North Shore–LIJ Health System, Inc.

POLICY TITLE: **Electronic Mail** **(E-Mail) Acceptable Use**	**ADMINISTRATIVE POLICY AND PROCEDURE MANUAL**
POLICY #: 900.11	**CATEGORY: Information Services**
Site Approval Date: 1/30/14 **Site Implementation Date:**	**Effective Date: 9/08** **Last Revised/Reviewed: 10/13**
Prepared by: Office of the CIO–IS Policy and Procedure Committee	**Superseded Policy(s)/#:** **n/a**

GENERAL STATEMENT OF PURPOSE

This policy defines the authorized and appropriate use of the North Shore-LIJ Email System.

POLICY

The North Shore-Long Island Jewish Health System, Inc. ("Health System") Electronic Mail (Email) system offers users an efficient way to communicate. The exchange of data between users via Email must be protected from unauthorized access, be monitored to help prevent security breaches, and maintain confidentiality of data. Email content and use is monitored by Information Services (IS) staff members to support operational, maintenance, auditing, security and investigative activities.

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

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

Personal Identifiable Information (PII) is 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 reveal a clearly identifiable person. Typical examples of PII include: Social Security numbers, full names, credit card information, bank account numbers, phone numbers and addresses.

PROCEDURE & GUIDELINES

A. Format of Email

Messages should be constructed so information is clear and concise, and cannot be misconstrued.

- Email messages must reflect actual origination information, and should specify sender's name, title, department and contact information, including address, phone and fax numbers.
- Misrepresenting, obscuring, or suppressing a sender's identity within messages or on Email systems is prohibited.
- Email must contain an appropriate and relevant subject line.
- Subject lines must not contain identifiable *Sensitive and Highly Sensitive* information (such as PHI, PII, or employee private data).
- Emails which contain PHI in the content must be identified in the subject line with the word *PHI* or *Secure*. In the alternative, you may click on the Encrypt & Send button (located above the send button) to force encryption.
- Use care when addressing Email to a distribution list, ensuring that all members in that lis*t a*re a*ppropr*iate recipients of the Email.

B. Content of Email

The Health System Email system is for business use. However, infrequent and minimal personal use is permitted as allowed by a user's manager or supervisor, provided it does not interfere with the performance of the user's work related duties and responsibilities. Such use must be consistent with professional conduct, law enforcement guidelines and not for personal financial gain.

- Email size must not exceed 25MB (including attachments).
- Emails are to be considered an extension of the Health System and must be professional in all aspects.
- Internal Health System Email communication is routed via an internal network. This network can be used to communicate PHI or PII when necessary for the completion of job duties within the following guidelines:
  - Addresses should be confirmed before sending to ensure the Email is delivered to the appropriate recipient.
  - The minimum necessary amount of PHI or PII should be included in the Email to accomplish the intended purpose.
- Whenever possible, avoid including in an Email *Sensitive or Highly Sensitive* information such as PHI and PII except where such PHI relates specifically to treatment and then only the minimum amount of PHI required should be included. Email communication with patients or with staff members concerning patient care will be considered and treated with the same degree of privacy and confidentiality as the written medical record.
- All Email sent outside of the Health System which are used to transmit Sensitive or Highly Sensitive information must be encrypted to meet requirements of the HIPAA Security Rule (164.312(a)(1) and 164.312(e)(1).
- Sensitive and Highly Sensitive information may be sent via Email provided the sender adheres to the following guidelines.
  - Addresses should be confirmed before sending to ensure the Email is delivered to the appropriate recipient.
  - The minimum necessary amount of PHI should be included in the Email to accomplish the intended purpose.
  - The Health System provides a method for secure Email encryption. Contact the IS Helpdesk for additional information.
- All Email communication with patients or with staff concerning patient care must only be sent through the Health System's Email portal and never through internet-based Email services such as AOL, Optimum, Yahoo, Gmail, and so on.
- Requests for exceptions to these policies will be reviewed by the OCIO Security Officer who may consult with the Chief Corporate Compliance Officer or the Chief Technology Officer, to identify a secure alternative for transmission.
- In the event that an Email containing patient information may have been inadvertently delivered to the wrong recipient (for example, due to an incorrect Email address), immediate notification must be made to the local Privacy officer or the Office of Corporate Compliance.
- When sending health system Sensitive, Highly Sensitive or proprietary business data outside of the health system, the message must be sent encrypted by including the word Secure or PHI in the subject line.

C. Email Forwarding

Users should exercise caution forwarding messages.

- Never forward suspicious Email (potentially virus infected, unknown senders and recipients, etc).
- The Health System will not forward internal Email to an external address as a service.
- Incoming Email must not be auto-forwarded to an external, non Health System Email account.

D. Receiving Email

Unsolicited or unexpected Email received from outside or unknown parties should never be opened. Instead, they should be deleted immediately to prevent potentially malicious access to the Health System network.

