Washington State Health Care Authority	**MEMORANDUM OF UNDERSTANDING AMENDMENT**	HCA Contract No.: K1598-1 Amendment: 02
THIS AMENDMENT TO THE CONTRACT is between the Washington State Health Care Authority and the party whose name appears below, and is effective as of the date set forth below.		
CONTRACTOR NAME Washington Association of Local Public Health Officials	**CONTRACTOR doing business as (DBA)**	
CONTRACTOR ADDRESS 206 Tenth Ave SE Olympia, WA 98501-1311	**WASHINGTON UNIFORM BUSINESS IDENTIFIER (UBI)**	

WHEREAS, HCA and the Washington State Association of Local Public Health Officials (WSALPHO) previously entered into the Contract for real time access to WSALPHO's Random-Moment-Time-Study (RMTS) system and related databases to HCA, and;

WHEREAS, HCA and WSALPHO wish to amend the Contract pursuant to Section III Statement of Work; Section IV Data Sharing; Section VI Period of Performance; and Section VII Contract Management;

NOW THEREFORE, the HCA and WSALPHO agree the MOU is amended as follows.

1. **Section III STATEMENT OF WORK**. The Statement of Work has been amended. Attached hereto as Attachment 1 is the updated Statement of Work.

2. **Section IV DATA SHARING.** The Data Share Agreement which was identified as Attachment A of the MOU has been amended. Attachment 2 hereto represents the updated Date Share Agreement between the Parties.

3. **Section VI PERIOD OF PERFORMANCE.** The period of performance of this MOU shall begin on the date of execution and will continue through December 31, 2018 unless terminated sooner, as provided herein.

4. **Section VII CONTRACT MANAGEMENT.** The individuals listed below, or their successors, shall be the contact person for all communications regarding contract performance and deliverables. The HCA Contract Manager has the authority to accept or reject the services provided and has the responsibility to monitor WSALPHO's performance.

WSALPHO	HCA
Jaime Bodden	Jon Brogger
206 Tenth Avenue SE	PO Box 45530

Olympia, WA 98501-1311 (360) 489-3011 jbodden@wsac.org	Olympia, WA 98504-5530 (360) 725-1647 jon.brogger@hca.wa.gov

5. All other terms and conditions of the Contract remain unchanged and in full force and effect.

The effective date of this amendment is date of execution.

The parties signing below warrant that they have read and understand this Amendment and have authority to execute the Amendment. This Amendment will be binding on HCA only upon signature by HCA.

CONTRACTOR SIGNATURE DocuSigned by: Jaime Bodden EC3521C1809E460...	PRINTED NAME AND TITLE Jaime Bodden Managing Director, WSALPHO	DATE SIGNED 12/22/2017
HCA SIGNATURE DocuSigned by: James Gayton 0E3A2FE546AF45F...	PRINTED NAME AND TITLE James W. Gayton Contract Administrator	DATE SIGNED 12/27/2017

Attachment 1

Statement of Work

WSALPHO will provide services and staff, and otherwise do all things necessary for or incidental to the performance of work, as set forth below.

General System Requirements: WSALPHO will provide a System that:

1. Complies with this agreement, the CMS approved CAP, HCA-LHJ MAC agreements, and any updates or amendments;
2. Is fully integrated and operates the following in compliance with the methodology described in the CAP and required by CMS:
    a. A statistically valid time study, specifically an RMTS;
    b. A mathematically sound MER calculation process;
    c. A mathematically sound, web-based claiming process;
    d. A documentation storage function for individual LHJ, consortia, and program level MAC related documentation;
3. Resides on an IT infrastructure provided by WSALPHO and is fully accessible via internet connection;
4. Is fully functional and compatible with Apple, Microsoft, and with commonly used Internet browsers including but not limited to, Internet Explorer, Google Chrome, Safari, and Firefox;
5. Has the ability to interface with multiple active directories for generating email reminders;
6. Requires password authentication or secure encryption for all interactions with the System;
7. Operates in a transparent manner with established internal controls, documented processes, system specifications, and data easily traceable to the source.
8. Is tested on a documented schedule, or more often, to ensure System integrity
9. With a dedicated Help Desk that can be accessed either online or through a toll-free number and staffed during standard business days, for systems-related questions pertaining to the System;
10. Maintains all information and data in a transparent and usable report format, and is maintained according to the Secretary of State retention schedule. Data must be available on demand, at the consortia, LHJ, subunit, subcontract, job title, and individual level.
11. Provides HCA with unlimited, real-time access to all platforms of the time study or claiming data. This includes but is not limited; to online portals, databases, and excel spreadsheets.
12. Provides a certification function for all data entered into the System.
13. Is flexible and capable of modifying existing reports or producing new or adhoc reports. This also includes historical data.
14. Operates on a quarterly schedule, based on the calendar year (January-March, April-June, July-September, October-December) with documented and published timelines for critical functions (such as for generating moments, completing participant training, or entering new participants).
15. Maintains a standardized, statewide contact list template (including basic demographics, designated RMTS/Fiscal coordinators, A19-1A and contract signature authorities) for participating LHJs and updates as needed.

