SAINT LOUIS UNIVERSITY

USE OF ELECTRONIC MAIL CONTAINING PHI

Policy Number: OUC-053 **Version Number: 2.0**
Effective Date: 04/14/2003
Responsible University Official: Privacy Officer
Approved By: Executive Staff
Legal and Compliance Committee

1.0 INTRODUCTION

Saint Louis University (hereinafter the "University") is committed to provide services in compliance with all state and federal laws governing its operations, incorporating the highest levels of business and professional ethics. The Privacy Rule allows covered health care providers to share protected health information for treatment purposes without patient authorization, as long as they use reasonable safeguards when doing so. These treatment communications may occur orally or in writing, by phone, fax, e-mail, or otherwise. Covered entities must have in place reasonable and appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information that is disclosed using e-mail.

The Security Rule includes standards for access control, integrity, and transmission security required to restrict access to, protect the integrity of, and guard against unauthorized access to e-PHI. The standard for transmission security also includes addressable specifications for integrity controls and encryption. A covered entity must assess its use of open networks and identify the available and appropriate means to protect e-PHI as it is transmitted. The Security Rule allows for e-PHI to be sent over an electronic open network as long as it is adequately protected.

2.0 PURPOSE

The purpose of this policy is to define appropriate standards for secure and effective use of Saint Louis University's electronic mail for transmitting protected health information.

3.0 PERSONNEL AFFECTED

This policy applies to all regular full-time and part-time faculty and staff and volunteers within all divisions of the University, including employees, professional staff members, residents, agents, representatives and consultants with access to patients' protected health information.

4.0 DEFINITIONS

Protected Health Information (PHI): Any individually identifiable health information transmitted or maintained in any form or medium, including oral, written, and electronic. Individually identifiable health information relates to an individual's health status or condition, furnishing health services to an individual or paying or administering health care benefits to an individual. Information is considered PHI where there is a reasonable basis to believe the information can be used to identify an individual.

Workforce: Employees, volunteers, trainees, contractors, and other persons under the direct control of the covered entity, whether or not paid by the covered entity.

5.0 POLICY

Electronic mail is an integrated tool in the University's business processes. This policy applies to all usage of the University's electronic mail systems where the mail either originated from or is received into a University computer or network.

User Responsibilities

The user is any person who has been authorized to read, enter, or update information created or transmitted via Saint Louis University's electronic mail system.

Electronic mail is intended to be used as a business tool to facilitate communications and the exchange of information needed to perform an employee's job. Incidental personal use is permissible so long as: (a) it does not consume more than a trivial amount of resources, (b) does not interfere with worker productivity, and (c) does not preempt any business activity.

Users have an obligation to use e-mail appropriately, effectively, and efficiently.

Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed and stored by others. Therefore, users must utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.

E-mail should not be used for urgent or time-sensitive communications.

Business e-mail accounts and passwords should not be shared or revealed to anyone else besides the authorized user(s).

Prohibited Uses:

Use of electronic mail is to be in compliance with all applicable state and federal statutes and Saint Louis University's policies and procedures. Prohibited usage of University electronic mail system includes, but is not limited to:

- Copying or transmission of any document, software or other information protected by copyright and/or patent law, without proper authorization by the copyright or patent owner;
- Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.
- Use of e-mail system for solicitation of funds, political messages, gambling, commercial, or illegal activities
- Disclosure of an individual s personal information without appropriate authorization
- Transmission of information to individuals inside or outside the company without a legitimate business need for the information.
- Use of e-mail addresses for marketing purposes without explicit permission from the target recipient.
- Transmission of highly confidential or sensitive information, e.g., HIV status, mental illness, chemical dependency and workers compensation claims.
- Forwarding of e-mail from in-house or outside legal counsel, or the contents of that mail, to individuals outside of the company without the express authorization of counsel.
- Misrepresenting, obscuring, suppressing, or replacing a user s identity on an electronic communication.
- Obtaining access to the files or communications of others with no substantial company business purpose.
- Attempting unauthorized access to data or attempting to breach any security measure on any electronic communication system, or attempting to intercept any electronic communication transmissions without proper authorization.

This list is not considered all-inclusive. Further questions regarding appropriate use of electronic mail should be directed to the employee s supervisor or University Security Officer or University Privacy Officer.

Ownership and User Privacy of E-Mail

Use of electronic mail is a part of Saint Louis University's business processes. All messages originated or transported within or received into the University's electronic mail system are considered to be the property of Saint Louis University.

All users of e-mail systems do so with the understanding that they have no expectation of privacy relating to that use. Saint Louis University reserves the right to access the electronic mail system for the purpose of ensuring the protection of legitimate business interests and proper utilization of its property. Such purposes may include, but are not limited to:

- Locating and retrieving lost messages,
- Performing duties when an employee is out of the office or otherwise unavailable;

- Maintaining control of the system by analyzing message patterns and implementing revisions as needed;
- Collecting or monitoring electronic communications in order to ensure the ongoing availability and reliability of the system.
- Recovering from systems failures and other unexpected emergencies; and
- Investigating suspected breaches of security or violations of policy with probable cause;
- Electronic mail information is occasionally visible to staff and contractors engaged in routine testing, maintenance, and problem resolution. Staff and contractors assigned to perform such assignments will not intentionally seek out and read, or disclose to others, the content of e-mail.

