North Shore – LIJ Health System, Inc.

POLICY TITLE: **Internet, Cloud, Instant Messaging and Other Web Services Usage Policy** **Previously Titled:** **Internet Usage Policy**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.01	**CATEGORY: Information Services**
System Approval Date: 4/17/14 **Site Implementation Date:**	**Effective Date: 5/09** **Last Reviewed: 10/28/10**
Prepared by: **Office of the CIO – IS Policy & Procedure Committee**	**Superseded Policy(s)/#:** **900.18 Instant Messaging Policy**

GENERAL STATEMENT OF PURPOSE

The purpose of this policy is to establish a framework around controlled access to the Internet from the Computer Network, and establish rules for appropriate behavior with the intent to protect the availability, integrity and confidentiality of data where appropriate.

For the purposes of this policy, Internet usage and other web services refers to web browsing, instant messaging, cloud storage and web collaboration via computers, bring your own device (BYOD), smartphones, and devices connected to the Computer Network.

POLICY

The North Shore-LIJ Health System ("Health System") will provide its workforce with Internet access through the Computer Network for the express purpose of performing work-related activities or research. Internet access is a privilege, and the Health System reserves the right to monitor, control, restrict or deny usage. Unauthorized use of the Internet is prohibited.

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

Bring Your Own Device (BYOD): Any non-Health System device owned 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 Wired Network: The private wired network used for business purposes by North Shore-LIJ Health System. This includes all business and health care related applications and services. Computers and other devices connect to the enterprise wired network via a cable plugged into a wall jack.

Enterprise Wireless Network: The private wireless 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 (Please refer to the Wireless *Policy (900.15)* for more information about the Enterprise Wireless Network).

Guest Wireless Network: A public network available to any user within the confines of the Health System (Please refer to the Wireless *Policy (900.15) for* more information about the Guest Wireless Network).

Handheld Device: A small (typically less than 2 pounds) device, including tablets and iPads, used for computing and/or communication on the Computer Network. This does not include smartphones.

Instant Messaging (IM): An electronic method of communicating that enables immediate correspondence between two or more users in the form of text messages. Messages are exchanged by typing them into a computer or a portable computing device with instant messaging software installed. This may require the use of external services (such as AIM, MSN, or Google).

Online Meeting: The use of WebEx, GotoMeeting, or similar services that share content amongst individuals on a call that leverages the internet for collaborative, interactive meetings. This method of collaboration may support document sharing, audio conference, chat, and video.

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

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

Users: Any workforce including but not limited to, employees, medical staff, volunteers, students, physician office staff, and other persons with Internet access through the Computer Network.

Video Conferencing: Method of communication using two-way audio and video with the ability to share presentations from one room to many. Additionally, individuals may join via an audio conference and/or through desktop video to the conference.

PROCEDURE/GUIDELINES

A. General Procedures

1. Users are responsible for all activity they conduct on the Internet, as defined by this policy.
2. Users of the enterprise wired and wireless network will be required to sign the Health System "Confidentiality Agreement and Acknowledgement Regarding Use of Computers, E-Mail and the Internet" form.

3. Guests using BYOD are only permitted on the Guest Network, and not permitted on the enterprise wired and wireless networks. Since the Guest Network is not encrypted, users should take care in the websites to which they connect and the data they send over it.
4. Individuals provided with Internet access must be familiar with and adhere to the *Computer Use Policy* (900.00), the *Electronic Mail (E-mail) Acceptable Use Policy* (900.11), and the *Anti-Virus Policy* (900.06) available on HealthPort.
5. All information obtained during the employee's work concerning the Health System, patients thereof, or employees, must be handled as specified by the *Data Classification and Handling Policy* (900.12). Information posted to Websites over the Internet becomes public domain and therefore requires caution. **Posting of *Sensitive* and *Highly Sensitive* information is prohibited.**
6. Users are responsible for complying with additional restrictions on what confidential information may be disclosed which is separately addressed in the *Use, Access and Disclosure of Protected Health Information with Valid Authorization Policy* (800.02)
7. Sending and receiving Internet traffic via wireless devices (such as BYOD, smartphones, and handheld devices) on the enterprise wireless network is also subject to this policy.

    - Users must contact the IS Help Desk to request authorization to connect their wireless device to the Enterprise wireless network and enabling Internet access via the device. See the *Computer Use Policy* (900.00) and the *Wireless Policy* (900.15) for more details.
    - The Health System provides a Guest wireless network for visitors, guests, and workforce members connecting wirelessly with a BYOD.