<u>**Specific System Requirements**</u>: WSALPHO will provide a System that complies with the time study methodology and claiming process described in the CMS approved CAP, including but not limited to:

1. Standardized and documented process for entering and/or updating time study data including:
    a. Staff/participant demographics
    b. Agency and staff/participant calendars
    c. Assigned RMTS/Fiscal coordinators, code reviewers, or other pertinent roles

2. Producing reports validating statistical validity of the time study, including the methodology for determining statistical validity.

3. Recording and displaying (and in report format) each moment with following, if applicable:
    a. The participant's original activity code and narrative description
    b. The clarifying question and response,
    c. Activity code correction and comments
    d. The name of each individual asking clarifying questions or completing code corrections
4. Standardized data entry for salary and benefit expenses via:
    a. Roll-up format for RMTS participants,
    b. Data entry format for individual direct charge staff
    c. Roll-up format for all other staff salary and benefit expenses

5. Standardized data entry for non-personnel expenses via:
    a. Roll-up format by account code, for all "other" costs and identified by CP or direct charge
    b. Roll-up format by vendor for personal service contracts and identified by CP or direct charge

6. Standardized data entry for single cost objective MAC activity documentation, by individual.

7. Standardized data entry for indirect cost rates.

8. Standardized and documented MER process utilizing the HCA Medicaid Management Information System (MMIS); ProviderOne, and:
    a. A published template to be used for the client-list upload
    b. The procedure for calculating the client-based, clinic-based, and modified county-wide MER
    c. Published reports for each LHJ MER that is calculated

9. Standardized data entry for Certified Public Expenditure (CPE)
    a. Roll-up format by State Auditor's Office GAAP and Cash-Basis Budgeting, Accounting, and Reporting System (BARS) 7-digit codes
    b. Certification function validating compliance with CPE criteria

10. A standardized and documented process for revenue offset and calculation of the Federal Financial Participation (FFP) reported on A19-1A

11. Producing an electronic A19-1A invoice voucher accessible by HCA, to include an approve or reject function

12. Producing a printable A19-1A invoice voucher upon electronic approval by HCA

Program Requirements: WSALPHO will support the LHJ MAC program by:

1. Hosting an LHJ Steering Committee and designating one representative from the Lead agency of each Consortium and one representative from each LHJ participating in its own RMTS.
    a. WSALPHO will represent LHJs statewide through the LHJ Steering Committee in all aspects of the MAC program, and specifically through collaborative policy development with HCA. WSALPHO must obtain written agreement for this representation from each LHJ participating in the MAC program and using the

WSALPHO System. Copies of the written agreement must be provided to HCA.

b. WSALPHO will ensure that the LHJ Steering Committee will communicate any changes, updates, modifications to the vendor URMTS system in advance to all participating LHJs. In addition, all participating LHJs must be notified when system errors are identified and resolved.

c. WSALPHO will establish and maintain committee bylaws, policies and processes

2. Configuring the RMTS consortia organization, and submitting an annual consortia proposal by December 1st of each year and to include:
   a. Number of consortia
   b. Number of LHJs assigned per consortia
   c. Name of each LHJ assigned per consortia
   d. Lead Agency (LHJ) assigned to each consortia
   e. Geographic map identifying each LHJ per consortia
   f. Detailed description of changes to the consortium organization including why the changes are necessary
   g. Narrative and technical summary of anticipated impact to the LHJ MAC program

3. Hosting quarterly RMTS consortium calls on a documented and published schedule.

4. Completing a random 10% quality assurance review of each RMTS.

5. Providing training and technical assistance for the System and all platforms of the time study or claiming data. Training must be provided to each LHJ and HCA on a documented schedule each time there are changes, modifications, etc. to the System, or as requested.

6. Preparing and publishing detailed information, instructions, online training or other materials on the technical aspects and functions of the System.

7. Providing a standardized and documented change request process. This must include review with HCA, and documented approvals or denials.

8. Collaborating with HCA to prepare and publish detailed information, instructions, and training for the MAC program, specifically for LHJ coordinators and participants. All program training must be approved by HCA prior to publication or use.

9. Completing any and all updates, modifications, or other changes requested by HCA and/or CMS to the System, data, reports, or methodology within a mutually agreed time frame discussed and approved in writing by all parties.

10. Maintaining all data and records as required by HCA and the Secretary of State.

11. Providing complete and unlimited access to all MAC related data to HCA.

12. Producing and/or collaborating with HCA to update or produce new documents, templates, forms, standard reports, adhoc reports, or other materials or information as needed within a timeframe agreed, in writing, by both parties.

13. Providing a written report from a certified and licensed Accountant verifying that all System calculations (RMTS, MER, Offset, FFP etc.) are mathematically sound and accurate within 90 days after any changes are made to any calculations in the System.

14. Providing a written report within 45ays following any MAC training series that summarizes training feedback, trends and observations.

