## EXHIBIT 7 DATA SHARING AGREEMENT

### DATA SHARING TERMS AND CONDITIONS

**PURPOSE**

The purpose of this Data Share Agreement (DSA) is to provide the terms and conditions that govern data sharing and security to fulfill the terms of this Contract.

**1. DEFINITIONS**

Definitions in Section 3.36 of this Contract are incorporated into Exhibit 7, except for the purposes of this Exhibit the following terms have the given meanings and supersede any conflicting definition in the Contract:

**"Agreement"** means this Data Sharing Agreement, which is Exhibit 7 to the Contract.

**"Authority"** or **"HCA"** means the Washington State Health Care Authority, any section, unit or other entity of the Authority, or any of the officers or other officials lawfully representing the Authority.

**"Authorized User(s)"** means an individual or individuals with an authorized business need to access HCA Confidential Information.

**"CFR"** means the Code of Federal Regulations. All references in this Data Share Agreement to CFR chapters or sections shall include any Successor, amended, or replacement regulation. The CFR may be accessed at http://www.gpoaccess.gov/cfr/index.html

**"Confidential Information"** means information that is exempt from disclosure under Chapter 42.56 RCW or other federal or state laws. Confidential Information includes, but is not limited to, Personally Identifiable Information (PII) and Protected Health Information (PHI).

**"Contract"** means the entire HCA Contract Number K1469, including any Exhibits, documents, or materials incorporated by reference.

**"Contract Consultant"** means the individual designated to receive legal notices, and to administer, amend, or terminate this Agreement.

**"Contractor"** means the individual or entity performing services pursuant to this Agreement and includes the Contractor's owners, members, officers, directors, partners, employees, and/or agents, unless otherwise stated in this Agreement. For purposes of any permitted Subcontract, "Contractor" includes any Subcontractor and its owners, members, officers, directors, partners, employees, and/or agents.

**"Data"** means the information that is disclosed or exchanged as described by this Contract.

**"Data Access"** refers to rights granted to Contractor employees to directly connect to HCA's systems, networks and /or applications via the State Governmental Network (SGN) combined with required information needed to implement these rights.

**“Data Transmission”** refers to the methods and technologies to be used to move a copy of the data between HCA and Contractor systems, networks and/or employee workstations.

**“Data Storage”** refers to the state data is in when at rest. Data can be stored on off-line devices such as CD’s or on-line on Contractor servers or Contractor employee workstations.

**“Data Encryption”** refers to ciphers, algorithms or other mechanisms that will encode data to protect its confidentiality. Data encryption can be required during data transmission or data storage depending on the level of protection required.

**“Encrypt”** means the conversion of data into a form that cannot be read without the decryption key or password. For purposes of this Agreement, data is not encrypted unless the encryption uses a key length of at least 128 bits.

**“Hardened Password”** means a string of at least eight characters containing at least three (3) of the following character classes: (1) upper case letters, (2) lower case letters, (3) numerals and (4) special characters such as an asterisk, ampersand or exclamation point.

**“Personal Information”** means information identifiable to any person, including, but not limited to, information that relates to a person’s name, health, finances, education, business, use or receipt of governmental services or other activities, addresses, telephone numbers, social security numbers, drivers license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

**“Physically Secure”** means that access is restricted through physical means to authorized individuals only.

**"Protected Health Information"** or **"PHI"** is defined in 45 CFR § 160.103.

**“RCW”** means the Revised Code of Washington. All references in this Agreement to RCW chapters or sections shall include any Successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at: http://apps.leg.wa.gov/rcw/.

**“Regulation”** means any federal, state, or local regulation, rule, or ordinance.

**“Secured Area”** means an area to which only authorized representatives of the entity possessing the Confidential Information 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.

**“Sensitive Information”** means information that is not specifically protected by law, but should be limited to official use only, and protected against unauthorized access.

**“Subcontract”** means any separate agreement or contract between the Contractor and an individual or entity (“Subcontractor”) to perform all or a portion of the duties and obligations that the Contractor is obligated to perform pursuant to this Agreement.

**“Successor”** means any entity which, through amalgamation, consolidation, or other legal succession becomes invested with rights and assumes burdens of the original Contractor.

**"Tracking"** means a record keeping system that identifies when the sender begins delivery of Confidential Information to the authorized and intended recipient, and when the sender receives confirmation of delivery from the authorized and intended recipient of Confidential Information.

