North Shore–LIJ Health System, Inc.

POLICY TITLE: User Password Policy	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.10	**CATEGORY: Information Services**
System Approval Date: 10/17/13 **Site Implementation Date:**	**Effective Date: 7/14/09** **Last Revised/Reviewed: 9/13**
Prepared by: Office of the CIO-IS Policy & Procedure Committee	**Superseded Policy(s)/#:** **N/A**

GENERAL STATEMENT of PURPOSE

The purpose of this document is to provide a list of requirements for the development and use of passwords that control access to computer systems and networks to protect data. A poorly chosen password may result in the compromise of networks and confidential data.

POLICY

It is the policy of North Shore-LIJ Health System, Inc. ("Health System") that suitable passwords be used to control access to the Health System network and computing devices that access or may access the Health System network or contain or may contain certain confidential information of the Health System, including protected health information (PHI), personal identifiable information (PII) or sensitive or highly sensitive information, in order to protect the confidentiality, integrity and availability of Health System confidential data.

SCOPE

This policy applies to all members of the North Shore–LIJ Health System workforce including, but not limited to, employees, medical staff, volunteers, students, physician office staff, and other persons performing work for or at North Shore–LIJ Health System.

DEFINITIONS

Handheld Device: A small (typically less than 2 pounds) device, including tablets and iPads, for computing and communication with the Health System computer network.

Smartphone: A device that has both voice and data access (to the Health System computer network and/or the Internet).

STANDARDS

The following are minimum requirements for selecting strong passwords when connecting to the computer network and other systems and applications where the technology or functionality exists.

- Systems and applications which cannot meet these standards must use the strongest settings possible.
- All users must be assigned a Universal ID by Information Services before being allowed to access any subsequent system components. A Universal ID is a specific type of User ID that is used to gain access to the Health System Computer Network. Universal IDs have passwords that strictly comply with the password standards set forth in this document.
- Smartphone and handheld device password standards are described below in the separately defined sections.

1. Password Creation Guidelines

a. Computers

- Passwords lengths for:
  - *User* accounts shall be a minimum of six (6) characters.
  - *Privileged* accounts (such as system administrators) shall be at least eight (8) characters.
- Passwords should contain characters from at least three of the following 4 categories:
  - Lower case letter [a–z].
  - Upper case letter [A–Z].
  - Numeric [0–9].
  - Special character [! @ # $ % ^ & * ( ) _ + |~ - = \ ` { } [ ] : " ; ' < > ? , . / space].

b. Smartphones and Handheld Devices

- All Smartphones using NSLIJ email, IM or applications processing PHI must be password protected.
- For Blackberry, the password will be set by the end user during the delivery process or remotely when the IS security-policy configuration is activated. Passwords for other cellular /Smartphone devices must be set by the end user when configuring the device.
- The password must be a minimum of four (4) mixed, non-repeating characters, including one special character. Password complexity will be enforced via the IS security-policy configuration.

c. All devices

- Passwords should not contain words found in dictionaries (including foreign language dictionaries).
- Passwords should not be based on a user's personal information or information maintained within the Health System's application. (For example, user ID, Social Security numbers (SSN), names of family members, and so on, are not permitted.)
- Any unauthorized reconfiguration of a device is prohibited.

2. Password Controls

Computers

- A password expiration warning message displays for a minimum of 14 days before a password expires.
- Five (5) consecutive failed login attempts within 15 minutes result in a user's account being locked for 15 minutes.

a. Smartphones and Handheld Devices

- Entering the Blackberry password incorrectly seven (7) times in a row will erase the device and require reactivation. (After six (6) attempts, the end user should contact the Information Services Help Desk immediately to reset a password if they are unable to enter it correctly.)

b. All devices

- The end user must be sure that password and locking features are enabled on devices.
- Passwords have a lifetime not to exceed 90 days after which they must be changed.
- User accounts that have not been logged into for 90 days must be disabled.
- New passwords must be different from the previous 12 passwords.
- If an account has been locked or disabled, a Service Request must be submitted to re-enable the account.

3. Password Management

Password Management addresses proper user authentication requirements, and assigning, communicating, and resetting of passwords.

- Authentication information stored on any Health System network system shall be limited to the minimal amount required for authentication and protected against unauthorized access.
- Authentication must comprise at least one of the following methods for all users:
  - Something you know, such as a password or passphrase.
  - Something you have, such as a token device or smart card.
  - Something you are, such as a biometric.
- Passwords must be encrypted when stored on systems or transferred across networks between systems.
- The Information Services (IS) Help Desk is responsible for documenting and processing requests for password resets.
- Default passwords on new systems or applications must be changed from their initial values.