15. Producing the following written, standardized quarterly reports and collaborating with HCA regarding any action needed to ensure the statewide LHJ MAC program is in compliance and at low audit risk. These reports may be provided in a web-based, on demand format as appropriate:

    a. Summary System status report, due 45 business days after the end of each quarter, to include:

        i. Any consortium or structural changes to the RMTS
        ii. All new user IDs issued or terminated or changes to system access
        iii. Updates to the technical or system specifications
        iv. System errors and warnings
        v. System outages and resolutions
        vi. Deployed or proposed system patches
        vii. Work performed during scheduled maintenance
        viii. Established or proposed protocols for a work-around
        ix. Security breaches or concerns

    b. Summary Consortium report, due 45 business days after the end of each quarter, to include:

        i. Written summaries of each call
        ii. Meeting schedule and agendas
        iii. Training or technical assistance requested and/or completed
        iv. Major concerns or issues that may impact the MAC program or require troubleshooting

    c. Summary LHJ Steering Committee report, due 45 business days after the end of each quarter, to include:

        i. Official list of membership including name, joining date, role, employing agency, phone number, address, and email for all members
        ii. Updates to committee bylaws, policies, processes, contract terms or other changes affecting the structure, function, or actions of the steering committee
        iii. Meeting schedule and agendas
        iv. Actions taken or proposed to be taken and the intended result of the action, if any
        v. Results of actions taken during the previous quarter, if any

    d. Statewide analysis and summary of all Skilled Professional Medical Personnel (SPMP) activities, due 120 days after the end of each quarter, to include:

        i. Types/classifications of participating SPMP
        ii. Certifications and trainings achieved during quarter
        iii. Percent of SPMP activities allocated to 75%, and 50%
        iv. Comparison of SPMP reports produced by each LHJ
        v. Trends or concerns for SPMP participation
        vi. Recommendations for HCA directed activities based on community needs
        vii. Inappropriately recorded activities

e. Statewide RMTS analysis and quality assurance report, due 120 business days after the end of each quarter, to include:

i. Completion date for each RMTS 100% code review by LHJ and consortium
ii. Completion date for WSALPHO 10% random sample review
iii. Sortable list of all moments (and moment data) with code corrections
iv. Sortable list of all moments (and moment data) with clarifying questions and/or responses
v. Identified trends, recommendations, concerns, inappropriately recorded activities or other topics.

Attachment 2

Data Share Agreement

1. Purpose of the DSA

The purpose of this Data Share Agreement (DSA) is to provide eligibility data to Washington State Association of Local Public Health Officials (WSALPHO) in order for them to calculate the Medicaid Eligibility Rate (MER) based on the methodology developed by the Department of Social and Health Services (DSHS) Research and Data Analysis (RDA) Division for each Local Health Jurisdiction (LHJ) participating in the Medicaid Administrative Claiming (MAC) program. The MER is a critical component of the MAC claiming process.

2. Justification for Data Sharing

The Data to be shared under this DSA is necessary for Receiving Party to determine the Medicaid eligibility of individuals served at each LHJ over the course of a calendar quarter and calculate the MER based on the DSHS/RDA methodology for use in the MAC program.

HCA contracts with LHJs to participate in the Medicaid Administrative Claiming (MAC) program and provides partial reimbursement for the federal share of allowable MAC activities. To determine how these activities are reimbursed, HCA must submit a CAP to the CMS for approval. The CAP includes a description of, including but not limited to; RMTS methodology, claiming methodology, revenue offset, MER and oversight responsibilities

3. Definitions

"Agency" means the state of Washington Health Care Authority ("HCA") and includes any division, section, office, unit, officers or other officials lawfully representing HCA.

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

"Breach" means the acquisition, access, use, or disclosure of Protected Health Information in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the Protected Health Information, with the exclusions and exceptions listed in 45 CFR 164.402

"Business Associate" means a Business Associate as defined in 45 CFR 160.103, who performs or assists in the performance of an activity for or on behalf of HCA, a Covered Entity, that involves the use or disclosure of protected health information (PHI). Any reference to Business Associate in this DSA includes Business Associate's employees, agents, officers, Subcontractors, third party contractors, volunteers, or directors.

"Business Associate Agreement" means the HIPAA Compliance section of this DSA (Section 13) and includes the Business Associate provisions required by the U.S. Department of Health and Human Services, Office for Civil Rights.

"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.

"Client" means an individual who is eligible for or receiving federal or state funded Medicaid services provided by the Receiving Party.

"Confidential Information" means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information comprises both Category 3 and Category 4 Data as described in Section 6, *Data Classification*, which includes, but is not limited to, Personal Information and Protected Health Information. For purposes of this DSA, Confidential Information means the same as "Data."

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

"Contract Manager" means the individual identified on the cover page of this DSA who will provide oversight of the activities conducted under this DSA.

"Covered Entity" means HCA, which is a Covered Entity as defined in 45 CFR 160.103.

"Data" means the information that is disclosed or exchanged as described by this Data Share Agreement (DSA). For purposes of this DSA, Data means the same as "Confidential Information."

"Designated Record Set" means a group of records maintained by or for a Covered Entity, that is: the medical and billing records about Individuals maintained by or for a covered health care provider; the enrollment, payment, claims adjudication, and case or medical management record systems maintained by or for a health plan; or Used in whole or part by or for the Covered Entity to make decisions about Individuals.

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

"DSA" means this Data Share Agreement.

"Electronic Protected Health Information (ePHI)" means Protected Health Information that is transmitted by electronic media or maintained in any medium described in the definition of electronic media at 45 CFR 160.103.

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

"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).

"HIPAA Rules" means the Privacy, Security, Breach Notification, and Enforcement Rules at 45 CFR Parts 160 and Part 164.

"Individual(s)" means the person(s) who is the subject of PHI and includes a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

"Minimum Necessary" means the least amount of PHI necessary to accomplish the purpose for which the PHI is needed.

