Effective Date: 7/1/2019
Review Date: 9/10/2024
Revised Date: 9/3/2024

# North Sound Behavioral Health Administrative Services Organization, LLC

Section 4000 - Information Systems: Email and Internet Security

Authorizing Source: HCA Contract
Approved by: Executive Director Date: 9/10/2024 Signature:

**POLICY #4005.00**

**SUBJECT: Email and Internet Security**

**POLICY**

1. **E-Mail Security Policy**

   a. **Introduction**

   The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) require that these policies be established, enforced, and audited. North Sound BH-ASO uses these and other policies to set limits on the use of e-mail, PCs, cell phones, and telecommunications by employees.

   b. **Purpose**

   This policy statement provides specific instructions on the ways to secure electronic mail (e-mail) on personal computers and servers.

   c. **Scope**

   The policies apply to North Sound BH-ASO employees and contractors and covers e-mail located on North Sound BH-ASO computers if these systems are under the jurisdiction and/or ownership of North Sound BH-ASO, and within the North Sound BH-ASO Microsoft 365 Exchange email system.

   **i. Company Property**

   As a productivity enhancement tool, North Sound BH-ASO 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 the property of North Sound BH-ASO and are not the property of users of the electronic communications services.

   **ii. 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 North Sound BH-ASO staff and contractors have unique usernames and passwords to access the e-mail system.

   **iii. User Accountability**

   a. 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 North Sound BH-ASO to considerable risk.

b. 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 containing a dictionary word or personal details, and not a reflection of work activities. (Please reference the Password Protection procedure.)

**iv. No Default Protection**

Employees are reminded that North Sound BH-ASO 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. Utilize North Sound BH-ASOs secure email and file sharing options to make sure secure communications remain secure.

**v. Respecting Privacy Rights**

a. Except as otherwise specifically provided, employees may not intercept or disclose, or assist in intercepting or disclosing, electronic communications. North Sound BH-ASO is committed to respecting the rights of its employees, including their reasonable expectation of privacy. However, North Sound BH-ASO is also 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.
b. North Sound BH-ASO will make all e-mail messages sent or received that contain electronic Protected Health Information (ePHI) 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.
c. Consumers must consent to the use of e-mail for PHI. The Security Officer and the Privacy Officer are responsible for developing and implementing such a consent form. All e-mail concerning ePHI will start with a confidentiality statement developed by the Privacy Officer.

**vi. No Guaranteed Message Privacy**

North Sound BH-ASO 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.

**vii. Regular Message Monitoring**

It is the policy of North Sound BH-ASO *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. North Sound BH-ASO retains the right to monitor messages to ensure compliance with HIPAA and State regulations concerning security and client privacy. Users should structure their electronic communications in recognition of the fact that North Sound BH-ASO will from time to time examine the content of electronic communications.

**viii. 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. North Sound BH-ASO sensitive information must not be forwarded

to any party outside North Sound BH-ASO without the prior approval of their manager. Be certain to verify all recipients when emailing or forwarding messages that contain ePHI to verify they are authorized to receive that information.

**ix. Purging Electronic Messages**

Messages no longer needed for business purposes must be periodically purged by users from their personal email storage areas to simplify record management and related activities. If North Sound BH-ASO is involved in a litigation action, all electronic messages pertaining to that litigation will not be deleted until the North Sound BH-ASO Coordinator or their designated representative has communicated that it is legal to do so. The IT Department may enable 'Legal Hold' within Microsoft 365 to retain any emails that may be required for such litigation or recover purged emails from the journal archive.

**d. Responsibilities**

As defined below, North Sound BH-ASO staff responsible for electronic mail security has been designated to establish a clear line of authority and responsibility.

**i.** The Security Officer and the IT Department must establish e-mail security policies and standards and provide technical guidance on e-mail security to all North Sound BH-ASO staff.

**ii.** 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.

**iii.** The Security Officer and IT staff will monitor compliance with personal computer security requirements, including hardware, software, and data safeguards. Managers must ensure that their staff complies with the personal computer security policy established in this document. The Security Officer and IT staff will also provide administrative support and technical guidance to management on matters related to e-mail security.

**iv.** North Sound BH-ASO managers must ensure that employees under their supervision implement e-mail security measures as defined in this document.

**e. Contact point**

Questions about this policy may be directed to the IT Manager or Security Officer.

**f. 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 North Sound BH-ASO's Employee Conduct and Discipline policy.

**2. Internet Security Policy**

**a. 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 North Sound BH-ASO's official policy regarding Internet security. It applies to all users (employees, temporary workers, etc.) who use the Internet with North Sound BH-ASO computing or networking resources, as well as those who represent themselves as being connected, in one way or another, with North Sound BH-ASO.

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

**b. Purpose**

The purpose of this policy is to establish management direction, procedures, and requirements to ensure the appropriate protection of North Sound BH-ASO information and equipment via internet connections.

**c. Scope**

This policy applies to all employees, temporary workers, and other users at North Sound BH-ASO. 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 North Sound BH-ASO.

All information traveling over North Sound BH-ASO computer networks that has not been specifically identified as the property of other parties will be treated as though it is a North Sound BH-ASO 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 North Sound BH-ASO to prohibit unauthorized access, disclosure, duplication, modification, diversion, destruction, loss, misuse, or theft of this information.

