Effective Date: 1/7/2020
Review Date: 1/7/2020
Revised Date:

North Sound Behavioral Health Administrative Services Organization, LLC

Section 4000 - Information Systems: Data Use, Security and Confidentiality

Authorizing Source:
Approved by: Executive Director Date: 01/07/2020 Signature:

POLICY # 4025.00

SUBJECT: DATA USE, SECURITY AND CONFIDENTIALITY

POLICY

North Sound Behavioral Health Administrative (North Sound BH-ASO) and its subcontractors will apply special control and handling outlined in the Office of the Chief Information Officer (OCIO) 141.10 requirements to all confidential data granted to North Sound BH-ASO to fulfill its contracted requirements. It is North Sound BH-ASO's policy to apply *Least Privilege* access controls to its employees and subcontractors insuring everyone who is granted access to ePHI (electronic Protected Health Information) and Health Care Authority (HCA) data is granted access to the minimum amount necessary to accomplish their assigned tasks. North Sound BH-ASO will release HCA data to Programmers, Database Administrators (DBAs), data analysts, Subject Matter Experts (SMEs), support staff and any *individual* stakeholders who have a specific *"need to know"* based on their job role. North Sound BH-ASO Health Insurance Portability and Accountability Act (HIPAA) security and sanction Policies and related procedures govern the use of information disclosed to its employees and subcontractors. Employees who violate these procedures are subject to discipline up to and including termination from employment in accordance with North Sound BH-ASO Policy 3502.00 *Employee Conduct and Discipline.*

PROCEDURES

Data Classification

HCA classifies data into categories based on the sensitivity of the data pursuant to Office of the Chief Information Officer (OCIO) standards. Category 4 Data is information that is specifically protected from disclosure and for which:

1. especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
2. serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

Constraints on Use of Data

North Sound BH-ASO will not release or use HCA data for its own discretionary use. North Sound BH-ASO and its subcontractors must use any HCA data received or accessed under contract to carry out the purpose of that contract only. North Sound BH-ASO or its subcontractors will not conduct any ad hoc analyses, or any other use or reporting of the data without HCA's prior written consent. North Sound BH-ASO or its delegate subcontractors will not disclose any HCA data in any unauthorized fashion, or that is contrary to its contract requirements with the HCA.

SECURITY OF DATA

Data Protection

North Sound BH-ASO will protect and maintain all confidential information received from HCA, that is defined as confidential under state or federal law or regulation, or data that HCA has identified as confidential, against

unauthorized use, access, disclosure, modification or loss. This duty requires North Sound BH-ASO to employ reasonable security measures, which include restricting access to the confidential information by:

1. allowing access only to staff that have an authorized business requirement to view the confidential information.
2. physically securing any computers, documents, or other media containing the confidential information.

Data Security Standards
North Sound BH-ASO will comply with and enforce the data security requirements within this policy and the Washington OCIO Security Standard, 141.10, which will include any successor, amended, or replacement regulation (https://ocio.wa.gov/policies/141-securing-information-technologyassets/14110-securing-information-technology-assets).

Transmitting Data
When transmitting data electronically, including via email, the data will be encrypted using National Institute of Standards and Technology (NIST) 800-series approved algorithms (https://csrc.nist.gov/publications/sp). This includes transmission over the public internet. All North Sound BH-ASO electronic data *"in motion"* is required to be transmitted securely by one of our following available services:

1. Secure email via Office 365 Secured Email;
2. Cisco IronPort Registered Envelope Service (RES);
3. Our self-hosted Transport Layer Security (TLS) based secure Managed File Transfer (MFT); or
4. Secure Shell (SSH) file transfer to / from our (or our subcontractors) self-hosted on premise secure File Transfer Protocol (SFTP) servers

When transmitting Protected Health Information (PHI), Personally Identifiable Information (PII) or HCA data via paper documents outside of the building, North Sound BH-ASO employees will follow our internal PHI control and check out procedures.