"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, driver's license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

"Protected Health Information" or **"PHI"** means information created, received, maintained or transmitted by a Business Associate from or on behalf of a Covered Entity that relates 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 CFR 160 and 164. PHI includes demographic information that identifies the individual or about which there is reasonable basis to believe, can be used to identify the individual. 45 CFR 160.103. PHI is information transmitted, maintained, or stored in any form or medium. 45 CFR 164.501. PHI does not include education records covered by the Family Educational Right and Privacy Act, as amended, 20 USCA 1232g(a)(4)(b)(iv).

"ProviderOne" means the Medicaid Management Information System that is the State's Medicaid payment system managed by HCA.

"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.

"Receiving Party" means the entity that is identified on the cover page of this DSA and is a party to this Agreement, and includes the entity's owners, members, officers, directors, partners, trustees, employees, agents, and Subcontractors and their owners, members, officers, directors, partners, trustees, employees, and/or agents.

"Security Incident" means the attempted or successful unauthorized access, use, disclosure, modification or destruction of information or interference with system operations in an information system.

"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 Receiving Party and an individual or entity ("Subcontractor") to perform any duties that give rise to a business requirement to access the Data that is the subject of this DSA.

"Subcontractor" means an individual or entity (including its owners, members, officers, directors, trustees, employees, and/or agents) with whom the Receiving Party contracts to provide services or perform any duties that give rise to a business requirement to access the Data that is the subject of this DSA

"USC" means the United States Code. All references in this 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/.

"Use" includes the sharing, employment, application, utilization, examination, or analysis, of PHI within an entity that maintains such information

"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/.

4. AUTHORITY TO ACCESS DATA

Pursuant to the authority granted by CFR 433.15(b)(7) and RCW 43.70.522.

5. Description of Data to be Shared

A List of Medicaid eligible clients during the report quarter that omits clients that were in suspended status for all three months of the quarter. If a client was eligible at any point during the reported quarter, that client will show eligible on the report.

Below mentioned data elements will be shared from HCA's ProviderOne data warehouse (ODS). This data transfer will occur on a quarterly basis, and file will be transferred over the secured FTP Server. Notification will be sent to mer-data@hfa3.org and jbodden@wsac.org when data is ready to access. File format will be tab delimited text file.

Data Elements:

- MBR_MMIS_IDNTFR - the member identification number
- RPRTBL_RAC_CODE - the member eligibility code, indicating member status
- ELIGIBILITY_STATUS_NAME - the text of the member eligibility status, i.e. "ACTIVE"
- FIRST_NAME - member first name
- LAST_NAME - member last name
- MIDDLE_NAME - member middle name, if known
- RSDNTL_ADRS_LINE_1 - the street address of the member
- RSDNTL_ADRS_LINE_2 - additional street address lines, if necessary
- RSDNTL_ADRS_LINE_3 - additional street address lines, if necessary
- RSDNTL_CITY_NAME - the name of the city
- RSDNTL_STATE_NAME - the full name of the member's state
- RESIDENTIAL_ZIP_CODE - the 5-digit zip code for a member
- RSDNTL_COUNTY_CODE - the 5-digit county code for a member

- RSDNTL_COUNTY_NAME - the name of the member's county, not including the word "County". i.e. "KING" for a member living in King County.
- rsdntl_state_code – Member's residential state code

- Data Element See table above
- Time Frame data is provided quarterly, approximately 2 weeks after the end of a quarter
- Format of the Data File format will be tab delimited text file

6. Data Classification

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 Chief Information Officer. (See Section 4, *Data Security*, of *Securing IT Assets Standards* No. 141.10 in the *State Technology Manual* at http://ofm.wa.gov/ocio/policies/manual.asp)
The Data that is the subject of this DSA is classified as indicated below:
☐ 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;
☒ 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.

7. Constraints on Use of Data

7.1 The Data being shared/accessed is owned and belongs to HCA.

7.2 The Data shared under this Agreement can be used only for MER calculation process based on the DSHS/RDA methodology and no other purposes.

7.3 This Agreement does not constitute a release of the Data for the Receiving Party's discretionary use. Receiving Party may use the Data received or accessed under this DSA only to carry out the purposes described herein. Any analysis, use, or reporting that is not within the Purpose of this DSA is not permitted wthout HCA's prior written consent.

7.4 Any disclosure of Data contrary to this Agreement is unauthorized and is subject to penalties identified in law.

8. Security of Data

8.1 Data Protection

The Receiving Party shall protect and maintain all Confidential Information gained by reason of this Data Share Agreement against unauthorized use, access, disclosure, modification or loss. This duty requires the Receiving Party to employ reasonable security measures, which include restricting access to the Confidential Information by:

8.1.1 Allowing access only to staff that have an authorized business requirement to view the Confidential Information.

8.1.2 Physically securing any computers, documents, or other media containing the Confidential Information.

8.2 Data Security Standards

Receiving Party shall comply with the Data Security Requirements set out in Exhibit A and the Washington OCIO Security Standard, 141.10 (https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets).

8.3 Data Disposition

Upon request by HCA, at the end of the DSA term, or when no longer needed, Confidential Information must be disposed of as set out in Exhibit A, Section 5 *Data Disposition*, except as required to be maintained for compliance or accounting purposes. Receiving Party will provide written certification of disposition at HCA's request.

