

North Shore–LIJ Health System, Inc.

POLICY TITLE: Cellular & Smartphone Purchase & Usage Policy Previously Titled: Blackberry/iPhone Policy	ADMINISTRATIVE POLICY AND PROCEDURE MANUAL
POLICY #: 900.03	CATEGORY: Information Services
System Approval Date: 1/23/14	Effective Date: August 12, 2008
Site Implementation Date:	Last Revised/Reviewed: 7/10
Prepared by: Office of the CIO–IS Policy & Procedure Committee	Superseded Policy(s)/#: #900.04-Mobile Communications Device Policy

GENERAL STATEMENT of PURPOSE

The purpose of this policy is to establish guidelines for purchasing and using North Shore-Long Island Jewish Health System, Inc. (“Health System”) issued or configured cellular/Smartphone devices (for example, BlackBerry, iPhone, iPad, iPod Touch, Air Cards, Android based devices, and cell phones).

The Health System does not reimburse for personal mobile communications devices or accessories or any charges incurred through usage of such devices. Individuals/end users who have been authorized and approved by the Health System for use of a Corporate Mobile Communications Device, or Individuals/end users who have been authorized to access the Health System’s network with a personal device, will be issued such devices from the corporate vendor or granted such access as per the terms of this policy. Devices must be used in accordance with State, Federal, Local and Foreign laws (i.e. No texting while driving, hands free use of phone). Cellular/Smartphone device usage is monitored and audited. Anyone found in violation of this or any Health System security policy may be subject to disciplinary action, up to and including termination.

POLICY

This policy establishes guidelines for purchasing and using Handheld Devices including cellular/Smartphone devices used on the Health System network, and other Handheld Devices, and applies to the use of all electronic communications on cellular/Smartphone devices including but not limited to e-mail, SMS video/picture, text messaging and chat function. The Health System will not provide mobile communication devices to any non-health system employees; however appropriate exceptions may be made by approved site leadership.

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

Corporate Mobile Communications Device(s): Standard pre-negotiated, approved Health System devices such as a Smartphone or Handheld Device.

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

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

Site Leadership: An Executive Director, Senior Administrator and/or Corporate Vice President equivalent.

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

PROCEDURE/GUIDELINES

Handheld Devices are proven business tools that improve communication and productivity. Corporate Mobile Communications Devices have been approved by the Health System and are issued to certain employees and/or end users based on job requirements and proper approval.

Corporate Mobile Communications Devices allow access to corporate email, email attachments, text messaging, calendar, contacts, and in some cases, applications and the Health System's Intranet. These devices provide access to Protected Health Information (PHI) and other sensitive Health System information; as such, they must be treated as an extension of the Health System's network and handled with great care and diligence. This document establishes a policy for using and securing these devices. By accepting one of these devices from the Health System, or configuring a personal device to receive Health System emails, all end users must agree to abide by Health System Security Policies and take all necessary precautions to safeguard the device and any Health System information it contains.

A. Approval Process

The approval process is routed by PeopleSoft to the appropriate Site Leadership at each facility. Procurement of iPads is by exception only and must also follow the approval process routed by PeopleSoft and approved by Site Leadership.

Applications through PeopleSoft's ePro requisitioning process are required for each end user and for each device and/or replacement device.

Standards for equipment models have been negotiated and established for all Corporate Mobile Communications Devices by Health System Telecommunications and Procurement in order to ensure the best possible cost advantage for the Health System. No exceptions to the products will be made without further approval by Site Leadership or paid for personally by the end user.

Accessories (i.e. cases, headsets, power cords, car charges, etc.) for Corporate Mobile Communications Devices, beyond what is normally supplied in the original product packaging, are the personal financial responsibility of the end user.

Only private Blackberry end user requests require Site Leadership approval as each department is charged a one-time licensing fee and the mandatory annual maintenance fee for that license. In addition, the end user must add the Blackberry Enterprise data plan to their private account to be able to access the Health System Blackberry Enterprise Server (BES). This Enterprise data will have additional costs associated with it and is charged directly to the private end user's monthly cellular bill. All other Smartphone devices do not require a license, and therefore no additional fees are incurred.