- Users requesting password resets must validate their identity (for example, by providing answers to shared secret questions and/or items of relationship information) to establish the user's authenticity. Staff members should not be asked to provide their SSN as part of the validation process.
- User identification and authentication management on all system components is as follows:
    - The administrator ID is implemented in accordance with the authorization form and with the privileges specified on the authorization form.
    - All the appropriate signatures are obtained for authorization.
- If an account or password is suspected to have been compromised, staff should immediately report the incident to the IS Help Desk and change the potentially compromised passwords.
- Users must protect the secrecy of their passwords by, for example, not sharing their passwords with anyone, whether inside or outside the Health System, committing their passwords to memory, and not writing passwords down or leaving written copies of passwords in areas visible or accessible to others.

4. New passwords

- Should only be communicated to the user, the user's manager, or in accordance with contractual obligations.
- Must be created such that they can only be used one time, in order to change the password to something known to only the user.
- Users should change newly assigned passwords as soon as possible to something known only to them.
- May only be requested by the specific user affected, or as specified in contractual agreements
- Must be provided to the authorized user in-person; however, where this is not possible, then the password must be communicated using one of the following methods:
    - Via telephone, after authenticating the user in accordance with the approved authentication method or left on his or her private telephone voice mailbox.
    - Via security envelopes using interoffice or US mail.
    - PINS or passwords which are part of a multi-factor authentication scheme, such as with a token, should not be sent in the same envelope as the token.

5. Password and Account Revocation

- Immediately revoke access for all users who have been terminated or whose role has changed whereby the user no longer requires access to those systems when performing his or her job in the Health System.
- User accounts that have been inactive for at least 90 days must be removed or disabled.

6. Exceptions

- Systems and applications that do not meet these standards must apply to the OCIO Director of Networks and Systems Security for an exception to this policy.
- Refer to 100.009 Payment Card Industry Data Security Standards (PCI DSS) IT Security Policy for the policy and procedure requirements applicable to user passwords to access the segmented, secure network where Payment Card transactions (as defined in the policy) are processed. Should there be a discrepancy between 100.009 and this policy, 100.009 takes precedence.

7. Training

Each member of the workforce shall receive training and education on the password and password management requirements of this policy when the user receives his or her Universal ID for the first time and ongoing as part of the mandatory annual Corporate Compliance training.

GUIDELINES

- An individual's password must be changeable by the user.
- All Health System passwords are to be treated as confidential information, and should not be shared with anyone, including administrative assistants. If additional staff members require access to the account, the account owner must submit a Service Request.
- Passwords should never be written down or stored online unless appropriately secured or encrypted.
- Try to create passwords that can be easily remembered. One way to do this is to create a password based on the first character in each word of a song title or other phrase. For example, if the phrase is *This may be one way to remember!* the password would be *Tmb1w2r!* or some other variation.
- Do not use the same password for Health System accounts as for other non-Health System access (such as a home e-mail account, Websites, benefits, and so on).
- Users should never use the *Remember Password* feature of applications (for example, Eudora, Outlook, browsers).

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
NS-LIJHS Help Desk	(516) (718) (631) 470-7272
NS-LIJHS Help Desk Email	servicedesk@nshs.edu
Office of Corporate Compliance Help Line	(800) 894-3226
Office of Corporate Compliance Website	www.northshore-lij.ethicspoint.com

REFERENCES to REGULATIONS and/or OTHER RELATED POLICIES

- 100.009 Payment Card Industry Data Security Standards (PCI DSS) IT Security Policy
- 900.00 Computer Use Policy
- 900.03 Cellular and Smartphone Purchase Use Policy
- Human Resources Part XII-1 Termination of Employment: Voluntary, Involuntary
- Health Insurance Portability and Accountability Act (HIPAA), 45 CFR Parts 160 and 164
- PCI Data Security Standard (PCI DSS) v2.0

CLINICAL REFERENCES

None

FORMS

None

APPROVAL:	
System P&P Committee	7/14/09; 6/14/11; 8/29/13 (Provisional); 9/26/13 (Final)
System PICG/Clinical Operations Committee	7/23/09; 6/23/11; 10/17/13

Versioning History:

7/09

6/11