9. Data Confidentiality and Non-Disclosure

9.1 Data Confidentiality.

The Receiving Party will 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 the purpose and justification of this Agreement set out in Sections 1 and 2 above, except: (a) as provided by law; or (b) with the prior written consent of the person or personal representative of the person who is the subject of the Confidential Information.

9.2 Non-Disclosure of Data.

9.2.1 The Receiving Party must ensure that all employees who will have access to the Data described in this Agreement (including both employees who will use the Data and IT support staff) are instructed and made aware of the use restrictions and protection requirements of this Agreement before gaining access to the Data identified herein. The Receiving Party will also instruct and make any new employee aware of the use restrictions and protection requirements of this Agreement before they gain access to the Data.

9.2.2 Receiving Party must provide an annual reminder to staff of the use restrictions and protection requirements of this DSA.

9.2.3 Each employee who will access the Data will be required to sign the *User Agreement on System Usage and Non-Disclosure of Confidential Information*, Exhibit B hereto. Receiving Party will retain the signed copy of the *User Agreement on System Usage and Non-Disclosure of Confidential Information* on file for a minimum of six years from the date the employee's access to the Data ends. The documentation must be available to HCA upon request.

9.3 Penalties for Unauthorized Disclosure of Data

State laws (including RCW 74.04.060 and RCW 70.02.020) and federal regulations (including HIPAA Privacy and Security Rules, 45 CFR Part 160 and Part 164; Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR, Part 2; and Safeguarding Information on Applicants and Beneficiaries, 42 CFR Part 431, Subpart F) prohibit unauthorized access, use, or disclosure of Confidential Information. Violation of these laws may result in criminal or civil penalties or fines.

The Receiving Party accepts full responsibility and liability for any noncompliance with these laws and any violations of the Agreement.

10. Data or Systems Access

Vendor will download the file from SFTP server.

The Receiving Party must access these systems through the State Governmental Network (SGN), the Inter-Governmental Network (IGN) SecureAccessWashington (SAW) or through another method of secure access approved by HCA.

10.1 Receiving Party Point of Contact

The Receiving Party must identify a point of contact who will be the single source of access requests and the person HCA will contact for any follow up information or to initiate an audit under this DSA.

Name or Title Jaime Bodden
Address 206 Tenth Avenue SE
Olympia, WA 98501-1311
Telephone: (360) 489-3011
E-mail: jbodden@wsac.org

The Receiving Party Point of Contact address and information provided above may be changed by written notice to the HCA Point of Contact, email acceptable.

10.2 HCA Point of Contact

HCA's single point of contact for all inquiries, problem reporting or access requests from the Receiving Party is:

Name or Title Jon Brogger, MAPS 3
Address PO Box 45530
Olympia, WA 98504-5530
Telephone: (360) 725-1647
E-mail: jon.brogger@hca.wa.gov

The HCA Point of Contact address and information provided above may be changed by written notice to the Receiving Party Point of Contact, email acceptable.

10.3 HCA will grant the appropriate access permissions to Receiving Party employees or Subcontractor employees.

10.4 HCA does ***not*** allow shared User IDs and passwords for use with Confidential Information or to access systems that contain Confidential Information. Receiving Party shall ensure that only Authorized Users access and use the systems in this Agreement, use only their own User ID and password to access the systems and do not allow employees, agents or Subcontractors who are not authorized to borrow a User ID or password to access any systems.

10.5 The Receiving Party will notify the HCA Point of Contact within five (5) business days whenever an Authorized User who has access to the Data is no longer employed or contracted by the Receiving Party or whenever an Authorized User's duties change such that the user no longer requires access to the Data.

10.6 Receiving Party's access to the systems may be continuously tracked and monitored. HCA reserves the right at any time to terminate data access for an individual, conduct audits of systems access and use, and to investigate possible violations of this

Agreement and/or violations of federal and state laws and regulations governing access to Protected Health Information.

11. Public Disclosure Requests

If the Receiving Party receives a public records request under Chapter 42.56 RCW for any records containing Data subject to this DSA, Receiving Party agrees to notify the HCA Public Disclosure Officer within five (5) business days and to follow the procedure set out in this section before disclosing any records. The HCA Public Disclosure Officer can be contacted at PublicDisclosure@hca.wa.gov.

The Receiving Party must provide a copy of the records with proposed redactions to HCA when they are available and ready. HCA will respond within ten (10) business days of receipt of the redacted records to identify concerns with disclosure of the records, propose any changes to the Receiving Party redactions, or request more time if needed. If Receiving Party disagrees with any of HCA's concerns or proposed changes, Receiving Party must notify HCA of that disagreement and provide HCA with a minimum of fifteen (15) business days to obtain a restraining order or injunction under RCW 42.56.540 before disclosing any records.

12. Data Shared with Subcontractors

If Data access is to be provided to a Subcontractor under this DSA, the Receiving Party must include all of the Data security terms, conditions and requirements set forth in this Agreement in any such Subcontract. Because the Data includes PHI, Section 13.5 *Subcontracts and Other Third Party Agreements* also applies. In no event shall the existence of the Subcontract operate to release or reduce the liability of the Receiving Party to HCA for any breach in the performance of the Receiving Party's responsibilities.

