North Shore–LIJ Health System, Inc.

POLICY TITLE: **Computer Use Policy**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.00	**CATEGORY : Information Services**
System Approval Date: 1/23/14 **Site Implementation Date:**	**Effective date: 11/02** **Last Revised/Reviewed: 9/13**
Prepared by: **Office of the CIO– IS Policy and Procedure Committee**	**Superseded Policy(s)/#:** **n/a**

GENERAL STATEMENT of PURPOSE

This policy establishes rules and guidelines for the use of all computing devices, including desktops, laptops, smartphones, handheld devices and any other network enabled devices, as well as the corporate network of the North Shore-Long Island Jewish Health System, Inc. ("Health System"), hospitals, clinics, and all other facilities.

POLICY

Access to Health System computer systems and networks is provided for business use. Users must adhere to all established controls and acceptable behaviors to maintain the confidentiality, integrity, and availability of the Health System network, systems, and data.

SCOPE

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

DEFINITIONS

Bring Your Own Device (BYOD): Any non-Health System device used by a workforce member that is used for business purposes. Examples include personal laptops, smartphones, or handheld devices.

Computer Network: The Computer Network is comprised of all Health System computers, data, telecommunications infrastructure, enterprise wireless network, guest wireless network, and software applications utilized by all Health System entities.

Enterprise wireless network: The private network used for business purposes by North Shore-LIJ Health System. This includes all business and health care related applications and devices. **This network uses strong encryption to protect the data.**

Guest wireless network: A public network available to any user within the confines of the Health System.

Handheld Device: A small (typically less than 2 pounds) device, including tablets and iPads, used for computing and/or communication on the Computer Network.

Personal Identifiable Information (PII): Any information which can be used to track back to an individual. PII is therefore any information which can be used to identify an individual, whether directly or indirectly. The key test of PII is whether the data reveals a clearly identifiable person. Typical examples of PII include Social Security numbers, full names, credit card information, bank account numbers, phone numbers, and addresses.

Protected Health Information (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 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
18. Any other unique identifying number, characteristic, or code

Removable Media: Removable media includes, but is not limited to, floppy disks, CD’s, Zip drives, USB drives, and other removable storage devices.

Smartphone: A device that has both voice and data access (to the Computer Network and/or the Internet).

Treatment, Payment, and Healthcare Operations (TPO): TPO is information used to perform day-to-day work functions in the Health System.

PROCEDURE/GUIDELINES

1. **Consent and Agreement**
   All members of the Health System workforce as described in the scope will be required to sign the Health System's *Confidentiality Agreement and Acknowledgement Regarding Use of Computers, E-Mail and the Internet* form. All employees provided with access to Health System Computers should be familiar and adhere to the 900.01 Internet and Other Web Services Policy and 900.11 Electronic Mail (E-Mail) Acceptable Use Policy.

   The Health System will monitor and audit any and all user activity, system access, and electronic communications on the Health Systems' Computer Network. Users should have no expectation of privacy when using the Health System's computer equipment and network.

For vendors, consultants, and non-employees who have not signed the Health System's Confidentiality Agreement and Acknowledgement form, will be required to sign/consent to:

- A business associate's agreement, or
- Sign a non-disclosure agreement, or
- Confidentiality language in a signed agreement, or
- Confidentiality language and the protection of PHI in the signed research agreement.

OCIO, working with Legal, Procurement, and the Grants Management Office will determine the appropriate level of agreement that is required based on the type of access being requested.

Use of the guest network is a privilege and users are subject to terms and conditions posted on the Wireless Network Homepage. *Refer to the 900.15 Wireless Policy.*

2. **Passwords**
   All network and application accounts must be protected with a unique user ID and password. Passwords must conform to the standards defined in the 900.10 User Password Policy.

   BYOD, Smartphones, and handheld devices must be password protected according to the standards defined in the 900.10 User Password Policy.

