Effective Date: 6/28/2005
Revised Date:
Review Date:

North Sound Mental Health Administration

Section 4000 – Information Systems: Email and Internet Security

Authorizing Source:
Cancels:
See Also:
Responsible Staff: IS Specialist

Approved by: Executive Director
Motion #:

Date: 6/28/2005

POLICY #4005.00

SUBJECT: EMAIL AND INTERNET SECURITY

POLICY

A. E-Mail Security Policy

1. **Introduction**
   The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require that these policies be established, enforced, and audited. NSMHA uses these and other policies to set limits on the use of e-mail, PCs, cell phones, and telecommunications by employees.
2. **Purpose**
   This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) on personal computers and servers.
3. **Scope**
   The policies apply to NSMHA employees and contractors and covers e-mail located on NSMHA computers if these systems are under the jurisdiction and/or ownership of NSMHA.

   a. Company Property
   As a productivity enhancement tool, NSMHA encourages the business use of electronic communications (voice mail, e-mail, and fax). Electronic communications systems and all messages generated on or handled by electronic communications systems, including back-up copies, are considered to be the property of NSMHA and are not the property of users of the electronic communications services.

   b. User Separation
   These facilities must be implemented where electronic communications systems provide the ability to separate the activities of different users. For example, electronic mail systems must employ user IDs and associated passwords to isolate the communications of different users. But, fax machines that do not have separate mailboxes for different recipients need not support such user separation. All NSMHA staff and contractors have unique usernames and passwords to access the e-mail system.

   c. User Accountability

   i. Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. To do so exposes the authorized user to responsibility for actions the other party takes with the password, and it exposes NSMHA to considerable risk.

   ii. If users need to share data, they should utilize message-forwarding facilities, directories on local area network servers, and other authorized information-sharing mechanisms. To prevent unauthorized parties from obtaining access to electronic

communications, users must choose passwords that are difficult to guess - not a dictionary word, not a personal detail, and not a reflection of work activities. (Please reference the Password Protection procedure.)

d. No Default Protection

Employees are reminded that NSMHA electronic communications systems are not encrypted by default. If sensitive information must be sent by electronic communications systems, encryption or similar technologies to protect the data must be employed. See the IS Specialist if this requirement is needed.

e. Respecting Privacy Rights

i. Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. NSMHA is committed to respecting the rights of its employees, including their reasonable expectation of privacy. However, NSMHA also is responsible for servicing and protecting its electronic communications networks. To accomplish this, it is occasionally necessary to intercept or disclose, or assist in intercepting or disclosing, electronic communications.

ii. NSMHA will make all e-mail messages sent or received that contain protected health information (PHI) part of the consumer health records and will treat such e-mail messages with the same degree of confidentiality as other parts of the health record.

iii. Consumers must consent to the use of e-mail for PHI. The IS Specialist and the Privacy Officer are responsible for developing and implementing such a consent form. All e-mail concerning PHI will start with a confidentiality statement developed by the Privacy Officer.

f. No Guaranteed Message Privacy

NSMHA cannot guarantee that electronic communications will be private. Employees should be aware that electronic communications could, depending on the technology, be forwarded, intercepted, printed, and stored by others. Furthermore, others can access electronic communications in accordance with this policy.

g. Regular Message Monitoring

It is the policy of NSMHA NOT to regularly monitor the content of electronic communications. However, the content of electronic communications may be monitored to support operational, maintenance, auditing, security, and investigative activities. NSMHA retains the right to monitor messages to ensure compliance with HIPAA regulations concerning security and client privacy. Users should structure their electronic communications in recognition of the fact that NSMHA will from time to time examine the content of electronic communications.

h. Message Forwarding

Recognizing that some information is intended for specific individuals and may not be appropriate for general distribution, electronic communications users should exercise caution when forwarding messages. NSMHA sensitive information must not be forwarded to any party outside NSMHA without the prior approval of their manager.

i. Purging Electronic Messages

Messages no longer needed for business purposes must be periodically purged by users from their personal electronic message storage areas. After a certain period—generally six months— electronic messages backed up to a separate data storage media (tape, disk, CD-ROM, etc.) will be automatically deleted by IS staff. Not only will this increase scarce

storage space; it will also simplify record management and related activities. If NSMHA is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the NSMHA Coordinator or his designated representative has communicated that it is legal to do so. Note: By default, the IS/IT Department turns on the Outlook Auto-Archiving settings.

