Sample E-Mail Security Policy and Procedure:

SUBJECT: ELECTRONIC MAIL

ISSUED BY: Security Policies Committee

DATE ISSUED:

SUPERSEDES:

AFFECTS:

I. PURPOSE
The purpose of this policy is to define appropriate standards for secure arid effective use of <ORGANIZATION NAME> electronic mail system.

II. POLICY
Electronic mail has become an integrated tool in <ORGANIZATION NAME> business processes. This policy applies to all usage of <ORGANIZATION NAME> electronic: mail systems where the mail either originated from or is received into a <ORGANIZATION NAME> computer or network. It applies to all users including, but not limited to, employees, professional staff, contractors, students, and volunteers.

User Responsibilities

The user is any person who has been authorized to read, enter, or update information created or transmitted via <ORGANIZATION NAME> 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 <ORGANIZATION NAME> policies and procedures. Prohibited usage of <ORGANIZATION NAME> electronic mail system includes, but is not limited to:

1. 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;
2. Engaging in any communication that is threatening, defamatory, obscene, offensive, or harassing.
3. Use of e-mail system for solicitation of funds, political messages, gambling, commercial, or illegal activities
4. Disclosure of an individuals personal information without appropriate authorization
5. Transmission of information to individuals inside or outside the company without a legitimate business need for the information.
6. Use of e-mail addresses for marketing purposes without explicit permission from the target recipient.
7. Transmission of highly confidential or sensitive information, e.g., HIV status, mental illness, chemical dependency, and workers compensation claims.
8. 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.
9. Misrepresenting, obscuring, suppressing, or replacing a user s identity on an electronic communication.
10. Obtaining access to the files or communications of others with no substantial company business purpose.
11. 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 <TITLE OF THE INFORMATION SECURITY ADMINISTRATOR>.

Ownership and User Privacy of E-Mail

Use of electronic mail is a part of <ORGANIZATION NAME> business processes. All messages originated or transported within or received into <ORGANIZATION NAME> electronic mail system are considered to be the property of <ORGANIZATION NAME>.

All users of e-mail systems do so with the understanding that they have no expectation of privacy relating to that use. <ORGANIZATION NAME> 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:

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

3. Maintaining control of the system by analyzing message patterns and implementing revisions as needed;
4. Collecting or monitoring electronic communications in order to ensure the ongoing availability and reliability of the system.
5. Recovering from systems failures and other unexpected emergencies; and
6. Investigating suspected breaches of security or violations of policy with probable cause;

Electronic mail information is occasionally visible to IS staff engaged in routine testing, maintenance, and problem resolution. Staff assigned to carry out such assignments will not intentionally seek out and read, or disclose to others, the content of e-mail.

Supervisors and/or administrators must advise and receive approval from <TITLE OF THE INFORMATION SECURITY ADMINISTRATOR> of their intent to review an employees messages prior to accessing employee files.

Confidentiality of Electronic Mail

Users of <ORGANIZATION NAME> electronic mail system may have the capacity to forward, print and circulate any message transmitted through the system. Therefore:

1. Users should utilize discretion and confidentiality protections equal to or exceeding that which is applied to written documents.
2. 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:
    a. 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.
    b. A notation referring to the confidential or sensitive nature of the information should be made in the subject line.
    c. Confidential or sensitive information may be distributed to multiple recipients; however, the use of distribution lists is prohibited.
    d. 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 <ORGANIZATION NAME> record retention schedules.

Electronic mail tape 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 organizational needs.

Electronic mail tape 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.

1. Patient informed consent and agreement to guidelines for use of e-mail must be documented. Informed consent should address the following:
   A. E-mail communication is a convenience and not appropriate for emergencies or time-sensitive issues.
   B. No one can guarantee the security arid privacy of e-mail messages. Employers generally have the right to access any e-mail received or sent by a person at work.
   C. Highly sensitive or personal information should not be communicated via e-mail.
   D. 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 clinician may read and process the mail.
   E. Clinically relevant messages and responses will be documented in the medical record.
   F. 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.
   G. Indemnify <ORGANIZATION NANIE> for information loss due to technical failures.

2. Boundaries for clinical and operational staff usage of patient electronic mail must be defined. Considerations include:
   A. All employees, including physicians, sign a confidentiality and security agreement that addresses electronic technology.
   B. Use of a central address for receipt of all e-mail messages.
   C. Identification of processes to manage triage, routing, response, and filing of e-mail messages.
   D. Process to verify that message is from an established patient before responding.
   E. Reasonable precautions to ensure that e-mail responses to patients are not misdirected or otherwise become available to unintended parties.
   F. Use of discreet subject headers such as personal and confidential communication.
   G. Incorporation of all clinically relevant e-mail messages, including the full text of the patients query as well as the reply to the sender, in patients electronic or paper medical record.
   H. Obtaining of patients express authorization prior to any forwarding of patient identifiable information to a third party such as a consultant or health plan.

I. Prohibitions on use patients e-mail addresses for marketing or the supplying of addresses to third parties for advertising or any other use.

3. Technical security practices
   A. Restriction of access to the professional e-mail account in the same way access to medical records is restricted.
   B. Use of password protected programs and screen-savers for all workstations. Firewalls
   C. Use of the auto-reply feature to notify patients when an e-mail account will not be monitored during a vacation or office closure.
   D. 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.
   E. Prohibition on use of unsecured wireless e-mail communication when sending patient-identifiable information.

Compliance

Employees and users of <ORGANIZATION NAME> electronic mail system(s) who are found to be in violation of any part of this policy are subject to disciplinary action up to and including dismissal.