3. **Access Protection**
   Users must not share their user ID or password with any other persons, and must take action to protect their passwords from being discovered by other persons. Any suspected violations must be reported to the IS Help Desk immediately.

4. **Security Awareness**
   The Health System has established requirements for Security Awareness and education for those health care system workers who have access to information systems and assets. The

Health System also provides periodic security awareness messages, making use of appropriate communications methods, including the following:

- Network Sign-on Messaging, which must be acknowledged, where applicable.
- Email Security Awareness Messages.
- Health System First Day Orientation & Compliance Annual Training.
- Area-specific training programs.
- Intranet informational bulletins.

When necessary, the Health System provides special Security Alert Messages regarding developing situations, both internal and external to the Health System. Messages are communicated in the form of emails or memos and are emphasized on HealthPort's Security Portal. Security Tips, updated monthly, should be reviewed periodically and can be accessed via the home page of HealthPort.

5. **Screen Saver**

By default, all Health System computers will activate a privacy screen saver after a period of inactivity to prevent unauthorized viewing of the screen. This function is typically controlled by the IS Department and must not be disabled or modified by the User.

Screen saver inactivity times are based on an assessment by the OCIO Security Department, which includes user's responsibilities, physical location of the computer, and business operations.

6. **Device Lock**

When using a shared workstation or kiosk, users must always sign off at the completion of the session.

When leaving a private computer, users must either sign off or lock the computer by simultaneously pressing the CTRL+ALT+DEL keys and then clicking on the Lock Computer button. The Windows key+L combination may also be used to lock the computer. To unlock, press CTRL+ALT+DEL, type in your user logon password and click OK.

Authorized smartphones and handheld devices will be configured to lock after a period of inactivity.

7. **Application Inactivity Timeout**

Where applicable, applications are designed to time out or close after an appropriate period of inactivity, based upon the sensitivity of the data. While locking a computer will prevent other users from accessing the machine, it will not prevent these applications from closing according to their predefined timeouts.

By default, and where functionality exists, applications shall automatically log off after a period of inactivity. Automatic logoff times are based on an assessment of the application by the OCIO Security Department, which includes type of sensitive data involved, the physical location of the computer, and business operations. Where functionality does not exist, other appropriate administrative, physical and technical security safeguards will be implemented.

8. Virus and Malware Protection

- Virus protection software must be loaded, updated to current anti-virus signatures, and actively running pursuant to the 900.06 Anti-Virus Policy, including BYOD.
- Anti-virus functionality is controlled by the IS Department and must not be disabled or modified by the user.
- All non-standard devices must get prior approval from OCIO Security before being granted access to the network. Under no circumstances should unauthorized equipment be attached to the enterprise network (wired or wireless). *Refer to the 900.28 Procurement and Registration of Computer Equipment and Software Policy*.
- If a user suspects that his or her laptop or desktop has become infected with a virus or otherwise compromised, the user should scan his or her system using the corporate anti-virus program and immediately contact the IS Help Desk. Common symptoms of viruses include:
  - Unusual messages that appear on the screen.
  - Degraded system performance or increased frequency of system crashes.
  - Missing data.
  - Inability to access the hard drive.
  - Unexpected and excessive Web browser pop-ups.

  For help and more information, contact the IS Help Desk.

- Users must run a virus scan on all removable media devices (such as USB drives), where the technology or functionality exists, before accessing any files or programs stored on the device.
- Users who have mobile computers and/or infrequently connect their devices to the Health System Computer Network must update the virus definitions manually at least once a week. For assistance, contact the IS Help Desk.
- To avoid downloading a virus, users should not open executables or command files (files that have an .exe, .vbs, .bat or .com at the end of the filename) if they are unsure of the program's source or purpose.
- Prevention of virus infections, Denial of Service, or other types of malicious attacks is critical in ensuring the confidentially, integrity, and availability of the Health System computer network and data. Users are encouraged to be alert and should report any suspicious activity or system behavior to the IS Help Desk immediately.
- **The Health System expressly prohibits any potentially harmful computer activities, including, but not limited to, the following:**
  - Development of any form of computer virus or malicious code fragment.
  - Intentional distribution of a virus, worm, Trojan, and so on, regardless of type (nuisance, malicious, or destructive) for any reason or by any method.
  - Creation of false alarms using hoax virus messages, chain mail, or spam.
  - Downloading or installing any unlicensed or malicious software programs or hacking utilities (such as network sniffers, scanners, and password cracking programs) onto any computer that may be attached to the Health System network.
  - Intentional corruption of software programs or data to make them unusable or invalid.

