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

POLICY TITLE: Facility Access Controls for Protected Health Information (PHI) and Electronic Protected Health Information (EPHI)	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 100.99	**CATEGORY:** Administrative
System Approval Date: 3/19/15 **Site Implementation Date:**	**Effective Date:**11/12 **Last Reviewed/Approved:** 12/12
Prepared by: Scott Strauss, Corporate Director Security & Emergency Management	**Superseded Policy(s)/#:** N/A

GENERAL STATEMENT of PURPOSE

The Health System has developed a security plan to safeguard Protected Health Information (PHI) and Electronic Protected Health Information (EPHI) from unauthorized physical access and to safeguard the equipment from unauthorized physical access, tampering, and theft while ensuring that environmental safeguards are in place to protect the confidentiality, access and integrity of protected health information as commensurate with data criticality and risk assessment.

POLICY

This program documents the Health System's Facilities Security Plan(s) to safeguard the premises and buildings, exterior and interior from unauthorized physical access of PHI and EPHI and to safeguard the equipment and business documents including, but not limited to, clinical and business documents from unauthorized physical access, tampering and theft.

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 or "PHI": 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:

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 data, 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;
18. Any other unique identifying number, characteristic, or code.

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.

Facilities Security Plans: Document the Health System's plans to safeguard the premises and buildings, exterior and interior from unauthorized physical access and to safeguard the equipment and business documents including, but not limited to, clinical and business documents from unauthorized physical access, tampering and theft.

PROCEDURE/GUIDELINES

1. The Health System ensures health information ePHI and PHI or sensitive or highly sensitive information, as defined in the Data Classification and Data Handling Policy (#900.12), is adequately protected from physical access by unauthorized individuals.

2. The IT Risk Governance Committee is responsible for reviewing and assessing material security issues of the Health System facilities that relate to accessing PHI and ePHI.

3. Environmental safeguards are in place protect the integrity of ePHI and PHI or sensitive or highly sensitive information, and those safeguards are commensurate with the criticality of the data, as well as the risk of loss of confidentiality, access or integrity of the data.

Facility Security Plans and Control Mechanisms

4. The Vice President of Protective Services is responsible for ensuring periodic review and modification of Facilities Security Plans to determine if the Facilities Security Plans (completed at the site level) are sufficient in light of its risk assessment. If any discrepancy during a review or at any other time is identified, an investigation led by Protective Services is immediately conducted (by the site) to resolve the discrepancy. Protective Services shall share any material investigations or material changes to Facilities Security Plans with the IT Risk Governance Committee.

Access Control Validation Process and Procedures

5. The Health System has documented procedures for controlling access to facilities containing sensitive or highly sensitive data including ePHI and PHI based on an individual's role and/or function. The Health System has developed procedures pertaining to the control of these individuals. To comply with this standard the Health System has implemented the following:

    (i) The Health System has common controls and barriers that separate users with access to PHI and ePHI based on their role or function. Such common controls include the use of identification badges, locked doors, alarms, surveillance cameras, card access, keypad, and key lock systems designed to allow access to secure facilities on an as-needed basis to those individuals who require access for authorized and legitimate business purposes.

    (ii) The Enterprise Access Control Department or the application owner are responsible for ensuring that the identity and access privileges of an individual are validated before access is granted.

    (iii) The Health System requires individuals' access to be monitored while in its facilities and it is only granted to the areas, equipment and/or information relevant to the individual's purpose.

(iv) The Health System maintains a list of all individuals who have access to the facility. Protective Services and Human Resources, where applicable, are responsible for ensuring that the access list is updated from time to time as access and personnel change.

(v) The Health System maintains a list of all individuals who have access to software programs related to ePHI for testing and revision.

(vi) Information Services is responsible for ensuring that documentation pertaining to those with restricted access to designated Health System secure areas which house ePHI Systems is maintained and updated.

Maintenance Records

6. Applicable Health System facilities will have policies and procedures to document repairs, or modifications to the facility which are related to security (for example, hardware, walls, doors, locks). The Health System will evaluate the effect of the repairs or modifications to the Facility Security Plan(s) as appropriate.

7. Maintenance Records Procedure

   To comply with this standard:

   (i) The Director of Security or his/her appropriate designee will oversee facility changes related to physical security matters.

   (ii) Applicable Health System facilities will establish a log to document repairs and modifications to the facility.

      (a) Only repairs and modifications related to security will be documented.

      (b) The log will include date and the reason for the repair.

   (iii) The log will be retained at the facilities in accordance with the Records Retention and destruction Policy #100.97.

   (iv) The Director of Security or his/her appropriate designee will periodically review such log for the purpose of determining if there is a need to implement changes to a security policy and/or procedure based upon the recorded repairs and modifications.

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

Data Classification Policy #900.12
Records Retention and Destruction Policy #100.97

APPROVAL:	
System Administrative P&P Committee	2/26/15
System PICG/Clinical Operations Committee	3/19/2015

Standardized Versioning History:

*=Policy Committee Approval; ** =PICG/Clinical Operations Committee Approval

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