13. HIPAA Compliance

This section of the Agreement is the Business Associate Agreement required by HIPAA. The Receiving Party is a "Business Associate" of HCA as defined in the HIPAA Rules.

13.1 **HIPAA Point of Contact.** The point of contact for the Receiving Party for all required HIPAA-related reporting and notification communications from this Section 13 *HIPAA Compliance* and all required Non-PHI Data breach notification communications from Section 14 *Non-PHI Data Breach Notification,* is*:*

HCA Privacy Officer
Washington State Health Care Authority
626 8th Avenue SE
PO Box 42700
Olympia, WA 98504-2700
Telephone: 360-725-1116
E-mail: PrivacyOfficer@hca.wa.gov

13.2 **Compliance**. Business Associate must perform all Agreement duties, activities and tasks in compliance with HIPAA, the HIPAA Rules, and all attendant regulations as promulgated by the U.S. Department of Health and Human Services, Office for Civil Rights.

13.3 **Use and Disclosure of PHI**. Business Associate is limited to the following permitted and required uses or disclosures of PHI:

13.3.1 Duty to Protect PHI. Business Associate must protect PHI from, and will use appropriate safeguards, and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to ePHI, to prevent the unauthorized Use or disclosure of PHI for as long as the PHI is within its possession and control, even after the termination or expiration of this Agreement.

13.3.2 Minimum Necessary Standard. Business Associate will apply the HIPAA Minimum Necessary standard to any Use or disclosure of PHI necessary to achieve the purposes of this Agreement. See 45 CFR 164.514 (d)(2) through (d)(5).

13.3.3 Disclosure as Part of the Provision of Services. Business Associate will only Use or disclose PHI as necessary to perform the services specified in this Agreement or as required by law, and will not Use or disclose such PHI in any manner that would violate Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information) if done by Covered Entity, except for the specific uses and disclosures set forth below.

13.3.4 Use for Proper Management and Administration. Business Associate may Use PHI for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

13.3.5 Disclosure for Proper Management and Administration. Business Associate may disclose PHI for the proper management and administration of Business Associate, subject to HCA approval, or to carry out the legal responsibilities of the Business Associate, provided the disclosures are required by law, or Business Associate obtains reasonable assurances from the person to whom the information is disclosed that the information will remain confidential and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been Breached.

13.3.6 Impermissible Use or Disclosure of PHI. Business Associate must report to the contact identified in Subsection 13.1 in writing all Uses or disclosures of PHI not provided for by this Agreement within five (5) business days of becoming aware of the unauthorized Use or disclosure of PHI, including Breaches of unsecured PHI as required at 45 CFR 164.410 (Notification by a Business Associate), as well as any Security Incident of which it becomes aware. Upon request by HCA, Business Associate will mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or disclosure.

13.3.7 Failure to Cure. If HCA learns of a pattern or practice of the Business Associate that constitutes a violation of the Business Associate’s obligations under the terms of this Agreement and reasonable steps by the Business Associate do not end the violation, HCA may terminate this Agreement, if feasible. In addition, If Business Associate learns of a pattern or practice of its Subcontractors that constitutes a violation of the Business Associate’s obligations under the terms of their contract and reasonable steps by the Business Associate do not end the violation, Business Associate must terminate the Subcontract, if feasible.

13.3.8 Termination for Cause. Business Associate authorizes immediate termination of this Agreement if HCA determines that Business Associate has violated a material term of this Business Associate Agreement. HCA may, at its sole option, offer Business Associate an opportunity to cure a violation of this Business Associate Agreement before exercising a termination for cause.

13.3.9 Consent to Audit. Business Associate must give reasonable access to PHI, its internal practices, records, books, documents, electronic data and/or all other business information received from, or created or received by Business Associate on behalf of HCA, to the Secretary of DHHS and/or to HCA for use in determining compliance with HIPAA privacy requirements.

13.3.10 Obligations of Business Associate Upon Expiration or Termination. Upon expiration or termination of this Agreement for any reason, with respect to PHI received from HCA, or created, maintained, or received by Business Associate, or any Subcontractors, on behalf of HCA, Business Associate must:

i. Retain only that PHI which is necessary for Business Associate to continue its proper management and administration or to carry out its legal responsibilities;

ii. Return to HCA or destroy the remaining PHI that the Business Associate or any

Subcontractors still maintain in any form;

iii. Continue to use appropriate safeguards and comply with Subpart C of 45 CFR Part 164 (Security Standards for the Protection of Electronic Protected Health Information) with respect to Electronic Protected Health Information to prevent Use or disclosure of the PHI, other than as provided for in this Section, for as long as Business Associate or any Subcontractors retain the PHI;

iv. Not Use or disclose the PHI retained by Business Associate or any Subcontractors other than for the purposes for which such PHI was retained and subject to the same conditions set out in Subsection 13.3 *Use and Disclosure of PHI* that applied prior to termination; and

v. Return to HCA or destroy the PHI retained by Business Associate, or any Subcontractors, when it is no longer needed by Business Associate for its proper management and administration or to carry out its legal responsibilities.

13.3.11 Survival. The obligations of the Business Associate under this section will survive the termination or expiration of this Agreement.

13.4 **Individual Rights**.