- Intentional tampering with or changing software programs or data from their original form in a manner that violates their integrity and trustworthiness.
- Creation or use of *back doors* or other system workarounds which have the intent or effect of bypassing Health System security procedures or controls.
- Any unapproved or unauthorized modification or reconfiguration of applications installed by the Health System.

9. Backup of Computer Data

The IS Department is typically responsible for developing procedures to outline the safeguarding of all servers and networked storage. This includes backing up the network share drives, home drives, shared applications, and system data that reside on hardware in the computing centers (where the technology or functionality exists).

- Users should store all data on their network home drive or department shared drives only.
- Users are permitted to store and backup business related data only.
- Users are responsible for backing up data on their local PCs or laptops.
- If an IT asset is not in the custody of the IS department, it is the custodian department manager's responsibility to ensure safeguards are in place. *Refer to the 900.28 Procurement and Registration of Computer Equipment and Software Policy.*

10. Access & Modification of Computer Data

Users are prohibited from viewing or modifying any information unrelated to their work tasks, and/or job responsibilities. OCIO Security must be notified immediately if sensitive information unrelated to users' official assignments and/or job responsibilities is accessed or modified unintentionally or if intentional unauthorized access is suspected.

11. Copying of Computer Data

Users are not authorized to copy, move, or store work-related or patient-related data for any personal use or any reason not related to Health System business or operations. This applies especially to any data or content which may be considered PHI or PII, Health System intellectual property, proprietary information, or any information considered confidential in nature. Adequate security measures must be taken to ensure security of all Health System data stored on computers or media, regardless of location.

12. Storage of Computer Data

Users are not authorized to use Health System computer resources to store data or files that are not directly related to their work duties or responsibilities. Files that are deemed unauthorized or considered improper use of data storage resources may be deleted at the discretion of the Health System without notice to the user.

13. Storage of Confidential Information

The Health System has the duty to protect the confidentiality, integrity and availability of protected health information as required by law, professional ethics, and accreditation requirements.

- When not in use, PHI/PII must always be protected from unauthorized access. When left in an unattended room, such information must be appropriately secured.
- Confidential information must not be saved on local hard drives or other media except

when necessary to perform NSLIJ job duties. All saved confidential information on local hard drives or other media must have appropriate administrative, technical and physical safeguards applied. For example, encryption, security screens, screen monitors situated to prevent unauthorized viewing, and security locks where appropriate. If you have any questions or need any of these safeguards implemented such as encryption, please contact the IS Help Desk.

- When PHI/PII is being released electronically, Health System personnel must treat the protection of PHI/PII in the same manner as PHI recorded on paper, thereby restricting access to the communication only to authorized personnel and only using approved methods of transmission. (*Refer to 900.10 User Password Policy, 900.11 Electronic Mail Acceptable Use Policy, Internet and Other Web Services Usage Policy, and 900.25 Data Encryption and Integrity Policy.*)
- Internet/Cloud based storage (such as Google Drive, Dropbox, and Mozy) must not be used to store or disseminate confidential information such as PHI without proper approval processes that include IT Contracts, Office of Procurement, OCIO Security, and Research Administration when appropriate.
- Social networking sites (such as Facebook, Twitter, and Google+) must not be used to store or disseminate confidential information such as PHI for any reason and is strictly prohibited.
- PHI stored in medical equipment must be kept secure and disposed of according to established PHI disposal procedures.
- PHI/PII stored on any removable data storage media must be protected with strong encryption. Contact the IS Help Desk for assistance. (*Refer to the 900.26 Device and Media Control Policy for more information.*)
- Only USB drives with appropriate security controls and strong encryption must be used. Disposable media must be destroyed when no longer required.
- PHI/PII, or other sensitive data, is prohibited from being removed from the premises without management approval and appropriate safeguards.
- In general, access to sensitive or confidential data must be controlled and logged.

