Scope

The Spokane County Community Services, Housing, and Community Development Department (CSHCD), including:

- Spokane County Regional Behavioral Health (Administrative Services Organization) Division (SCRBH)
- Developmental Disabilities Division (DD)
- Network providers

1. Policy

1.1. The CSHCD and its Subcontractors shall protect all Protected Health Information (PHI) under CSHCD care using the following procedures.

1.2. The CSHCD SCRBH can share PHI as described in the following policies:

1.2.1. MIS – 23 Sharing Consumer Data; and

1.2.2. MIS – 24 Oaths of Confidentiality.

1.3. Device and Media Controls – Disposal and Re-use

1.3.1. All electronic media – such as fixed and removal disk drives, rewritable CD-ROMs, and back-up tapes that are used to store PHI, Category 4

References

45 Code of Federal Regulations (CFR) 164.310(d)(1)
Washington State Health Care Authority (HCA) Security Policy and Standards 6-16
Office of the Chief Information Officer (OCIO) Security Standard 141.10
CSHCD funding entities’ General Terms and Conditions, Security and Confidentiality provisions
Management Information Systems (MIS) – 57 Confidential Information Policy
Data, or information enabling security features of the provider’s information systems - are “sanitized” using the following procedures.

1.3.2. Before sale or disposal, all computer hardware is examined and certified as containing no PHI, Category 4 Data, or information enabling security features of CSHCD Information System (IS), including information that would enable a user to access CSHCD IS.

1.4. Data Segregation – The Washington State Health Care Authority (HCA) services data must be segregated or otherwise distinguishable from non-HCA data. This is to ensure that when no longer needed by CSHCD, all HCA data can be identified for return or destruction. It also aids in determining whether HCA data has or may have been compromised in the event of a security breach.

1.5. Data Transport and Access Control – Encryption and Decryption

1.5.1. When transporting PHI, Category 4 Data, or confidential information electronically, including via email, the data will be protected by physical controls, and/or encryption.

1.6. Definitions:

1.6.1. **Category 4 Data**: Data that is confidential and requires special handling due to statutes or regulations that require especially strict protection of the data and from which especially serious consequences may arise in the event of any compromise of such data. For CSHCD, data classified as Category 4 refers to data protected by the Health Insurance Portability and Accountability Act (HIPAA).

1.6.2. **Degaussing**: The process of decreasing or eliminating remnant magnetic fields.

1.6.3. Refer to MIS – 57 Confidential Information Policy for other definitions defined in contract (e.g. Confidential Information, Secured Area, etc.).

2. Procedures/Mechanisms

2.1. Protection of Data

2.1.1. **Hard disk drives**: Data stored on local workstation hard disks, including both magnetic disks or solid-state drive (SDD): Access to the data will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

2.1.2. **Network server disks**: Data stored on hard disks mounted on network servers and made available through shared folders: Access to the data will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible
only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

2.1.3. **Optical discs (CDs or DVDs).** Data created from the CSHCD SCRBH and written to an optical disk will be used in local workstations only and not be transported out of a secure area. When not in use for the contracted purpose, such discs must be locked in a drawer, cabinet, or other container to which only authorized users have the key, combination, or mechanism required to access the contents of the container. Workstations which access CSHCD SCRBH data on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

2.1.4. **Paper documents.** Any paper records must be protected by storing the records in a Secure Area which is only accessible to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

2.1.5. **Data storage on portable devices or media.** CSHCD SCRBH data shall not be stored on portable devices or media unless specifically authorized. If so authorized, the data shall be given the following protections:

2.1.5.1. Encrypt the data with a key length of at least one hundred twenty-eight (128) bits;

2.1.5.2. Control access to devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics;

2.1.5.3. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. Maximum period of inactivity is fifteen (15) minutes; and

2.1.5.4. Physically protect the portable device(s) and/or media by:

- 2.1.5.4.1. Keeping them in locked storage when not in use;
- 2.1.5.4.2. Using check-in/check-out procedures when they are shared; and
- 2.1.5.4.3. Taking frequent inventories.

2.1.5.5. When being transported outside of a Secure Area, portable devices and media with confidential CSHCD SCRBH data must be under the physical control of CSHCD SCRBH staff, contractor, or business associate with authorization to access the data.

2.1.5.6. Portable devices include, but are not limited to; smart phones, tablets, handhelds/PDAs, Ultra-mobile PCs, flash memory devices (e.g. USB flash drives or personal media players), portable hard disks, and laptop/notebook computers if those computers may be transported outside of a Secure Area.
2.1.5.7. Portable media includes, but is not limited to; optical media (e.g. CDs or DVDs), magnetic media (e.g. floppy disks, tape, Zip, or Jaz disks), or flash media (e.g. CompactFlash, SD, or MMC).