**"Transmitting"** means the transferring of data electronically, such as via email.

**"Transporting"** means the physical transferring of data that has been stored.

**"Trusted Systems"** include only the following methods of physical delivery:

i. Hand-delivery by a person authorized to have access to the Confidential Information;
ii. United States Postal Service (USPS) first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail;
iii. Commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and
iv. The Washington State Campus mail system.

For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.

**"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.

**"USC"** means the United States Code. All references in this Intergovernmental Data Share Agreement to USC chapters or sections shall include any Successor, amended, or replacement statute. The USC may be accessed at http://www.gpoaccess.gov/uscode/.

**"WAC"** means the Washington Administrative Code. All references in this Agreement to WAC chapters or sections shall include any Successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at: http://apps.leg.wa.gov/wac/

## 2. DATA CLASSIFICATION

HCA must classify data into categories based on the sensitivity of the data.
Agency data classifications must translate to or include the following classification categories:

☐ **Category 1 – Public Information**
Public information is information that can be or currently is released to the public. It does not need protection from unauthorized disclosure, but does need integrity and availability protection controls.

☐ **Category 2 – Sensitive Information**
Sensitive information may not be specifically protected from disclosure by law and is for official use only. Sensitive information is generally not released to the public unless specifically requested.

☐ **Category 3 – Confidential Information**

Confidential Information is information that is specifically protected from disclosure by law. It may include but is not limited to:

a. Personal information about individuals, regardless of how that information is obtained.
b. Information concerning employee personnel records.
c. Information regarding IT infrastructure and security of computer and telecommunications systems.
d. Contractor is required to complete a Business Associates Agreement (BAA).

☐ **Category 4 – Confidential Information Requiring Special Handling**
Confidential Information requiring special handling is information that is specifically protected from disclosure by law and for which:

a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements.
b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.
c. Contractor is required to complete a Business Associates Agreement (BAA).

## 3. DATA TRANSMISSION

When transmitting HCA Confidential Information electronically, including via email, the Data shall be protected by:

a. Transmitting the Data within the (State Governmental Network) SGN or Contractor's internal network, or;

b. Encrypting any Data that will be transmitted outside the SGN or Contractor's internal network with 128-bit Advanced Encryption Standard (AES) encryption or better. This includes transit over the public Internet.

## 4. CONSTRAINTS ON USE OF DATA

This Agreement does not constitute a release of the data for the Contractor's discretionary use, but may be accessed only to carry out the responsibilities for the purposes of this Contract and for treatment, payment, and health care operations purposes (such as terms are defined under HIPAA) of Contractor and the ACP Program Providers. Any ad hoc analyses or other use of the data, not specified in this Contract, is not permitted without the prior written agreement of HCA.

If Applicable - The raw data and analysis generated will not identify personal information by name, and will be used for summary reporting purposes only. Any and all reports utilizing the data shall be subject to review prior to publication or presentation

## 5. SECURITY OF DATA

A. Data Protection

Contractor shall take due care and take commercially best efforts to protect HCA data from unauthorized physical and electronic access.

B. Data Security Technology Standards

To maintain system and network security, data integrity, and confidentiality, data will meet requirements comparable to Office of the Chief information Officer OCIO Standard 141.10. HCA will annually document and report any exceptions to OCIO 141.10. HCA will honor any CTS exemptions stated in law or granted by OCIO.

C. IT Data Security Administration

HCA and Contractor IT Data Security Administrators will exchange documentation that outlines the data security program components supporting this Agreement.

**6. NON-DISCLOSURE OF DATA**

Before receiving the data identified above, the Contractor shall notify all staff that will have access to the data of the following requirements. This notification shall include all IT support staff as well as staff who will use the data. A copy of this notification shall be provided to HCA at the same time it is provided to relevant Contractor staff.

A. Non-Disclosure of Data

a) Contractor staff shall not disclose, in whole or in part, the data provided by HCA to any individual or agency, unless this Agreement specifically authorizes the disclosure. Data may be disclosed only to persons and entities that have the need to use the data to achieve the stated purposes of this Agreement and this Contract. Nothing herein shall prohibit disclosure of data that is part of an ACP Member's medical record pursuant to an authorization by such ACP Member.

b) Contractor shall not access or use the data for any commercial or personal purpose.

c) Any exceptions to these limitations must be approved in writing by HCA.

B. Penalties for Unauthorized Disclosure of Information

In the event the Contractor fails to comply with any terms of this Agreement or this Contract, HCA shall have the right to take such action as it deems appropriate. The exercise of remedies pursuant to this paragraph shall be in addition to all sanctions provided by law, and to legal remedies available to parties injured by unauthorized disclosure.