13.4.1 Accounting of Disclosures.

i. Business Associate will document all disclosures, except those disclosures that are exempt under 45 CFR 164.528, of PHI and information related to such disclosures.

ii. Within ten (10) business days of a request from HCA, Business Associate will make available to HCA the information in Business Associate's possession that is necessary for HCA to respond in a timely manner to a request for an accounting of disclosures of PHI by the Business Associate. See 45 CFR 164.504(e)(2)(ii)(G) and 164.528(b)(1).

iii. At the request of HCA or in response to a request made directly to the Business Associate by an Individual, Business Associate will respond, in a timely manner and in accordance with HIPAA and the HIPAA Rules, to requests by Individuals for an accounting of disclosures of PHI.

iv. Business Associate record keeping procedures will be sufficient to respond to a request for an accounting under this section for the six (6) years prior to the date on which the accounting was requested.

13.4.2 Access

i. Business Associate will make available PHI that it holds that is part of a Designated Record Set when requested by HCA or the Individual as necessary to satisfy HCA' obligations under 45 CFR 164.524 (Access of Individuals to Protected Health Information).

ii. When the request is made by the Individual to the Business Associate or if HCA ask the Business Associate to respond to a request, the Business Associate must comply with requirements in 45 CFR 164.524 (Access of Individuals to Protected Health Information) on form, time and manner of access. When the request is made by HCA, the Business Associate shall provide the records to HCA within ten (10) business days.

13.4.3 Amendment.

i. If HCA amends, in whole or in part, a record or PHI contained in an Individual's Designated Record Set and HCA has previously provided the PHI or record that is the subject of the amendment to Business Associate, then HCA will inform Business Associate of the amendment pursuant to 45 CFR 164.526(c)(3) (Amendment of Protected Health Information).

ii. Business Associate will make any amendments to PHI in a Designated Record Set as directed by HCA or as necessary to satisfy HCA's obligations under 45 CFR 164.526 (Amendment of Protected Health Information).

13.5 **Subcontracts and other Third Party Agreements.** In accordance with 45 CFR

164.502(e)(1)(ii), 164.504(e)(1)(i), and 164.308(b)(2), Business Associate must ensure that any agents, Subcontractors, independent contractors or other third parties that create, receive, maintain, or transmit PHI on Business Associate's behalf, enter into a written contract that contains the same terms, restrictions, requirements, and conditions as the HIPAA compliance provisions in this Contract with respect to such PHI. The same provisions must also be included in any contracts by a Business Associate's Subcontractor with its own business associates as required by 45 CFR 164.314(a)(2)(b) and 164.504(e)(5).

13.6 **Obligations.** To the extent the Business Associate is to carry out one or more of HCA's obligation(s) under Subpart E of 45 CFR Part 164 (Privacy of Individually Identifiable Health Information), Business Associate must comply with all requirements that would apply to HCA in the performance of such obligation(s).

13.7 **Liability.** Within ten (10) business days, Business Associate must notify the contact identified in Subsection 13.1 of any complaint, enforcement or compliance action initiated by the Office for Civil Rights based on an allegation of violation of the HIPAA Rules and must inform HCA of the outcome of that action. Business Associate bears all responsibility for any penalties, fines or sanctions imposed against the Business Associate for violations of the HIPAA Rules and for any imposed against its Subcontractors or agents for which it is found liable.

13.8 **Breach Notification.**

13.8.1 In the event of a Breach of unsecured PHI or disclosure that compromises the privacy or security of PHI obtained from HCA or involving HCA clients, Business Associate will take all measures required by state or federal law.

13.8.2 Business Associate will notify the contact identified in Subsection 13.1 by telephone and in writing within five (5) business days of any acquisition, access, use or disclosure of PHI not allowed by the provisions of this Agreement or not authorized by HIPAA Rules or required by law that potentially compromises the security or privacy of the Protected Health Information.

13.8.3 Business Associate will notify the HCA Privacy Officer identified in Section 13.1 above by telephone or e-mail within five (5) business days of any potential Breach of security or privacy of PHI by the Business Associate or its Subcontractors or agents. Business Associate will follow telephone or e-mail notification with a written (fax or email acceptable) explanation of the Breach, to include the following: date and time of the Breach, date Breach was discovered, location and nature of the PHI, type of Breach, origination and destination of PHI, Business Associate unit and personnel associated with the Breach, detailed description of the Breach, anticipated mitigation steps, and the name, address, telephone number, fax number, and e-mail of the individual who is responsible as the primary point of contact. Business Associate will coordinate and cooperate with HCA to provide a copy of its investigation and other information requested by HCA, including advance copies of any notifications required for HCA's review before disseminating and verification of the dates notifications were sent.

13.8.4 If HCA determines that Business Associate or its Subcontractor(s) or agent(s) is responsible for a Breach of unsecured PHI:

i. requiring notification of Individuals under 45 CFR § 164.404 (Notification to Individuals), Business Associate bears the responsibility and costs for notifying the affected Individuals and receiving and responding to those Individuals' questions or requests for additional information;

ii. requiring notification of the media under 45 CFR § 164.406 (Notification to the media), Business Associate bears the responsibility and costs for notifying the media and receiving and responding to media questions or requests for additional information;

iii. requiring notification of the U.S. Department of Health and Human Services Secretary under 45 CFR § 164.408 (Notification to the Secretary), Business Associate bears the responsibility and costs for notifying the Secretary and receiving and responding to the Secretary's questions or requests for additional information; and

iv. HCA will take appropriate remedial measures up to termination of this Agreement.