Confidentiality of Electronic Mail

Users of University's electronic mail system may have the capacity to forward, print and circulate any message transmitted through the system. Therefore:

- Users should utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.
- When e-mail is used for communication of confidential or sensitive information, specific measures must be taken to safeguard the confidentiality of the information. These safeguards are as follows:

    - Information considered confidential or sensitive must be protected during transmission of the data utilizing encryption or some other system of access controls that ensure the information is not accessed by anyone other than the intended recipient.
    - A notation referring to the confidential or sensitive nature of the information should be made in the subject line.
    - Confidential or sensitive information may be distributed to multiple recipients; however, the use of distribution lists is prohibited.
    - Confidential or sensitive information is to be distributed only to those with a legitimate need to know.

Retention of Electronic Mail

Generally, e-mail messages constitute temporary communications, which are non-vital and may be discarded routinely. However, depending on the content of an e-mail message, it may be considered a more formal record and should be retained pursuant to University record retention schedules.

Electronic mail tape or CD back-ups are performed on a regular basis for the purpose of business recovery. Information stored electronically is subject to the legal discovery process and can be subpoenaed. To manage this risk, consider short retention periods for e-mail back-ups and execute appropriate third party retention requirements consistent with business needs.

Electronic mail tape and CD back-ups are stored for *(Retention Period).*

Provider/Patient Use of E-mail

Use of provider/patient e-mail can facilitate improved communication between an individual and his or her provider. However, due to the inherent risks involved in e-mail use, the following policy considerations must be clearly addressed prior to using e-mail for provider/patient communications.

Patient Informed Consent and Agreement to Guidelines for Use of E-mail

- E-mail communication is a convenience and not appropriate for emergencies or time-sensitive issues.
- No one can guarantee the security and privacy of e-mail messages. Employers generally have the right to access any e-mail received or sent by a person at work.
- Highly sensitive or personal information should not be communicated via e-mail.
- Communication guidelines defined, including, (1) how often e-mail will be checked, (2) instructions for when and how to escalate to phone calls and office visits, and (3) the types of transactions that are appropriate for e-mail.
- Staff other than the health care provider may read and process the mail.
- Clinically relevant messages and responses will be documented in the medical record.
- E-mail message content must include (1) the category of the communication in the subject line, i.e., prescription refill, appointment request, etc., and (2) clear patient identification including patient name, telephone number and patient identification number in the body of the message.
- Indemnify Saint Louis University for information loss due to technical failures.

Boundaries for Operational Staff Usage of Patient Electronic Mail

Considerations include:

- All employees, including health care providers, sign a confidentiality and security agreement that addresses electronic technology.
- Use of a central address for receipt of all e-mail messages.
- Identification of processes to manage triage, routing, response and filing of e-mail messages.
- Process to verify that message is from an established patient before responding.
- Reasonable precautions to ensure that e-mail responses to patients are not misdirected or otherwise become available to unintended parties.
- Use of discreet subject headers such as personal and confidential communication.

- Incorporation of all relevant e-mail messages, including the full text of the patient's query as well as the reply to the sender, in patient s electronic or paper medical record.
- Obtaining of patient's express authorization prior to any forwarding of patient-identifiable information to a third party such as a consultant or health plan.
- Prohibitions on use patient's e-mail addresses for marketing or the supplying of addresses to third parties for advertising or any other use.

Technical Security Practices

- Restriction of access to the professional e-mail account in the same way access to medical records is restricted.
- Use of password protected programs and screen-savers for all workstations.
- Firewalls
- Use of the auto-reply feature to notify patients when an e-mail account will not be monitored during a vacation or office closure.
- Protection of information considered confidential or sensitive by utilizing encryption or some other system of access controls that ensure the information is not accessed by anyone other than the intended recipient.
- Prohibition on use of unsecured wireless e-mail communication when sending patient-identifiable information.

6.0 SANCTIONS

Individuals who fail to comply with this policy and the procedures associated with it will be subject to disciplinary actions guided by the University's Staff Performance Management Policy, Faculty Manual, or Student Guidelines.

Non-compliance in this Policy can result in disciplinary action, including but not limited to, restricted incentive payments, suspension or termination. It may also result in the enforcement of a corrective action plan, as well as notification of the suspected misconduct and/or violation to government regulatory agencies.

This Policy does not limit the University's ability to impose greater sanctions or impose immediate action against serious violations. Disciplinary actions appropriate to the severity of the infraction will be carried out as needed.

9.0 CHANGES TO THIS POLICY

Changes to this policy may be necessary from time to time. At a minimum, the policy and all other program policies, procedures and guidelines will be reviewed on an annual basis.

10.0 RELATED POLICIES & DOCUMENTS

- Compliance Hotline Reporting Policy

REVISION HISTORY

EFFECTIVE DATE	VERSION NUMBER	MODIFICATION
4/14/2003	1.0	New Policy
7/01/2008	1.1	Review & Change Format
3/01/2015	1.2	Review & Change Format
	2.0	Ownership Shifted from Provost to General Counsel