation should be escalated and reported to the IS Help Desk or the Office of Corporate Compliance Help Line. 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 Help Desk	(516) (718) (631) 470-7272
Northwell Health Help Desk Email	servicedesk@northwell.edu
IT Security Hotline Email	ITSecurity@northwell.edu
Office of Corporate Compliance Help Line	(800)-894-3226
Office of Corporate Compliance Website	www.northwell.ethicspoint.com

Note: The Data Privacy Committee includes members from the Audit, Corporate Compliance, HR, IT, Legal, Procurement and Risk Management departments.

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- NYS Employee Personal Identifying Information Law
- NYS Social Security Number Protection Law
- Health Insurance Portability and Accountability Act
- 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)
- NYS Mental Hygiene Law §33
- NYS Public Health Law §18
- Northwell Health Human Resources Policy and Procedure Manual, Part V
- Northwell Health Bylaws, Rules and Regulations of the Medical Staff
- 100.25 Health Care Proxy, Health Care Agent, Patient Representative and Support Person Designation Policy
- 800.42 Confidentiality, Use, Access and Disclosure of Protected Health Information
- 800.02 Use, Access and Disclosure of Protected Health Information with Valid Authorization
- 900.00 Computer Use Policy
- 900.01 Internet Usage Policy
- 900.03 Cellular and Smart Phone Purchase Usage Policy
- 900.11 Electronic Mail (E-Mail) Acceptable Use
- 100.97 Records Retention and Destruction
- 900.26 Device and Media Control Policy
- 800.47 Disposal Policy for Protected Health and Confidential Health System Information
- HR Policy, Part V/ Section 2 Confidentiality
- HR Policy, Part XII/Section 11 Social Media Acceptable Use

CLINICAL REFERENCES

N/A

FORMS

N/A

ATTACHMENTS

Addendum A: Data Handling Requirements

APPROVAL:	
System Administrative P&P Committee	11/10/09; 7/25/13; 3/31/16
System PICG /Clinical Operations Committee	11/19/09; 8/15/13; 4/21/16

Versioning History:

11/09

7/13

ADDENDUM A: DATA HANDLING REQUIREMENTS

DATA CREATION	Assign responsible Data Owner. Categorize the data as either: Public, Internal, Sensitive or Highly Sensitive.

HANDLING REQUIREMENTS

CATEGORY	PUBLIC	INTERNAL	SENSITIVE	HIGHLY SENSITIVE
Data Handling	No specific handling required.		• Data may only be handled with the approval of the Data Owner and for legitimate business purposes. • Data must be appropriately handled in a manner providing reasonable assurance that unauthorized persons do not gain access.	
Release to third parties	No special handling.	May be distributed with the consent of the data owner and in accordance with Northwell policies and guidelines.	Access to this information is on a limited need-to-know basis, and may be distributed only: • If required by law or regulation; or • Pursuant to a lawfully issued subpoena; or • As required by contract, subject to appropriate non-disclosure restrictions; or • If necessary in the course of a legal proceeding; or • With the consent of the individual; or • Pursuant to a waiver of authorization issued by a Northwell—authorized Institutional Review Board Access must be logged and reviewed by the data owner.	

TRANSMISSION REQUIREMENTS—see also policies 900.11, 900.11 A, 900.18, 900.01 and 900.03

CATEGORY	PUBLIC	INTERNAL	SENSITIVE	HIGHLY SENSITIVE
Interoffice mail	No special handling.		• Sealed inter-office envelope marked and labeled Confidential. • Notify recipient in advance. • Confirm receipt.	
Mail outside of organization	No special handling.		Trackable delivery required. For example, Federal Express or similar courier service.	