4. **Responsibilities**
   As defined below, NSMHA staff responsible for electronic mail security has been designated in order to establish a clear line of authority and responsibility.

   a. IS/IT Department must establish e-mail security policies and standards and provide technical guidance on e-mail security to all NSMHA staff.
   b. The Privacy Officer must review all such policies and procedures to ensure compliance with the agency's overall Privacy and Security Plan and to ensure compliance with applicable HIPAA regulations.
   c. IS staff must monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Managers must ensure that their staffs are in compliance with the personal computer security policy established in this document. IS staff must also provide administrative support and technical guidance to management on matters related to e-mail security.
   d. NSMHA managers must ensure that employees under their supervision implement e-mail security measures as defined in this document.

5. **Contact point**
   Questions about this policy may be directed to the IS Specialist or Privacy Officer.
6. **Enforcement**
   All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to discipline up to and including termination from employment in accordance with NSMHA's Employee Conduct and Discipline policy.

B. Internet Security Policy

1. **Introduction**
   The new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes NSMHA's official policy regarding Internet security. It applies to all users (employees, temporaries, etc.) who use the Internet with NSMHA computing or networking resources, as well as those who represent themselves as being connected, in one way or another, with NSMHA.

   All Internet users are expected to be familiar with and comply with these policies. Questions should be directed to the IS Specialist. Violations of these policies can lead to revocation of system privileges and/or disciplinary action, including termination.

2. **Purpose**
   The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of NSMHA information and equipment by internet connections.

3. Scope

This policy applies to all employees, temporaries, and other users at NSMHA. Throughout this policy, the word "worker" will be used to collectively refer to all such individuals. The policy also applies to all computer and data communication systems owned by and/or administered by NSMHA.

All information traveling over NSMHA computer networks that has not been specifically identified as the property of other parties will be treated as though it is a NSMHA corporate asset and, as such, is subject to the policies, procedures, and safeguards set forth in the agency's Privacy and Security Plan. It is the policy of NSMHA to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

In addition, it is the policy of NSMHA to protect information belonging to third parties that has been entrusted to NSMHA in confidence as well as in accordance with applicable contracts and industry standards.

A. Information Movement

i. No software can be downloaded. Request for download can be made to the IS/IT Department.
ii. All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated or inaccurate.
iii. Contacts made over the Internet should not be trusted with NSMHA information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal NSMHA information (see the following section).
iv. In more general terms, NSMHA internal information should not be placed in any location, on machines connected to NSMHA internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.
v. All publicly writable (common/public) directories on NSMHA Internet-connected computers will be reviewed and cleared on a regular basis by IS staff. This process is necessary to prevent the anonymous exchange of information inconsistent with NSMHA's business.
vi. Examples include pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material (i.e., erotica). Users are prohibited from being involved in any way with the exchange of the material described in the last sentence.

B. Information Protection

i. Wiretapping and message interception are straightforward and frequently encountered on the Internet. Accordingly, NSMHA secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by approved methods.

ii. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.

iii. Credit card numbers, telephone calling card numbers, log in passwords, and other parameters that can be used to gain access to goods or services must not be sent over the Internet in readable form. An encryption algorithm, approved by the NSMHA IS Specialist, must be used to protect these parameters as they traverse the Internet. An example would be a technology known as SSL (secure sockets layer) used to encrypt and decode information, which passes from the computer to their secure server during the ordering process. You can confirm that this is working during check-out by observing the small lock icon on your web browser; another approved area is the https sites.

iv. This policy does not apply to the process used to log in to your workstation. NSMHA uses an approved encryption mechanism that is detailed in the Privacy and Security Plan.

v. In keeping with the confidentiality agreements signed by all staff, NSMHA software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-NSMHA party for any purposes other than business purposes expressly authorized by management.

vi. Exchanges of software and/or data between NSMHA and any third party may not proceed unless a written agreement has first been signed. These agreements must conform to the Business Partner and/or Trading Partner regulations set forth in the HIPAA material, and all such agreements must be approved by the Privacy Officer.