The Contractor accepts full responsibility and liability for any violations of the Agreement.

C. Employee Awareness of Use/Non-Disclosure Requirements

The Contractor shall ensure that all staff with access to the data described in this Agreement or this Contract are aware of the use and disclosure requirements of this Agreement and will advise new staff of the provisions of this Agreement.

Contractor will provide an annual reminder to staff of these requirements. (Optional)

## 7. DATA CONFIDENTIALITY

A. The Contractor shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Agreement for any purpose that is not directly connected with Contractor's performance of the services contemplated hereunder, except:

   i. as provided by law; or,

   ii. in the case of Personal Information, with the prior written consent of the person or personal representative of the person who is the subject of the Personal Information.

B. Individuals will access data only for the purpose of this Agreement or this Contract or for treatment, payment, or healthcare operations.

C. The Contractor shall protect and maintain all Confidential Information gained by reason of this Agreement against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor to employ reasonable security measures.

D. When transporting six (6) or more records containing Confidential Information, outside a Secured Area, do one or more of the following as appropriate:

   i. Use a Trusted System.

   ii. Encrypt the Confidential Information, including:

      a. Encrypting email and/or email attachments which contain the Confidential Information.

      b. Encrypting Confidential Information when it is stored on portable devices or media, including but not limited to laptop computers and flash memory devices.

   iii. Send paper documents containing Confidential Information via a Trusted System.

E. Other than for purposes in furtherance of the Contract or in connection with Contractor's performance under the Contract, the Contractor shall not release, divulge, publish, transfer, sell, disclose, or otherwise make the Confidential Information or Sensitive Data known to any other entity or person without the express prior written consent of the Authority's Public Disclosure Office, or as required by law.

   If responding to public record disclosure requests under Chapter 42.56 RCW, the Contractor agrees to notify and discuss with the Authority's Public Disclosure Officer requests for all information that are part of this Contract, prior to disclosing the information. The Authority upon request shall provide the Contractor with the name and contact information for the Authority Public Disclosure Officer. The Contractor further agrees to provide the Authority with a minimum of two calendar weeks to initiate legal action to secure a protective order under RCW 42.56.540.

## 8. PROTECTION OF DATA HANDLING REQUIREMENTS

The Contractor agrees to store Data on one or more of the following media and protect the Data as described:

**a. Hard disk drives.** Data stored on local workstation hard disks. Access to the Data will be restricted to Authorized User(s) by requiring logon to the local workstation using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

**b. 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 Hardened 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.

For HCA Confidential Information stored on these disks, deleting unneeded Data is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in the above paragraph. Requirements relating to destruction of the Data is outlined in Section 9 of this Exhibit. Data Disposition may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

**c. Paper documents.** Any paper records must be protected by storing the records in a HIPAA-compliant manner.

**d. Access via remote terminal/workstation over the State Governmental Network (SGN).** Data accessed and used interactively over the SGN. Access to the Data will be controlled by HCA staff who will issue authentication credentials (e.g. a unique user ID and complex password) to Authorized Users. Contractor shall have established and documented termination procedures for existing Authorized Users with access to HCA Data. These procedures shall be provided to HCA staff upon request. The Contractor will notify HCA staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor, and whenever a user's duties change such that the user no longer requires access to perform work for this Contract.

**e. Access via remote terminal/workstation over the Internet through Secure Access Washington.** Data accessed and used interactively over the Internet. Access to the Data will be controlled by HCA staff who will issue remote access authentication credentials (e.g. a unique user ID and complex password) to Authorized Users. Contractor will notify HCA staff immediately whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Contractor and whenever a user's duties change such that the user no longer requires access to perform work for this Contract.

**f. Data storage on portable devices or media.**

1. HCA Data stored by the Contractor on portable devices or media shall be given the following protections:

a. Encrypt the Data with a key length of at least 128 bits using an industry standard algorithm (e.g., AES)

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

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

   a. Keeping them in locked storage when not in use

   b. Using check-in/check-out procedures when they are shared, and

   c. Maintaining an inventory

3. When being transported outside of a secure area, portable devices and media with confidential HCA Data must be under the physical control of contractor staff with authorization to access the Data.

4. Portable devices include any small computing device that can be transported. They include, but are not limited to; handhelds/PDAs/phones, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), and laptop/notebook/tablet computers.