Protection of Data
All North Sound BH-ASO electronic PHI (ePHI), PII or HCA data *"at rest"* is required to be stored and transported securely by:

1. encrypting client endpoints and servers using NIST 800-series approved algorithms (AES-128 bit or higher); with
2. encryption keys that are stored and encrypted independently of the data; with
3. access to the data available to authorized users using Access Control Lists (ACL), a unique user ID and a hardened password, including biometric authentication (iPhones); and
4. the use of key cards to provide access to physical locations accessible only to authorized personnel, with additional internal access controlled using combination locks; and
5. authorized HCA data allowed to be stored on portable/removable Media is encrypted with NIST 800-series approved algorithms (AES-128bit or higher), with encryption keys stored and protected independently of the data, also using NIST 800-series approved algorithms managed by North Sound BH-ASO Information System/Information Technology (IS/IT) staff; by
6. storing the encrypted removable storage devices in locked storage when not in use; and

7. using a check-in/check-out procedure to update and maintain inventory of devices when said devices are issued to authorized end users; by
8. ensuring that when being transported outside of a secured area, all issued storage devices containing confidential ePHI, PII or HCA data are always under the physical control of that authorized user.

Paper Documents
Any paper records containing confidential ePHI, PII or HCA information will be protected by storing the records in a locked file cabinet accessible to authorized personnel, located in a secured area accessible only to authorized personnel using their assigned access security badges.

Data Segregation
All confidential ePHI, PII or HCA data received and stored by North Sound BH-ASO is kept physically or logically segregated from other data. When physical or logical storage of HCA data is not possible, North Sound BH-ASO stores HCA data in a form distinguishable from other data by unique ID, directory structure, or independent file share to guarantee HCA data can be uniquely identified for return or secure destruction, or to determine if HCA data has or may have been compromised in the event of a security breach.

HCA data will be stored in one of the following ways:

1. on secured media (e.g. hard disk, flash drive.) which contains only HCA data; or
2. in a logical container on electronic media, such as a partition or folder dedicated to HCA's data; or
3. in a database that contains only HCA data; or
4. within a shared database – HCA data will be distinguishable from non-HCA data by the value of a specific field or fields (globally unique primary key(s)) within database records; or
5. physically segregated from non-HCA Data in a drawer, folder, safe, or other container when stored as physical paper documents.

When it is not feasible or practical to segregate HCA's data from non-HCA data, North Sound BH-ASO ensures HCA's data and all commingled non-HCA data is protected by HCA security standards.

Data Disposition
At the end of the contract term, or when no longer needed, all HCA confidential information and/or data will be returned to HCA or disposed of, except as required to be maintained for compliance or accounting purposes. HCA data to be destroyed will be destroyed using standards outlined in NIST 800-88 (http://csrc.nist.gov/publications/). For data stored on network disks, HCA data will be deleted by North Sound BH-ASO. If the disks containing HCA confidential data will not remain in a controlled and secured environment at North Sound BH-ASO, HCA confidential data will be securely sanitized (wiped) using North Sound BH-ASO secure media wiping procedures. If the media disks (hard drives or flash drives) are retired, replaced, or otherwise taken out of service and are removed from a North Sound BH-ASO secured area, they will be either:

1. three-pass secure wiped (sanitized) using a Department of Defense (DoD) 5220.22-M certified secure wiping utility if the media was previously encrypted with NIST compliant encryption algorithms; or
2. seven-pass wiped (sanitized) using a DoD 5220.22-M certified secure wiping utility if the media was previously unencrypted; or
3. physically signed over to and destroyed by a HIPAA compliant secure file / media shredding service that provides a signed *transfer and attestation of destruction* document.

North Sound BH-ASO maintains media sanitation logs and signed media destruction and attestation documentation in our records. Secure recycled physical media is marked as either donated or destroyed within the asset inventory

DATA CONFIDENTIALITY AND NON-DISCLOSURE

Data Confidentiality

North Sound BH-ASO does not use, publish, transfer, sell or otherwise disclose any confidential ePHI, PII or HCA information gained for any purpose not directly connected with our HCA contract, except for:

1. as provided by law; or
2. with the prior written consent of the person or personal representative of the person who is the subject of the confidential information.

Non-Disclosure of Data

North Sound BH-ASO ensures that all employees or subcontractors who have access to confidential PHI, PII, or HCA data (including employees and IT support staff) are instructed and aware of the use, restrictions and protection requirements of HCA before gaining access to HCA data. North Sound BH-ASO ensures that any new employee is made aware of the use restrictions and protection requirements before they are granted access to the data. North Sound BH-ASO ensures that each employee or subcontractor who will access HCA confidential data signs a non-disclosure of confidential information agreement to fulfill confidentiality and nondisclosure contract requirements.