B. Purchase

1. The purchase of a basic, 16GB Smartphone device on either Verizon or AT&T is covered and considered a supported alternative to a BlackBerry.
2. End users who require more storage must pay personally for the cost difference of the greater storage.
3. End users who need to replace Smartphones early in the contract period (either due to damage or because the user wants an early upgrade) will have to pay for the device personally.
4. Exceptions to 2 and 3 are at the discretion of applicable Site Leadership.
5. Personal phones can be added to the network provided they meet current Information Services Security support guidelines.
6. Only one corporate cellular/Smartphone device will be issued to an individual. Special consideration may be given to exceptions as approved by a facility's Site Leadership via the PeopleSoft approval process. When selecting Handheld Devices, the least expensive option to fulfill the business need should be chosen.
7. All cellular devices will be returned to the NSLIJ Cellular Department unless they were fully paid for by the user. Partially paid for devices are the property of NSLIJ and will be returned to the NSLIJ Cellular Department. These devices, when returned, can be redeployed to other users.

C. Usage

- Any cellular/Smartphone device related requests, as well as creation, modification and termination of end user accounts, must be handled by System Telecommunications. All Corporate Mobile Communications Devices are considered a business tool and company property.
- The Health System reserves the right to disconnect or modify any cellular/Smartphone device service or level of access at anytime. The Health System will make every effort to secure the device remotely via Information Services (IS) security policies, through training and awareness, and written policy. However, it is the end user's responsibility to safeguard the device.
- Corporate Mobile Communications Devices that indicate no use for over thirty (30) days will have the service cancelled by System Telecommunications. Any end user having his or her service cancelled will need to submit a new request through PeopleSoft with justification for reconnection or new service.
- The authorized end user or individuals specifically authorized by the Health System are the only individuals permitted to use the device.
- Where it is determined that an employee is no longer an authorized end user due to a change in position, termination, or where an employee has failed to comply with this policy, disciplinary action may be initiated and may result in but not be limited to revocation of corporate mobile communications devices. In addition, refer to Part III-10; Human Resources Policy and Procedure regarding Resignation, Discharge, Suspension, Layoff and Death.
- Any unauthorized reconfiguration of a device is prohibited.
- The use of still and video camera features on devices is governed by regulatory and Health System policies.
- Approved Corporate Mobile Communications Devices end users must also refer to the Human Resources Electronic Communications Systems Policy and the IS Electronic Mail

Acceptable Use Policy for additional information and Health System Policy regarding the transmission of Health System data.

- 411 calling are not permitted and are monitored monthly. Toll Free, Web lookup, and Yellow Pages information services are available and should be used as an alternate method.
- All damaged, upgraded, transferred, and retired cellular/Smartphone devices must be returned to the System Telecommunications group.
- Use of SMS text messaging on Smartphones (e.g. iPhone to iPhone text messaging or any mobile phone texting function) for business purposes is acceptable with the following exception: SMS texting should not be used to communicate *Sensitive* and *Highly Sensitive* information such as PHI or PII. Encrypted email is the only permitted method to electronically communicate this information to another individual when required.
- Individual Department management shall periodically review whether the continued use of a Corporate Mobile Communications Device is consistent with an employee's on-going job responsibilities and promptly notify System Telecommunications if an employee's plan should be cancelled for any reason.

D. Travel

- International travel must be approved one week in advance by Site Leadership.
- Those employees in possession of a Corporate Mobile Communications Device are expected to use these devices for all communication, including while on Health System domestic travel. Under normal course of business, hotel phone charges will not be reimbursed. Any exceptions are at Accounts Payable's sole discretion and must be supported by business justification and documentation.

E. Billing

- Accounts Payable no longer sends monthly statements to end users. The cellular vendors send a disc and/or invoices to System Telecommunications and Telesoft (third party outside auditing firm). The invoices are electronically uploaded into PeopleSoft.

ENFORCEMENT

Users should report any violations of this policy immediately to his or her manager. If appropriate, the violation is to 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

- 900.11 Electronic Mail Acceptable Use Policy
- 900.12 Data Classification Policy
- Human Resources Part XII-3 Electronic Communication Systems
- 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

FORMS

None

APPROVAL	
System Policy & Procedure Committee	7/13/2010; 12/19/13
System PICG/Clinical Operations Committee	7/29/2010; 1/23/14

Versioning History:

8/2008