

## Confidential Information Security Requirements

### 1. Definitions

In addition to the definitions set out in Section 2 of this Contract K4030 for PATH Services, the definitions below apply to this Attachment.

- a. "Hardened Password" means a string of characters containing at least three of the following character classes: upper case letters; lower case letters; numerals; and special characters, such as an asterisk, ampersand or exclamation point.
  - i. Passwords for external authentication must be a minimum of 10 characters long.
  - ii. Passwords for internal authentication must be a minimum of 8 characters long.
  - iii. Passwords used for system service or service accounts must be a minimum of 20 characters long.
- b. "Portable/Removable Media" means any Data storage device that can be detached or removed from a computer and transported, including but not limited to: optical media (e.g. CDs, DVDs); USB drives; or flash media (e.g. CompactFlash, SD, MMC).
- c. "Portable/Removable Devices" means any small computing device that can be transported, including but not limited to: handhelds/PDAs/Smartphones; Ultramobile PC's, flash memory devices (e.g. USB flash drives, personal media players); and laptops/notebook/tablet computers. If used to store Confidential Information, devices should be Federal Information Processing Standards (FIPS) Level 2 compliant.
- d. "Secured Area" means an area to which only Authorized Users have access. Secured Areas may include buildings, rooms, or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.
- e. "Transmitting" means the transferring of data electronically, such as via email, SFTP, webservices, AWS Snowball, etc.
- f. "Trusted System(s)" means the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.

- g. "Unique User ID" means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase, or other mechanism, authenticates a user to an information system.

## 2. Confidential Information Transmitting

- a. When transmitting HCA's Confidential Information electronically, including via email, the Data must be encrypted using NIST 800-series approved algorithms (<http://csrc.nist.gov/publications/PubsSPs.html>). This includes transmission over the public internet.
- b. When transmitting HCA's Confidential Information via paper documents, the Receiving Party must use a Trusted System.

## 3. Protection of Confidential Information

The Contractor agrees to store Confidential Information as described:

- a. Data at Rest:
  - i. Data will be encrypted with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the data. Access to the Data will be restricted to Authorized Users through the use of access control lists, a Unique User ID, and a Hardened Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Systems which contain or provide access to Confidential Information must be located in an area that is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
  - ii. Data stored on Portable/Removable Media or Devices:
    - Confidential Information provided by HCA on Removable Media will be encrypted with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the Data.
    - HCA's data must not be stored by the Receiving Party on Portable Devices or Media unless specifically authorized within the Data Share Agreement. If so authorized, the Receiving Party must protect the Data by:
      1. Encrypting with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the data;
      2. Control access to the devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics;
      3. Keeping devices in locked storage when not in use;
      4. Using check-in/check-out procedures when devices are shared;

5. Maintain an inventory of devices; and
  6. Ensure that when being transported outside of a Secured Area, all devices with Data are under the physical control of an Authorized User.
- b. Paper documents. Any paper records containing Confidential Information must be protected by storing the records in a Secured Area that is accessible only 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.

#### 4. Confidential Information Segregation

HCA Confidential Information received under this Contract must be segregated or otherwise distinguishable from non-HCA data. This is to ensure that when no longer needed by the Contractor, all HCA Confidential Information can be identified for return or destruction. It also aids in determining whether HCA Confidential Information has or may have been compromised in the event of a security Breach.

1. The HCA Confidential Information must be kept in one of the following ways:
  - i. on media (e.g. hard disk, optical disc, tape, etc.) which will contain only HCA Data; or
  - ii. in a logical container on electronic media, such as a partition or folder dedicated to HCA's Data; or
  - iii. in a database that will contain only HCA Data; or
  - iv. within a database and will be distinguishable from non-HCA Data by the value of a specific field or fields within database records; or
  - v. when stored as physical paper documents, physically segregated from non-HCA Data in a drawer, folder, or other container.

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

#### 2. Confidential Information Shared with Subcontractors

If HCA Confidential Information provided under this Contract is to be shared with a Subcontractor, the contract with the Subcontractor must include all of the Confidential Information Security Requirements.

#### 3. Confidential Information Disposition

When the Confidential Information is no longer needed, except as noted below, the Confidential Information must be returned to HCA or destroyed. Media are to be destroyed using a method documented within NIST 800-88 (<http://csrc.nist.gov/publications/PubsSPs.html>).

For HCA's Confidential Information stored on network disks, deleting unneeded Confidential Information is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in Section 3, above. Destruction of the Confidential Information as outlined in this section of this Attachment may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.