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

**i. Information Movement**

a. No software can be downloaded. All download requests must be made to the IT Department and approved by the Security Officer.
b. 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.
c. Contacts made over the Internet should not be trusted with North Sound BH-ASO information unless a due diligence process has first been performed. This due diligence process applies to the release of any internal North Sound BH-ASO information (see the following section).
d. In more general terms, North Sound BH-ASO internal information should not be placed in any location, on machines connected to North Sound BH-ASO internal networks, or on the Internet, unless the persons who have access to that location have a legitimate need-to-know.
e. All publicly writable (common/public) directories on North Sound BH-ASO Internet-connected computers will be reviewed and cleared on a regular basis by IT staff. This process is necessary to prevent the anonymous exchange of information inconsistent with North Sound BH-ASO's business.
f. 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.

**ii. Information Protection**

a. Wiretapping and message interception are straightforward and frequently encountered on the Internet. Accordingly, North Sound BH-ASO secret, proprietary, or private information must not be sent over the Internet unless it has first been encrypted by current NIST and FIPS approved methods.

b. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet.
c. 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 North Sound BH-ASO Security Officer, must be used to protect these parameters as they traverse the Internet. An example would be a technology known as TLS (transport layer security) 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 indication is the https in the website URL.
d. This policy does not apply to the process used to log in to your workstation. North Sound BH-ASO uses an approved encryption mechanism that is detailed in the Privacy and Security Plan.
e. In keeping with the confidentiality agreements signed by all staff, North Sound BH-ASO software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-North Sound BH-ASO party for any purposes other than business purposes expressly authorized by management.
f. Exchanges of software and/or data between North Sound BH-ASO 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.
g. North Sound BH-ASO strongly supports strict adherence to software vendors' license agreements. When at work, or when North Sound BH-ASO computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden.
h. Likewise, off-hours participation in pirate software bulletin boards and similar activities represents a conflict of interest with North Sound BH-ASO 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.

**iii. No Expectation of Privacy**

a. Staff using North Sound BH-ASO 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.
b. At any time and without prior notice, North Sound BH-ASO reserves the right to examine e-mail, personal file directories, and other information stored on North Sound BH-ASO staff computers and servers. This examination assures compliance with internal policies, supports the performance of internal investigations, and assists with the management of North Sound BH-ASO information systems.

**iv. Access Control**

a. All users needing to establish a connection with North Sound BH-ASO computers via the Internet must authenticate themselves at a firewall before gaining access to North Sound BH-ASO's internal network. This authentication process must be done via an encrypted connection established by the IT Department and approved by the Security Officer.

b. 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.
c. Staff may not alter the settings of network connections. All portable computers requiring external network connections shall have client firewalls in place, as established by the IT Department to prevent non-North Sound BH-ASO users from gaining access to BH-ASO systems and information.

**v. Reporting Security Problems**

a. If sensitive North Sound BH-ASO information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Security Officer and Privacy Officer must be notified immediately.
b. If any unauthorized use of North Sound BH-ASO's information systems have taken place, or is suspected of taking place, the Security Officer 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 Security Officer and Privacy Officer must be notified immediately.
c. 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).
d. Users must not "test the doors" (probe) security mechanisms at either North Sound BH-ASO or other Internet sites unless they have first obtained permission from the Security Officer and Privacy Officer.

**d. <u>Responsibilities</u>**

As defined below, North Sound BH-ASO groups and staff members responsible for Internet security have been designated to establish a clear line of authority and responsibility.

i. The Security Officer and the IT Department must establish Internet security policies and standards and provide technical guidance on PC security to all North Sound BH-ASO staff.
ii. The Security Officer and the IT staff must monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Managers must ensure that their staff follows the Internet security policy established in this document. IT staff must also provide administrative support and technical guidance to management on matters related to Internet security.
iii. The Security Officer and IT 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.
iv. IT staff must check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.
v. IT staff must verify user access controls are defined on these systems in a manner consistent with need-to-know.
vi. North Sound BH-ASO information owners must see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in-house, regulatory and contractual sensitivity classifications.
vii. North Sound BH-ASO managers must ensure that:

a. Employees under their supervision implement security measures as defined in this document.
b. Employees under their supervision delete sensitive (confidential) data from their disk files when the data is no longer needed or useful.
c. Employees under their supervision who are authorized to use personal computers are aware of and comply with the policies and procedures outlined in all North Sound BH-ASO documents that address information security.

viii. Users of North Sound BH-ASO Internet connections must:

a. Know and apply the appropriate North Sound BH-ASO policies and practices pertaining to Internet security.
b. Not permit any unauthorized individual to obtain access to North Sound BH-ASO Internet connections.
c. Not use or permit the use of any unauthorized device in connection with North Sound BH-ASO personal computers.
d. Not use North Sound BH-ASO Internet resources (software/hardware or data) for other than authorized company purposes.
e. Ensure that data under his/her control and/or direction is properly safeguarded according to its level of sensitivity.
f. Report to the Security Officer any incident that appears to compromise the security of North Sound BH-ASO information resources. These include missing data, virus infestations, and unexplained transactions.
g. Access only the data and automated functions for which they are authorized during normal business activity.
h. Obtain Security Officer authorization for any uploading or downloading of information to or from North Sound BH-ASO multi-user information systems if this activity is outside the scope of normal business activities.

**e. Contact Point**

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

**Automatically Forwarded Email**

North Sound BH-ASO employees must exercise utmost caution when sending any email messages from the internal North Sound BH-ASO network to an outside network. To prevent inadvertent transmission of sensitive information, users shall not configure their email client to automatically forward email messages. Any email that contains sensitive information and must be sent from the internal North Sound BH-ASO network to an outside network, shall be encrypted.

**Enforcement**

All managers are responsible for enforcing this policy and procedures. Employees who violate this policy are subject to discipline up to and including termination from employment in accordance with North Sound BH-ASO's Employee Conduct and Discipline policy.

**ATTACHMENTS**

None