14. Special Provisions for Sharing Research Related Data

- The process and data involved in sharing confidential information, such as PII or PHI, for research purposes must not be done unless there is approval from a health system authorized IRB and may require an agreement approved by the Grants Management Office.
- The process and data involved in sharing confidential information other than PII or PHI related to a sponsored program must not begin unless it is authorized in an agreement approved by the Grants Management Office.

15. Remote Access

Remote access is available for all authorized employees, affiliated doctors, and approved third party users. The use of remote access to the Health System Computer Network is a privilege intended to assist and enhance normal business functions and is subject to all requirements of this Computer Use Policy and all other policies and procedures established by the IS Department. Access to applications is at the discretion of management and may require additional authorization. Further information regarding the use of the Health System's Remote Access capability is covered under the 900.08 User Remote Access Policy.

16. Software Configuration Changes

- Updates and Patches: Updates and patches to approved applications are made and distributed by the IS Department. In some cases, users may be prompted to accept or acknowledge a planned patch or update.
- Personal Software: Users are prohibited from loading personal software onto Health System computers without prior approval from his or her Department Manager and IS Department. Users who wish to load personal software onto Health System computers must submit a Service Request Form to the IS Help Desk.
- Freeware and Shareware: Users must not download or install any programs that are shared on the Internet or made available free of charge. Users who need to load software onto Health System computers (such as Adobe Acrobat® Reader) must submit a Service Request Form to the IS Help Desk.
- Nonstandard software used for research purposes must also be approved by Research Administration.
- Security Applications: The IS Department deploys security applications (for example, Symantec Anti-virus, BigFix) on all Health System computers. These applications may not be uninstalled or reconfigured in anyway.

17. Peer-to-Peer and File Sharing Software

The use of peer-to-peer file sharing software (such as Napster, Limewire, Morpheus, BitTorrent, Gnutella) is prohibited. This restriction extends to file sharing capabilities in all Instant Messaging Clients.

18. Software Piracy

Health System policy, as well as federal law, prohibits the unauthorized copying or distribution of copyrighted material, with the exception of the software owner's right to make a single backup copy for archival purposes. Users must comply with all applicable laws designed to protect copyrighted software and intellectual property.

- Users must not load any software on their computer for which neither they nor the Health System has a proper license.
- Users are prohibited from installing any software that has a single-user license on more than one computer.
- Users are prohibited from making unauthorized copies of Health System licensed software.
- Users are prohibited from giving, loaning or selling copies of Health System software to any other person or entity.
- Users who violate these rules may be subject to internal disciplinary action and to civil or criminal prosecution for violation of state, federal, or international law.

19. Hardware Configuration Changes

Users are prohibited from changing their computers' hardware configuration without consulting the IS Help Desk for approval and guidance regarding compatible equipment and supported technologies. Nonstandard Hardware associated with the performance of work used by research departments must also be installed and configured with the knowledge and assistance of Research Administration; contact Research Administration for support of nonstandard hardware used for research. The IS Help Desk is not responsible for the support of non-standard hardware.

When adding peripheral equipment, the following applies:

- Modems: Users will not install analog modems in their computers without prior approval from the IS Department. Modems will be configured according to security standards.
- Storage Devices: Users must receive approval from their Department Manager before attaching storage devices (such as portable hard drives) to their computers.
- Local Printers: The configuration and utilization of shared network printers must adhere to the applicable Health System policies pertaining to PHI/PII and other sensitive information.
- Users must obtain approval from his or her department manager and the IS Department before installing any non-standard hardware device on his or her computer. Examples include external DVD writers.
- Unauthorized reconfiguration of a device is prohibited.