2.2. **Data Disposition**

2.2.1. When the contracted work has been completed or when no longer needed, HCA data shall be returned to HCA or destroyed in accordance with the methods specified below. Media on which data may be stored and associated acceptable methods of destruction are as follows:

<table>
<thead>
<tr>
<th>Data stored on:</th>
<th>Will be destroyed by:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Server or workstation hard Disks and SSDs, or Removable media (e.g. floppies, USB flash drives, or portable hard disks,) excluding optical discs.</td>
<td>Using a &quot;wipe&quot; utility which will overwrite the data at least three (3) times using either random or single character data; or Degaussing sufficiently to ensure that the data cannot be reconstructed; or Physically destroying the disk.</td>
</tr>
<tr>
<td>Paper documents with sensitive or confidential information.</td>
<td>Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of data will be protected.</td>
</tr>
<tr>
<td>Paper documents containing confidential information requiring special handling (e.g. PHI)</td>
<td>On-site shredding, pulping, or incineration.</td>
</tr>
<tr>
<td>Optical discs (e.g. CDs or DVDs)</td>
<td>Incineration, shredding, or completely defacing the readable surface with a coarse abrasive.</td>
</tr>
<tr>
<td>Magnetic tape</td>
<td>Degaussing, incinerating or crosscut shredding.</td>
</tr>
<tr>
<td>Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip, or similar disks)</td>
<td>Using a &quot;wipe&quot; utility which will overwrite the data at least three (3) times using either random or single character data; or Physically destroying the disk; or Degaussing magnetic media sufficiently to ensure that the data cannot be reconstructed.</td>
</tr>
</tbody>
</table>

2.3. **Device and Media Controls - Disposal**

2.3.1. All storage devices and media containing PHI or Category 4 Data are to be given to the CSHCD SCRBH Administrator or Health Insurance Portability and Accountability Act (HIPAA) Security Officer for disposal.

2.3.2. Only staff authorized by the CSHCD SCRBH Administrator or HIPAA Security Officer may dispose of CSHCD storage devices and media.

2.3.3. Before disposal, the storage media are sanitized by the methods specified in the procedures of this policy.
2.3.4. All software and data are removed from all computer equipment prior to sale or disposal of the equipment. Disk drives are sanitized by the methods specified in the procedures of this policy.

2.3.5. Logs are maintained of all computer equipment and storage media that have been disposed of by the CSHCD. These logs include the date on which storage media was/were sanitized and a description of the sanitizing method used, as specified in the procedures of this policy.

2.4. **Device and Media Controls – Reuse**

2.4.1. Before re-use, storage media are sanitized by the methods specified in the procedures of this policy.

2.5. **Data Segregation**

2.5.1. HCA, DSHS and/or CSHCD data will be kept on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-HCA or non-DSHS data; or

2.5.2. HCA, DSHS and/or CSHCD data will be stored in a logical container on electronic media, such as a partition or folder dedicated to HCA or DSHS data; or

2.5.3. HCA, DSHS and/or CSHCD data will be stored in a database which will contain no non-HCA or non-DSHS data; or

2.5.4. HCA, DSHS and/or CSHCD data will be stored within a database and will be distinguishable from non-HCA or non-DSHS data by the value of a specific field or fields within database records; or

2.5.5. When stored as physical paper documents, HCA, DSHS and/or CSHCD data will be physically segregated from non-HCA or non-DSHS data in a drawer, folder, or other container; or

2.5.6. When it is not feasible or practical to segregate HCA, DSHS or CSHCD data from non-HCA, non-DSHS or non-CSHCD data, then both the HCA or DSHS and CSHCD data and the non-HCA, non-DSHS CSHCD data with which it is commingled must be protected as described in this policy.

2.6. **Data Transport and Access Control – Encryption and Decryption**

2.6.1. CSHCD staff shall protect data, including email, by transporting the data within the CSHCD internal network.

2.6.1.1. All CSHCD staff will use encryption software when sending emails containing electronic protected health information (ePHI) or confidential information, including attachments, to recipients outside the Spokane County email system.

2.6.2. All ePHI, and confidential CSHCD information sent outside the Spokane County network by CSHCD staff, or sent outside a network provider's internal network by their staff, will be encrypted in transit by the user to prevent use by unauthorized Individuals.

2.6.2.1. CSHCD staff shall protect data by encrypting the data directly or sending it via encrypted Secure File Transfer Protocol (SFTP) in
order that the data is encrypted while in transit outside the contractor’s internal network. This includes transit over the public internet.

2.6.2.2. Data should be encrypted directly, or securely encrypted via SFTP, when it is transmitted over a network that might be accessible by unauthorized individuals. Information that can be used to alter or defeat the CSHCD security measures should also be encrypted.

2.6.3. For Spokane County CSHCD employees - Texts, “Skype,” and Email Messages are subject to public disclosure. Texts and “Skype” messages from work devices and computers should not contain PHI, Category 4 Data, confidential information, or business sensitive information.

2.6.3.1. SMARSH Text Archiving enabled on CSHCD SCRBH cell phones used by clinicians who have been approved to have text enabled capabilities in their Spokane County cell phones.

2.6.4. The CSHCD HIPAA Security Officer determines the technical methods for implementing encryption and decryption.

2.7. Notification of Compromise or Potential Compromise. The compromise or potential compromise of HCA/DSHS/CSHCD shared data must be reported to the CSHCD Administrator or the CSHCD HIPAA Security Officer within one (1) business day of discovery, and to the HCA or DSHS Contract contact by the CSHCD HIPAA Security Officer or designee within five (5) business days of discovery.

3. Monitoring

3.1. The CSHCD will require annual attestations of compliance with this policy from all applicable Subcontractors.

3.1.1. If required, due to a HIPAA incident or breach, or General Compliance/Fraud, Waste, Abuse complaint, CSHCD will monitor Subcontractors. This monitoring will include:

3.1.1.1. Desk check and/or on-site monitoring the providers’ corresponding policy(ies) and its implementation through the investigation process; and

3.1.1.2. Document any appropriate recommendations, findings, and/or corrective actions as required.