North Sound BH-ASO retains the signed copy of employee non-disclosure agreement in each employee's personnel file for a minimum of six (6) years from the date the employee's access to the data ends. North Sound BH-ASO will make this documentation available to HCA upon request.

Penalties for Unauthorized Disclosure of Data

North Sound BH-ASO complies with all applicable federal and state laws and regulations concerning collection, use, and disclosure of PII and PHI. Violation of these laws may result in criminal or civil penalties or fines. North Sound BH-ASO and its subcontractors accept full responsibility and liability for any noncompliance with applicable laws, the HCA contract, its employees, and its subcontractors.

Data Shared with Subcontractors

If North Sound BH-ASO provides HCA data access to a subcontractor under this contract, North Sound BH-ASO will include all the data security terms, conditions and requirements set forth by HCA in any such subcontract. However, no subcontract will terminate the North Sound BH-ASO's legal responsibility to HCA for any work performed under contract nor for oversight of any functions and/or responsibilities North Sound BH-ASO delegates to any subcontractor.

Data Breach Notification

Any Breach or potential compromise of HCA Data will be reported to the HCA Privacy Officer at PrivacyOfficer@hca.wa.gov and to the HCA BH-ASO Contract Manager at hcabhaso@hca.wa.gov within five (5) business days of discovery. If North Sound BH-ASO does not have full details, we will report what information we have available and provide full details within fifteen (15) business days of discovery.

To the extent possible, these reports will include:

1. the identification of any Individual whose PHI has been or may have been improperly accessed, acquired, used, or disclosed;

2. the nature of the unauthorized use or disclosure, including a brief description of what happened, the date of the event(s), and the date of discovery;
3. a description of the types of PHI involved;
4. the investigative and remedial actions North Sound BH-ASO or our subcontractor took, or will take, to prevent and mitigate the harmful effects and protect against recurrence;
5. any details necessary for a determination of the potential harm to Individuals whose PHI is believed to have been used or disclosed and the steps those individuals should take to protect themselves; and
6. any other information HCA reasonably requests.

North Sound BH-ASO will immediately take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or HCA, including but not limited to:

1. 45 Code of Federal Regulation (CFR) Part 164, Subpart D;
2. Revised Code of Washington (RCW) 42.56.590;
3. RCW 19.255.010; or
4. Washington Administrative Code (WAC) 284-04-625.

North Sound BH-ASO will notify HCA in writing within two (2) business days of determining notification must be sent to non-Medicaid Individuals. At HCA's request North Sound BH-ASO will:

1. provide draft Individual notification to HCA at least five (5) business days prior to notification and allow HCA an opportunity to review and comment on the notifications.
2. coordinate its investigation and notifications with HCA and OIC as applicable.

HIPAA Compliance

North Sound BH-ASO will perform all its duties, activities, and tasks under the HCA contract in compliance with HIPAA, the HIPAA Rules and the Health and the Office for Civil Rights (OCR) as applicable. North Sound BH-ASO and its subcontractors will fully cooperate with HCA efforts to implement HIPAA requirements. Within ten business days, North Sound BH-ASO will notify the HCA Privacy Officer at PrivacyOfficer@hca.wa.gov, with a copy to the HCA BH-ASO Contract Manager at hcabhaso@hca.wa.gov , of any complaint, enforcement, or compliance action initiated by OCR based on an allegation of violation of HIPAA or the HIPAA Rule, and will notify HCA of the outcome of that action.

North Sound BH-ASO will accept all responsibility for any penalties, fines, or sanctions imposed for violations of HIPAA or the HIPAA Rules, and for any sanction imposed against its Subcontractors or agents for which it is found liable.

Inspection

North sound BH-ASO understands that HCA reserves the right to monitor, audit, or investigate the use of PII and PHI of individuals collected, used, or acquired by north Sound BH-ASO during the terms of the HCA contract. All HCA representatives conducting onsite audits of North Sound BH-ASO must agree to keep confidential any patient-identifiable information which may be reviewed during any site visit or audit.

Material Breach

North Sound BH-ASO will indemnify and hold HCA and its employees harmless from any damages related to the North Sound BH-ASO or its subcontractor's unauthorized use or release of PII or PHI of Individuals.

REFERENCES

Securing IT Assets Standards No. 141.10 (https://ocio.wa.gov/policies/)

ATTACHMENTS
None