vii. NSMHA strongly supports strict adherence to software vendors' license agreements. When at work, or when NSMHA computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.

viii. Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with NSMHA work, and are therefore prohibited. Similarly, reproduction of words posted or otherwise available over the Internet must be done only with the permission of the author/owner. Violation of this policy can lead to disciplinary action, including termination

C. No Expectation of Privacy

i. Staff using NSMHA information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, staff should not send information over the Internet if they consider it to be private.

ii. At any time and without prior notice, NSMHA reserves the right to examine e-mail, personal file directories, and other information stored on NSMHA computers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of NSMHA information systems.

D. Access Control

i. All users needing to establish a connection with NSMHA computers via the Internet must authenticate themselves at a firewall before gaining access to NSMHA's internal network. This authentication process must be done via an encrypted connection established by the IS/IT Department.
ii. Examples are handheld smart cards or user-transparent challenge/response. This will prevent intruders from guessing passwords or from replaying a password captured via a "sniffer attack" (wiretap). Designated "public" systems do not need these authentication processes because anonymous interactions are expected.
iii. Staff may not alter settings of network connections. All portable computers requiring external network connections shall have firewall in place, as established by the IS/IT Department to prevent non-NSMHA users from gaining access to NSHMA systems and information.

E. Reporting Security Problems

i. If sensitive NSMHA information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the IS Specialist and Privacy Officer must be notified immediately.
ii. If any unauthorized use of NSMHA's information systems has taken place, or is suspected of taking place, the IS Specialist and Privacy Officer must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the IS Specialist and Privacy Officer must be notified immediately.
iii. Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely, but should instead be shared on a need-to-know basis. (See Malicious Software Prevention Procedure)
iv. Users must not "test the doors" (probe) security mechanisms at either NSMHA or other Internet sites unless they have first obtained permission from the IS Specialist and Privacy Officer.

4. <u>Responsibilities</u>

As defined below, NSMHA groups and staff members responsible for Internet security have been designated in order to establish a clear line of authority and responsibility.

A. IS/IT Department must establish Internet security policies and standards and provide technical guidance on PC security to all NSMHA staff.
B. IS staff must monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Managers must ensure that their staffs are in compliance with the Internet security policy established in this document. IS staff must also provide administrative support and technical guidance to management on matters related to Internet security.

C. IS staff must periodically, and no less than semi-annually, conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.
D. IS staff must check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.
E. IS staff must check that user access controls are defined on these systems in a manner consistent with the need-to-know.
F. NSMHA information owners must see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with inhouse sensitivity classifications.
G. NSMHA managers must ensure that:

i. Employees under their supervision implement security measures as defined in this document.
ii. Employees under their supervision delete sensitive (confidential) data from their floppy disk files when the data is no longer needed or useful.
iii. Employees under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all NSMHA documents that address information security.

H. Users of NSMHA Internet connections must:

i. Know and apply the appropriate NSMHA policies and practices pertaining to Internet security.
ii. Not permit any unauthorized individual to obtain access to NSMHA Internet connections.
iii. Not use or permit the use of any unauthorized device in connection with NSMHA personal computers.
iv. Not use NSMHA Internet resources (software/hardware or data) for other than authorized company purposes.
v. Maintain exclusive control over and use of his/her password, and protect it from inadvertent disclosure to others.
vi. Select a password that bears no obvious relation to the user, the user's organizational group, or the user's work project, and that is not easy to guess.
vii. Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
viii. Report to the IS Specialist any incident that appears to compromise the security of NSMHA information resources. These include missing data, virus infestations, and unexplained transactions.
ix. Access only the data and automated functions for which he/she is authorized in the course of normal business activity.
x. Obtain IS Specialist authorization for any uploading or downloading of information to or from NSMHA multi-user information systems if this activity is outside the scope of normal business activities.

5. <u>Contact Point</u>

Questions about this policy may be directed to the IS Manager or Privacy Officer.

6. **Enforcement**

All managers are responsible for enforcing this procedure. Employees who violate this procedure are subject to discipline up to and including termination from employment in accordance with NSMHA's Employee Conduct and Discipline policy.

ATTACHMENTS

None