DATA USE, SECURITY AND CONFIDENTIALITY

1. Definitions

The definitions below apply to this Policy:

a. **"Authorized User"** means an individual or individuals with an authorized business need to access HCA's Confidential Information under this Contract.

b. **"Breach"** means the unauthorized acquisition, access, use or disclosure of Data shared under this Contract that compromises the security, confidentiality or integrity of the Data.

c. **"Data"** means the information that is disclosed or exchanged as described by this Contract. For purposes of this Exhibit, Data means the same as "Confidential Information."

d. **"Disclosure"** means the release, transfer, provision of, access to, or divulging in any other manner of information outside the entity holding the information.

e. **"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.

    ii) Passwords for external authentication must be a minimum of 10 characters long.

    iii) Passwords for internal authentication must be a minimum of 8 characters long.

    iv) Passwords used for system service or service accounts must be a minimum of 20 characters long.

f. **"HIPAA"** means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as modified by the American Recovery and Reinvestment Act of 2009 ("ARRA"), Sec. 13400 – 13424, H.R. 1 (2009) (HITECH Act).

g. **"HIPAA Rules"** means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 C.F.R. Parts 160 and Part 164.

h. **"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).

i. **"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.

j. **"Protected Health Information" or "PHI"** means information that related to the provision of health care to an individual; the past, present, or future physical or mental health or condition of an individual; or past, present or future payment for provision of

health care to an individual. 45 C.F.R. § 160.103. PHI is information transmitted, maintained, or stores in any for or medium. 45 C.F.R § 164.501. PHI does not include education records covered by the Family Educational Right and Privacy Act, as amended, 20 U.S.C. § 1232g(a)(4)(b)(iv).

k. **"ProviderOne"** means the Medicaid Management Information System, which is the State's Medicaid payment system managed by the HCA.

l. **"Transmitting"** means the transferring of data electronically, such as via email, SFTP, web-services, AWS Snowball, etc.

m. **"Trusted System(s)"** means the following methods of physical deliver: (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.

n. **"U.S.C."** means the United States Code. All references in this Exhibit to U.S.C. chapters or sections will include any successor, amended, or replacement statute. The U.S.C. may be accessed at http://uscode.house.gov/

o. **"Use"** includes the sharing, employment, application, utilization, examination, or analysis, of Data.

2. Data Classification

a. The State classifies data into categories based on the sensitivity of the data pursuant to the Security policy and standards promulgated by the Office of the state of Washington Chief Information Officer. (See Section 4, Data Security, of Securing IT Assets Standards No. 141.10 in the State Technology Manual at https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets. Section 4 is hereby incorporated by reference.)

The Data that is the subject of this Contract is classified as Category 4 – Confidential Information Requiring Special Handling. Category 4 Data is information that is specified 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.

3. Constraints on Use of Data

a) This Contract does not constitute a release of the Data for the Contractor's discretionary use. Contractor must use the Data received or accessed under this Contract only to carry out the purpose of this Contract. Any ad hoc analyses or other use or reporting of the Data is not permitted without HCA's prior written consent.

b) Any disclosure of Data contrary to this Contract is unauthorized and is subject to penalties identified in law.

c) The Contractor must comply with the *Minimum Necessary Standard*, which means that Contractor will use the least amount of PHI necessary to accomplish the Purpose of this Contract.

i) Contractor must identify:

(1) Those persons or classes of persons in its workforce who need access to PHI to carry out their duties; and

(2) For each such person or class of persons, the category or categories of PHI to which access is needed and any conditions appropriate to such access.

ii) Contractor must implement policies and procedures that limit the PHI disclosed to such persons or classes of persons to the amount reasonably necessary to achieve the purpose of the disclosure, in accordance with this Contract.

4. Security of Data

a) Data Protection

i) The Contractor must protect and maintain all Confidential Information gained by reason of this Contract, information 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 the Contractor 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.

b) Data Security Standards

i) Contractor must comply with the Data Security Requirements set out in this section 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-technology-assets/14110-securing-information-technology-assets.) The Security Standard 141.10 is hereby incorporated by reference into this Contract.

ii) Data Transmitting

(1) When transmitting Data electronically, including via email, the Data must be encrypted using NIST 800-series approved algorithms (https://csrc.nist.gov/publications/PubsSPs.html). This includes transmission over the public internet.

(2) When transmitting Data via paper documents, the Contractor must use a Trusted System.

iii) Protection of Data. The Contractor agrees to store and protect Data as described.

(1) Data at Rest:

(a) Data will be encrypted with NIST 800-series approved algorithms. Encryptions keys will be stored and protected independently of the data. Access 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 that 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.

(2) Data stored on Portable/Removable Media or Devices

(a) 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.

(b) HCA's Data must not be stored by the Contractor on Portable Devices or Media unless specifically authorized within the Contract. If so authorized, the Contractor 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. Controlling 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. Maintaining an inventory of devices; and

6. Ensuring that when being transported outside of a Secured Area, all devices containing Data are under the physical control of an Authorized User.

(3) Papers 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 a container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

iv) Data Segregation

(1) HCA Data 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 of HCA's Data can be identified for return or destruction. It also aids in determining whether HCA's Data has or may have been compromised in the event of a security breach.

HCA's Data must be kept in one of the following ways:

(a) On media (e.g. hard disk, optical disc, tape, etc.) which contains only HCA Data;

(b) In a logical container on electronic media, such as partition or folder dedicated to HCA's Data;

(c) In a database that contains only HCA Data;

(d) Within a database – HCA data must be distinguishable from non-HCA Data by the value of a specific field or fields within database records;

(e) Physically segregated from non-HCA Data in a drawer, folder, or other container when stored as physical paper documents.

(2) When it is not feasible or practical to segregate HCA's Data from non-HCA data, both HCA's Data and the non-HCA Data with which it is commingled must be protected as described in this Exhibit.

c) Data Disposition

i) Upon request by HCA, at the end of the Contract term, or when no longer needed, Confidential Information/Data must be returned to HCA or disposed of a set out below, except as required to be maintained for compliance or accounting purposes.

Media are to be destroyed using method documented within NIST 800-88 (http://csrc.nist.gov/publications/PubsSPs.html).

ii) For Data stored on network disks, deleting unneeded Data is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in Section 1)b)iii), above. Destruction of the Data as outlined in this section of this Exhibit may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.