Salish Behavioral Health Administrative Services Organization

Policy Name: DATA USE, SECURITY AND CONFIDENTIALITY

Policy Number: IS601

Effective Date: 01/01/2020

Revision Dates:

Reviewed Date: 4/08/2019; 9/25/2020

Executive Board Approval Dates: 5/17/2019; 11/1/2019

PURPOSE

To address the security, privacy and confidentiality of our data and protect it from unauthorized access.

POLICY

Salish Behavioral Health Administrative Services Organization (SBH-ASO) and its subcontractors will meet the Data Use, Security and Confidentiality requirements as set out in Exhibit O of the HCA BH-ASO Contract.

PROCEDURE

Data Classification

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

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

Constraints on Use of Data

SBH-ASO will not release or use HCA data for its own discretionary use. SBH-ASO and its subcontractors must use any HCA data received or accessed under contract to carry out the purpose of that HCA BH-ASO contract only. SBH-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. SBH-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

SBH-ASO and its subcontractors 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 SBH-ASO and its subcontractors 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

SBH-ASO and its subcontractors 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 NIST 800-series approved algorithms (http://csrc.nist.gov/publications/PubsSPs.html). This includes transmission over the public internet. All SBH-ASO electronic data *"in motion"* is required to be transmitted securely by one of its following available services:

(1) secure email via Barracuda,
(2) SSH file transfer to / from SBH-ASO (or subcontractors) SFTP server hosted by WATech (sft.wa.gov).

When transmitting PHI, PII or HCA OCIO Category 4 Data via paper documents outside of the building, SBH-ASO employees will follow applicable PHI control and check out procedures.

Protection of Data
All SBH-ASO electronic ePHI, PII or HCA OCIO Category 4 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)
(2) encryption keys that are stored and encrypted independently of the data
(3) the use of Key Cards to provide access to Physical locations accessible only to authorized personnel
(4) authorized HCA OCIO Category 4 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 Kitsap County IS staff; by
(5) storing the encrypted removable storage devices in locked storage when not in use; and
(6) using check-in/check-out procedures to update and maintain inventory of devices when said devices are issued to authorized end users; by
(7) ensuring that when being transported outside of a Secured Area, all issued storage devices containing confidential ePHI, personally identifiable information (PII) or HCA OCIO Category 4 data are always under the physical control of that authorized user.

Paper Documents
Any paper records containing Confidential ePHI, PII or HCA/OCIO Category 4 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 assigned security badges.

Data Segregation
All confidential ePHI, PII or HCA/OCIO Category 4 data received and stored by SBH-ASO is kept physically or logically segregated from other data. When physical or logical storage of HCA data is not possible, SBH-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 determining if HCA data has or may have been compromised in the event of a security breach.

HCA's 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, 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, SBH-ASO stores HCA's data and all commingled non-HCA data is protected by the HCA security standards.

Data Disposition

At the end of the contract term, or when no longer needed, all Confidential HCA 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 SBH-ASO. If the disks containing HCA confidential data will not remain in a controlled and secured environment at SBH-ASO, SBH-ASO will ensure that HCA confidential data will be securely sanitized (wiped) using Kitsap County IS 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 SBH-ASO secured area, they will be either:

(1) three-pass secure wiped (sanitized) using a 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* documentation.

SBH-ASO maintains media sanitation logs and signed media destruction and attestation documentation in our records for a minimum of ten years. Secure recycled physical media is marked as either donated or destroyed within Kitsap County IT asset inventory.

DATA CONFIDENTIALITY AND NON-DISCLOSURE

Data Confidentiality

SBH-ASO and its subcontractors do not use, publish, transfer, sell or otherwise disclose any PHI, PII or HCA/OCIO confidential 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

SBH-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. SBH-ASO ensures that any new employee or its subcontractor is made aware of the use restrictions and protection requirements before they are granted access to the data. SBH-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.

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

Penalties for Unauthorized Disclosure of Data
SBH-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. SBH-ASO and its subcontractors accept full responsibility and liability for any noncompliance with applicable laws, or the HCA contract, its employees, and its subcontractors.

Data Shared with Subcontractors
If SBH-ASO provides HCA data access to a Subcontractor under this Contract, SBH-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 SBH-ASO's legal responsibility to HCA for any work performed under contract nor for oversight of any functions and/or responsibilities SBH-ASO delegates to any subcontractor.