8. Computers are configured with anti-virus software and the latest virus definitions in compliance with Policy 900.06 Anti-Virus Policy. If your computer is performing slow or in an erratic or unexpected matter, it may be infected by a virus or malware. **DO NOT CONNECT TO THE HEALTH SYSTEM NETWORK**. In this situation, seek assistance from the IS Help Desk.

    - Users are prohibited from disabling antivirus or firewall protection. Users must be aware that copyright laws protect most content downloaded from the Internet and other laws protect trademarks and intellectual property. Users must exercise care when downloading any material from the Internet, and will be held responsible for copyright violations.

B. Internet Usage

1. Internet access is provided to users with the understanding that new technologies and Web-based services can greatly enhance business activities or improve patient care. Some Internet technologies however place significant bandwidth burdens on the Computer Network. High utilization services such as YouTube and Netflix are generally blocked due to performance impact on the network. For business related requirements for these or similar services, please contact the OCIO Director of Network and System Security for permission.
2. The Health System may, at any time, determine it is necessary to monitor User activity, filter certain Websites or URLs, or completely block access to the Internet. These monitoring, filtering, or blocking actions may be imposed across entire sections of the Computer Network, or may be focused on certain individual Users or groups of Users, at the discretion of their manager, and/or OCIO Security.
3. Reasonable personal use of the Internet may be permitted at the discretion of the employee's Manager. This includes accessing financial sites, personal research, and shopping on-line. Accessing pornographic sites and sites that promote racism, gambling, illegal activities or other inappropriate business material is strictly prohibited.
4. Technical controls shall be employed by Information Services to hard block access to Internet Websites and protocols that are deemed inappropriate for the Health System's environment. Websites that are hard blocked cannot be bypassed by the users. The following protocols and categories of Websites will be blocked.
   - Adult/Sexually Explicit Material
   - Gambling
   - Hacking
   - Illegal Drugs
   - Peer to Peer File Sharing
   - Personals and Dating
   - SPAM, Phishing and Fraud
   - Spyware
   - Tasteless and Offensive Content
   - Violence, Intolerance and Hate
5. Some Websites that are deemed inappropriate by the Health System are soft blocked instead of hard blocked. Websites that are soft blocked are initially blocked, but the user will be presented with an option to continue to view the Website for business related purposes. This usage is logged and monitored for compliance with this policy.

C. Other Web Services

1. Use of Instant Messaging (IM) for business purposes is acceptable with the following exception: under no circumstances should IM be used to communicate *Sensitive* and *Highly Sensitive* information such as PHI or PII. Encrypted email is the only permitted

method to electronically communicate *Sensitive and Highly Sensitive* information to another individual when required.

2. Internet/Cloud based storage (such as Google Drive, Dropbox, and Mozy) must not be used to store or disseminate *Sensitive* and *Highly Sensitive* information such as PHI or PII without proper approval processes that include IT Contracts, Office of Procurement, OCIO Security, and Research Administration when appropriate. Users must follow proper procedures by saving *Sensitive* and *Highly Sensitive* information on a shared drive (Please see §13, *Storage of Confidential Information* in Policy *900.00 Computer Use* for more information). Online meetings and video conferencing (such as WebEx and GotoMeeting) may be used to communicate with multiple users inside and outside of the Health System. However, the following safeguards must be taken while collaborating with others:
   - Users should not use online meetings or video conferencing where *Sensitive* and *Highly Sensitive* information such as PHI or PII is to be discussed or displayed.
   - Users must use de-identified test data if EMR or clinical systems are to be displayed or shared.
   - Users must be aware of what is viewable by participants (for example, windows open on one's shared computer screen, white boards in the background, email).
3. Peer-to-Peer file sharing software (such as Napster, Limewire, Morpheus, BitTorrent, and Gnutella) is prohibited. This restriction extends to the file sharing capabilities of all Instant Messaging Clients on computers, smartphones, and handheld devices.
4. The use of Web sites addresses that contain *Sensitive* and *Highly Sensitive* information, such as PHI or passwords, is strictly prohibited.

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
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

- 800.02 Use, Access and Disclosure of Protected Health Information with Valid Authorization
- 900.00 Computer Use Policy
- 900.11 Electronic Mail (E-Mail) Acceptable Use
- 900.12 Data Classification and Handling Policy
- 900.15 Wireless Policy
- Health Insurance Portability and Accountability Act, 45 CFR Parts 160 and 164, Final Security Rule

CLINICAL REFERENCES

None

FORMS

None

APPROVAL

Committee name	**Approval date**
System P&P Committee	5/09; 9/09; 10/10; 1/30/14
System PICG/Clinical Ops Committee	5/09; 9/09; 10/28/10; 4/17/14

Versioning History:

3/00
11/02
7/05
5/09
9/09
10/10