Files downloaded from personal Email accounts or extracted from inbound messages must be scanned for viruses prior to being opened. Unscanned files could potentially contain viruses, worms or other malicious malware.

Unauthorized access, interception or disclosure of Email is prohibited.

E. Inappropriate Content

Employees are prohibited from sending Email containing the following:

- Any material, text or speech that violates Health System business use of the Email system or this policy. For more information please reference HR Policy Part 13; Section 3.
- Chain Email letters or their equivalent.
- Solicitations or private business activities.
- Public representation of the Health System issued via Email, unless granted specific approval from the Public Relations department.

F. Prohibited Usage

- Health System Email may not be used for any activities deemed unlawful, criminal or immoral, and the Health System retains the right to remove from its information systems any material it views as inappropriate, offensive or potentially illegal.
- The Health System Email must not be used for the creation or distribution of any disruptive or offensive messages, including offensive comments about race, gender, disabilities, age, sexual orientation, pornography, religious beliefs and practice, political beliefs, or national origin.
- Employees are prohibited from the intentional sending of *spam* (unsolicited electronic communications sent to multiple users not specifically requesting the information).
- Employees who receive any Email with content they feel violates these policies should report the matter to their supervisor immediately or the Information Services Helpdesk.

G. Backup Media

Email back-ups will be made in accordance with standard Health System back-up procedures.

H. Email Communication with Patients

All physicians, physician practices and/or clinicians who choose to communicate with patients through the use of Email must adhere to the following:

- All Email must conform to all previously stated policies.
- All patients must sign an *E-Mail/Electronic Communication Consent* prior to initiating Email communication.
- With the exception of appointment scheduling, Email communication is only to take place with patients previously seen and evaluated in the practice or by the clinician.
- Email communication with patients should be used only for non-emergency, non-urgent or non-critical information.
- Copies of all Email communications relative to ongoing medical care of the patient must be maintained as part of the patient's medical record. All clinically-relevant online clinician-patient Email communications must be a permanent part of the patient's medical record.
- Email communication with patients residing outside the state for which the clinician holds a license should not include diagnosis and/or treatment of patient's medical conditions (for example, reading or interpretation of specimens, slides or images; ordering tests or prescribing medications).

I. Email Communication with Staff Members

- Email communication to Quality Management or to any staff member regarding quality assurance information must contain the following footer: "*CONFIDENTIAL Education Law 6527; Public Health Law 2805, J., K., L., M.*"
- Copies of all Email communications relative to ongoing medical care of the patient must be maintained as part of the patient's medical record. All clinically relevant clinician-clinician Email communications must be a permanent part of the patient's medical record.

J. Mass Email Communication to all Health System Email Accounts

- Only authorized users are permitted to use the mailing list identified by the Internal Communications Department.
- Content of the Health System-wide Email must be relevant to the Health System community and/or business.

K. Use of Individual Mail Lists in the Global Address List

- Use of individual mailing lists is not restricted; however, the same Health System policies apply—content must be restricted to the Health System community and/or business.
- Individual mail lists are created by the Information Services Department. Requests for a new distribution list can be obtained by filling out a Service Request form which is

available on Health Port. Lists will contain a maximum of 400 users. Once lists are created they will be managed by the individual who has requested them.

L. Archiving of Email

All Email is archived in long-term storage by the IS Department, and may be monitored, reviewed and restored at the discretion of management at each facility. The Email system is intended for business purposes and all Email remains the property of the Health System. Employees and other users of Health System Email should have no expectation of privacy related to their Email accounts.

Users are able to retrieve their archive as needed. A video on "How to Archive your Email" can be found on the IS Website, under the Security Safeguards section located on HealthPort.

M. Email for Persons Not Employed by the Health System

In some instances, a Health System Email address will be provided to persons who are not directly employed by the Health System, such as independent contractors and voluntary attending physicians. The provision of such an Email address facilitates the timely and effective communications about matters such as, in the case of voluntary physicians, urgent and emerging public health issues and clinical updates that may impact patient treatment or outcomes. However, the use of a Health System Email address by a non-employee is not intended to signify that such person is an employee or agent of the Health System, and non-employees may not use their Health System Email address in a manner that implies otherwise. Use of a Health System Email address by a non-employee shall conform to all of the requirements set forth in this policy.

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

- 900.12 Data Classification Policy
- HIPAA Req's 164.312 (a) (1); 164.312 (e) (1)

- HR Policy XIII-3 Electronic Communications Systems
- HR Policy XII-1 Termination of Employment: Voluntary, Involuntary
- HR Policy V-3 Conduct in the Workplace/Progressive Discipline

CLINICAL REFERENCES
None

FORMS
None

APPROVAL

Committee	**Approval date**
System P&P Committee	9/09/08; 4/14/09; 8/10/10; Provisional approval - 1/30/14
System PICG/Clinical Ops Committee	9/25/08; 4/23/09; 9/23/10;

Versioning History:
9/08
4/09
8/10