5. Portable media includes any Data storage that can be detached or removed from a computer and transported. They include, but are not limited to; optical media (e.g. CDs, DVDs), magnetic media (e.g. floppy disks, tape,), USB drives, or flash media (e.g. CompactFlash, SD, MMC).

**9. DATA DISPOSITION**

When the contracted work has been completed or when no longer needed, except as noted in 7.a above, Data shall be returned to HCA or destroyed. Notwithstanding the foregoing, Contractor may retain a copy of the Data if required for audit purposes and/or if the return or destruction of such Data is not feasible, in which case this Agreement's requirements shall continue to apply to such Data for so long as it is retained. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

| DATA STORED ON: | WILL BE DESTROYED BY: |
|---|---|
| Server or workstation hard disks, or<br><br>Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks) | Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character Data, or<br><br>Degaussing sufficiently to ensure that the Data cannot be reconstructed, or<br><br>Physically destroying the disk |
| Paper documents with sensitive or confidential Data | Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of Data will be protected. |

| DATA STORED ON: | WILL BE DESTROYED BY: |
|---|---|
| Paper documents containing Confidential Information requiring special handling (e.g. Protected Health Information) | On-site cross-cut shredding by a method that renders the Data unreadable, pulping, or incineration |
| Optical discs (e.g. CDs or DVDs) | Incineration, shredding, or cutting/breaking into small pieces. |
| Magnetic tape | Degaussing, incinerating or crosscut shredding |

**10. NOTIFICATION OF COMPROMISE OR POTENTIAL COMPROMISE**

The Contractor shall have an established and documented policy to deal with the compromise or potential compromise of Data that complies with the HITECH Act of ARRA 209. The Contractor shall provide HCA staff a copy of such policy upon request. Contractor shall be responsible for any cost associated with a compromise or potential compromise.

Contractor will report to HCA any use or disclosure of the Protected Health Information not provided for by this Agreement or this Contract. Contractor will make these reports to the HCA contract manager within five (5) Business Days after the use or disclosure, or within five (5) Business days after Contractor discovers a use or disclosure that is likely to involve ACP Members, whichever is later. If Contractor cannot provide conclusive information relating to the use or disclosure until a full investigation has occurred, then it will provide what information it can within five (5) Business days, and full details no later than fifteen (15) Business days after discovery of the use or disclosure.

**11. NOTICE OF BREACH**

For purposes of this provision, “breach” has the meaning defined in 45 CFR § 164.402.
If Contractor or any Subcontractor of it allegedly makes or causes, or fails to prevent, a use or disclosure constituting a Breach, and notification of that use or disclosure must (in the judgment of HCA) be made under 45 CFR part 164, subpart D (§§ 164.402 et seq.) or under RCW 45.56.590 or RCW 19.255.010 or other applicable law, then

(a) HCA may choose to make the notifications or direct Contractor to make them, and

(b) When there is a reasonable basis for believing that there is a risk of financial harm to ACP Members, Contractor will offer to pay for reasonable cost of notification and twelve (12) months of credit monitoring to ACP Members impacted by the breach.

Contractor will ensure that any agents, including a Subcontractor, to whom it provides any of the Data agrees to the same restrictions and conditions that apply to the limited data set recipient with respect to such information.

The reporting obligations of this Section do not apply to Covered Entity functions of network member providers of Contractor, including their role as treatment providers for ACP Members.

**12. DATA SHARED WITH SUB-CONTRACTORS**

The Contractor is prohibited to enter into subcontracts for the purposes under this Agreement that are exclusively focused on the provision of Covered Services directly to ACP Members under the

Contract without obtaining prior written approval from HCA. In no event shall the existence of the subcontract operate to release or reduce the liability of the Contractor to HCA for any breach in the performance of the Contractor's responsibilities.

Additionally, the Contractor is responsible for ensuring that all terms, conditions, assurances and certifications set forth in this Agreement are carried forward to any subcontracts. Contractor and its Subcontractors agree not to release, divulge, publish, transfer, sell or otherwise make known to unauthorized persons personal information without the express written consent of HCA or as provided by law.

**13. OVERSIGHT**

The Contractor agrees that HCA will have the right, upon at least ten (10) business days' notice, to review (including onsite facility review) activities and methods in implementing this Agreement in order to assure compliance therewith, within the limits of technical capabilities.

Notwithstanding anything in this Contract or Agreement, Contractor represents and warrants that Contractor and Sub-Contractor electronic health record system or other clinical information systems are used for treatment, payment or healthcare operations and HCA agrees it will not subject such systems to systemic external audit.