20. Printers

Network and local printers are provided for Health System employees to perform necessary work-related functions. Although printed documents are sometimes necessary, users are encouraged to develop habits or adopt techniques that make the work environment as *paperless* as possible.

When confidential electronic information must be printed, the paper copies must be treated with an appropriate level of sensitivity, and disposed of when no longer needed in accordance with Health System policy.

21. Wireless and Guest Network

- All wireless devices used within the Health System must comply with the transmission protocols, security measures, and encryption standards approved by the IS Department.
- The Health System provides a separate wireless network for visitors and guests.

22. Physical Security

- Users must actively follow best practices to protect Health System computers from loss or theft, such as positioning the monitor so it cannot be observed by unauthorized individuals.
- Office doors should always be locked when an office is unoccupied, during both off-hours and business hours, if practical.
- Physical relocation of any Health System computer equipment except for mobile devices (e.g., laptops, Smartphones, and handheld devices) is prohibited, unless approved and performed by the IS Department.
- Users must secure computers (especially laptop computers) to a desk or other large object as required in order to prevent theft. Department managers are responsible for evaluating the need for computer locks and should contact the IS Department for purchase of

approved locking devices, as the use of an incorrect locking device may void the computer manufacturer’s warranty.

23. Device Security

The small size and portability of some computers such as laptop computers, Smartphones, and handheld devices increases the likelihood for such devices to be lost or stolen. Users must therefore take extra care to ensure that sensitive data and confidential information contained on the devices is secure.

- Only authorized end users or individuals specifically authorized by the Health System are permitted to use assigned computers, Smartphones, handheld devices.
- Prevent access to the device and protect all software programs and data with passwords.
- Encryption technology must be employed to protect stored data. An enterprise solution is provided by the Health System.
- Devices must never be left unattended in public areas, and should be stored in locked drawers or cabinets when not in use.
- When passing through an airport security screening point, do not put the device on the X-ray belt until the path through the metal detector is clear.
- Never leave a device in a vehicle overnight and keep the device out of sight during short stops.
- Users must immediately report the loss of or theft of devices to the IS Help Desk.

24. Computers in Open Areas

Users who work in public areas and have computers whose monitors may be viewed by patients or visitors (known as *open areas*) must take precautions to prevent unauthorized persons from viewing their computer screens while working. Department managers should consider measures like placement of the monitor, changing the location of desks, or installing monitor privacy screens to avoid the viewing of confidential data such as PHI/PII.

Refer to 100.009 Payment Card Industry Data Security Standards (PCI DSS) IT Security Policy for the policy and procedures related to computer use within 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**.**

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
OCIO Security Email	security2@nshs.edu
Research Administration	(516) 562-3467
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

- 900.01 Internet and Other Web Services Usage Policy
- 900.03 Cellular and Smartphone Purchase Policy
- 900.08 Remote Access Policy
- 900.10 User Password Policy
- 900.11 Electronic Mail Acceptable Use
- 900.12 Data Classification Policy
- 900.15 Wireless Policy
- 900.25 Data Encryption and Integrity Policy
- 900.26 Device and Media Control Policy
- 900.28 Procurement and Registration of Computer Equipment and Software Policy
- 100.009 Payment Card Industry Data Security Standards (PCI DSS) IT Security Policy
- Human Resources Part XII-1 Termination of Employment: Voluntary, Involuntary
- 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 (February 17, 2009)

CLINICAL REFERENCES

None

APPROVAL	
System Administrative P&P Committee	6/09; 10/09; 10/10; 1/11/11; 10/25/12 (Provisional); 11/29/12 (Final); 8/29/13 (Provisional); 12/19/13 (Final)
System PICG Committee/Clinical Operations Committee	7/09; 10/09; 10/10: 1/27/11; 12/13/12; 1/23/14

Versioning History:
03/03
07/09
09/09
10/09
10/10
01/11
10/12