TRANSMISSION REQUIREMENTS—see also policies 900.11, 900.11 A, 900.18, 900.01 and 900.03 (continued)				
CATEGORY	**PUBLIC**	**INTERNAL**	**SENSITIVE**	**HIGHLY SENSITIVE**
Email	No special handling.		• Encrypted email sent to an external address. • Confirm intended email address. • Do not include confidential information in the subject line.	
IM (Instant Messaging) and Texting	No special handling.		Do not use for Confidential data.	
Fax	Use cover sheet. Use care in dialing.	Locate in non-public area. Use cover sheet. Use care in dialing.	• Locate in area not accessible to general public and unauthorized persons. • Use of confidential coversheet required. • Use particular care in dialing. • Telephone notification prior to transmission and subsequent telephone confirmation of receipt required. • Remove originals from the fax. • Erase fax cache periodically where possible.	
Internal Network Communications	No special handling.		Distribute on an as-needed basis only as necessary. Encrypt where possible.	
External Network Communications (for example, internet or social networks)	No special handling.		• Do not post any Confidential data in a public forum, such as an unprotected cloud service, electronic forum or social network. • Encrypt electronic data being transmitted externally.	
Audible Communication (such as PA, phone, mobile, conference calls, verbal communications)	No special handling.	Use reasonable precautions so that others cannot overhear.	• Use audio conference passwords. As appropriate, these passwords should be changed periodically. • Private meeting area, avoiding proximity to unauthorized listeners. • Speakerphone use discouraged. • No overhead pages.	

ADDENDUM A: DATA HANDLING REQUIREMENTS

STORAGE REQUIREMENTS—see also policies 900.00 and 900.11				
CATEGORY	**PUBLIC**	**INTERNAL**	**SENSITIVE**	**HIGHLY SENSITIVE**
Printed Material	No special handling.		• Store in a secure area. • Maintain a clear desk. Workforce members should "clear their desks" at the end of each work day. This not only includes documents and notes, but also any post-its, and removable media with PHI. • Documentation owned and/or created by Northwell must be labeled CONFIDENTIAL.	
Electronic Documents	No special handling.	Storage on Northwell—approved devices is required.	• Storage on Northwell-approved devices is required. • Control access and print capability. • Store on secure network drives only (not on hard drives or desktops). • Documentation owned and/or created by Northwell must be labeled CONFIDENTIAL.	
Electronic media (such as memory sticks, hard drives, CDs)	No special handling.		Use Northwell-approved encryption.	
Mobile Devices	All mobile devices must employ encryption.			
E-mail	No special handling.		• Use of corporate email system is required. • Where possible, refrain from using email for Confidential data.	
REUSE/DESTRUCTION REQUIREMENTS—see also policies 800.47 and 900.26				
CATEGORY	**PUBLIC**	**INTERNAL**	**SENSITIVE**	**HIGHLY SENSITIVE**
Printed Materials	No special handling. Consider recycling.		Must be discarded in appropriately identified document container for shredding or destruction (except if subject to a legal hold).	
Electronic media (such as memory sticks, hard drives, CDs)	No special handling.		• Media subject to a legal hold may not be reused. If other media are to be reused, all data must first be removed by Information Services. • All discarded media must be destroyed following the	

		guidelines outlined in Policies 800.47 and 900.26.

ADDENDUM A: DATA HANDLING REQUIREMENTS

PHYSICAL SECURITY REQUIREMENTS—see also policy 900.00 and 900.03				
CATEGORY	**PUBLIC**	**INTERNAL**	**SENSITIVE**	**HIGHLY SENSITIVE**
Desktop computers	Users must be authenticated. Password lock, sign-off or power-off when not in use.		• Users must be authenticated with a unique ID. • Screen filters should be used to obscure view, and where applicable, password lock, sign-off or power-off when computer is not in use.	
Mobile Devices (laptops, smartphones etc.)	Laptop users must be authenticated. All mobile devices must utilize password lock, sign-off or power-off when not in use.		• All mobile devices should be kept in a safe location. If lost or stolen, the IS Help Desk should be contacted immediately so that protective measures can be taken to prevent misuse of the device. • Laptop users must be authenticated with a unique ID. • All mobile devices must utilize password lock, sign-off or power-off when not in use.	
Servers	All servers must be located in a secure data center.		All servers must be located in a secure data center.	
Printing/faxing/photocopying	All servers must be located in a secure data center.		Documents must not be left unattended.	

ACCESS CONTROL REQUIREMENTS				
CATEGORY	**PUBLIC**	**INTERNAL**	**SENSITIVE**	**HIGHLY SENSITIVE**
Data Availability	Available to the general public.	Available to authorized users.	• Available only to authorized users. • Data owner may consider more stringent access control.	