

Effective Date: 7/1/2019

Review Date: 10/8/2024

Revised Date: 9/17/2024

## **North Sound Behavioral Health Administrative Services Organization, LLC**

Section 4000 - Information Systems: Privacy and Security Plan

Authorizing Source: HCA Contract

Approved by: Executive Director

Date: 10/8/2024

Signature:

### **POLICY #4009.00**

#### **SUBJECT: PRIVACY AND SECURITY PLAN**

#### **BACKGROUND**

The use of computers and computer networks has become an integral part of the behavioral health and human services industry. These technologies will continue to bring enormous advantages to our industry and will continue to enable us to innovate in the means of delivering services to individuals. These technologies have also brought significant risks regarding individual confidentiality and privacy. Many organizations have opted to establish security and privacy policies that give specific guidelines on an employee's use of these technologies, in all locations. The requirements of the Health Insurance Portability and Accountability Act of 1996 (HIPAA), HCA/MCO Contracts, and the Washington State OCIO require that such policies be established, enforced, and audited.

#### **POLICY**

It is the policy of North Sound Behavioral Health Administrative Services Organization (North Sound BH-ASO) that all employees must preserve the Confidentiality, Integrity and Availability (CIA) of Protected Health Information (PHI), HCA data, PII, and other sensitive information. The purpose of this policy is to ensure that North Sound BH-ASO employees have the necessary information to carry out their responsibilities while protecting confidential information. To that end, North Sound BH-ASO employees will:

1. Collect and use PHI only for the purposes of supporting the delivery, payment, integrity, and quality of mental health services. North Sound BH-ASO employees and agents will not use or supply protected health information for non-health care uses, such as direct marketing, employment, or credit evaluation processes.
2. Collect and use individual health information only:
  - a. As a basis for required reporting of health information.
  - b. To receive reimbursement for services provided.
  - c. For research and similar purposes designed to improve the quality and to reduce the cost of health care.
3. Recognize that protected health information collected about individuals must be accurate, timely, complete, and available when needed. North Sound BH-ASO employees will:
  - a. Use their best efforts to ensure the accuracy, timeliness, and completeness of data to ensure that authorized personnel can access it when needed.
  - b. Maintain records for the retention periods required by law and professional standards.
  - c. Implement reasonable measures to protect the integrity of all data maintained about individuals.

- d. Recognize that individuals have a right of privacy. North Sound BH-ASO employees will always respect individuals' individual dignity. North Sound BH-ASO employees will respect individuals' privacy to the extent consistent with providing the highest quality health care possible and with the efficient administration of the facility.
4. Act as responsible information stewards and treat all individual data and related financial, demographic, and lifestyle information as sensitive and confidential. Consequently, North Sound BH-ASO employees will:
    - a. Treat all individual data as confidential in accordance with professional ethics and legal requirements.
    - b. Not divulge protected health information unless the individual (or his or her personal representative) has properly authorized the disclosure or the disclosure is otherwise authorized by law.
    - c. When releasing protected health information, take appropriate steps to prevent unauthorized re-disclosures, such as specifying that the recipient may not further disclose the information without individual authorization or as allowed by law.
    - d. Implement reasonable measures to protect the confidentiality of information maintained about individuals.
    - e. Remove individual identifiers when appropriate, such as in statistical reporting and in research studies.
    - f. Not disclose financial or other individual information except as necessary for billing or authorized purposes as authorized by law and professional standards.
  5. Recognize that mental health information is particularly sensitive, as is HIV/AIDS information, developmental disability information, alcohol and drug abuse information, and other information about sexually transmitted or communicable diseases and that disclosure of such information could severely harm individuals, such as by causing loss of employment opportunities and insurance coverage, as well as the pain of social stigma. Consequently, North Sound BH-ASO employees will treat such information with additional confidentiality protections as required by law, professional ethics, and accreditation requirements.
  6. North Sound BH-ASO and all its employees must adhere to this policy. North Sound BH-ASO will not tolerate violations of this policy. Violation of this policy is grounds for disciplinary action, up to and including termination of employment and criminal or professional sanctions in accordance with North Sound BH-ASO clinical information sanction policy and personnel rules and regulations.
    - a. **Reporting Security Problems**
      - i. If sensitive North Sound BH-ASO information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, Privacy and Security Officers must be notified immediately.
      - ii. 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.
    - b. **Additional Responsibilities**

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

- i. The IT Department will establish an Internet security infrastructure consisting of hardware, software, policies, and standards, and department staff will provide technical guidance on PC security to all North Sound BH-ASO staff. The Security Officer with the IT Department will respond to virus infestations, hacker intrusions, and similar events.
- ii. The security Officer and IT staff will monitor compliance with Internet security requirements, including hardware, software, and data safeguards. Program directors must ensure that their staff follows the Internet 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 Internet security.
- iii. The Security Officer and the IT staff will periodically, and no less than annually, conduct a risk assessment of each production information system they are responsible for to determine both risks and vulnerabilities.
- iv. IT staff will check that appropriate security measures are implemented on these systems in a manner consistent with the level of information sensitivity.
- v. IT staff will check that user access controls are defined on these systems in a manner consistent with the need-to-know.
- vi. North Sound BH-ASO information owners will see to it that the sensitivity of data is defined and designated on these systems in a manner consistent with in house sensitivity classifications.
- vii. North Sound BH-ASO managers will 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 disks 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.
  - d. Employees and contract personnel under their supervision complete the pre-exit clearance process upon their official termination of employment or contractual agreement.
- 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. Maintain exclusive control over and use of their password and protect it from inadvertent disclosure to others.
  - f. 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. (See Access Codes and Password policy)
  - g. Ensure that data under their control and/or direction is properly safeguarded according to its level of sensitivity.

- h. 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.
- i. Access only the data and automated functions for which they are authorized during normal business activity.

**c. Contact Point**

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

**d. Disciplinary Process**

Violation of these policies may subject employees or contractors to disciplinary procedures up to and including termination.

**ATTACHMENTS**

None