13.9 Miscellaneous Provisions.

13.9.1 Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or amended.

13.9.2 Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

14. Non PHI Data Breach Notification

The Breach of non-PHI Data shared under this Agreement must be reported to the HCA Privacy Officer at PrivacyOfficer@hca.wa.gov within five (5) business days of discovery. The Receiving Party must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by applicable law or reasonable requested by HCA in order to meet its regulatory obligations.

15. Amendments and Alterations

This Agreement, or any term or condition, may be modified only by a written amendment signed by all parties. Only personnel authorized to bind each of the parties shall sign an amendment.

16. Assignment

The Receiving Party shall not assign rights or obligations derived from this Agreement to a third party without the prior, written consent of HCA and the written assumption of the Receiving Party's obligations by the third party.

17. Dispute Resolution

In the event that a dispute arises under this Agreement, the parties will make every effort to resolve the dispute informally and at the lowest level. If a dispute cannot be resolved informally a Dispute Board will determine resolution in the following manner:
(a) HCA will appoint one member to the Dispute Board and Receiving Party will appoint a second member. These first two members will select the third member;
(b) The Dispute Board will review the facts, DSA terms, and applicable statutes and rules and as quickly as reasonably possible, make a written determination of the dispute, including its analysis and reasoning for the decision based on the application of the DSA terms, and applicable statutes and rules to the facts;
(c) Participation in this dispute process must precede any judicial or quasi-judicial action and will be the final administrative remedy available to the parties.

18. Entire Agreement

This Agreement including all documents attached to or incorporated by reference, contain all the terms and conditions agreed upon by the parties. No other understandings or representations, oral or otherwise, regarding the subject matter of this Agreement, shall be deemed to exist or bind the parties.

19. Governing Law and Venue

This Agreement is governed by, and will be construed and enforced in accordance with the laws of the State of Washington. In the event of a lawsuit involving this Agreement, jurisdiction is proper only in the Superior Court of Washington, and venue is proper only in Thurston County, Washington.

20. Incorporated Documents and Order of Precedence

20.1 Each of the documents listed below is, by this reference, incorporated into this

Agreement as though fully set forth herein.

20.1.1 Exhibit A – Data Security Requirements

20.1.2 Exhibit B - User Agreement on System Usage and Non-Disclosure of Confidential Information

20.1.3 Section 4 of OCIO 141.10, *Securing Information Technology Assets Standards: Data Security* (https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology -assets.)

20.2 In the event of any inconsistency in this Contract, the inconsistency shall be resolved in the following order of precedence:

20.2.1 Applicable federal and state statutes, laws, and regulations;

20.2.2 Sections of this Data Share Agreement;

20.2.3 Attachments, Exhibits and Schedules to this Data Share Agreement.

21. Inspection

No more than once per quarter, during the term of this Agreement and for six (6) years following termination or expiration of this Agreement, HCA shall have the right at reasonable times and upon prior notice to access the Receiving Party’s records and place of business for the purpose of monitoring, auditing, and evaluating the Receiving Party’s compliance with this Agreement, and applicable laws and regulation.

22. Insurance

22.1 HCA certifies that it is self-insured under the State’s self-insurance liability program, as provided by RCW 4.92.130, and will pay for losses for which HCA is found liable.

22.2 The Receiving Party certifies that it is self-insured, is a member of a risk pool, or maintains the types and amounts of insurance identified below and shall provide certificates of insurance to that effect to HCA upon request.

22.3 Required Insurance or Self-Insured Equivalent

Commercial General Liability Insurance (CGL) – to include coverage for bodily injury, property damage, and contractual liability, with the following minimum limits: Each Occurrence - $1,000,000; General Aggregate - $2,000,000. The policy shall include liability arising out of premises, operations, independent contractors, products-completed operations, personal injury, advertising injury, and liability assumed under an insured contract. The State of Washington, HCA, their elected and appointed officials, agents, and employees shall be named as additional insureds.

22.4 Cyber Liability/Privacy Breach Response Coverage. For the term of this Agreement and 3 years following its termination or expiration, Receiving Party must maintain insurance to cover costs incurred in connection with a security incident, privacy Breach, or potential compromise of Data, including:

i. Computer forensics assistance to asses the impact of a Data Breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with Breach notification laws;
ii. Notification and call center services for individuals affected by a security incident or privacy Breach;
iii. Breach resolution and mitigation services for individuals affected by a security incident or privacy Breach, including fraud prevention, credit monitoring, and identity theft assistance; and
iv. Regulatory defense, fines, and penalities from any claim in the form of a regulatory proceeding resulting from a violation of any applicable privacy or security law(s) or regulation(s).

22.5 If any of the required policies provide coverage on a claims-made basis:

i. The retroactive date must be shown and must be before the date of the Agreement or of the beginning of Agreement work.
ii. If coverage is cancelled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the Agreement effective date, the Receiving Party must purchase "extended reporting" coverage for a minimum of 3 years after completion of Agreement work.

The State of Washington, including but not limited to HCA, must be named as additional insureds.

In the event of cancellation, non-renewal, revocation or other termination of any insurance coverage required by this Agreement, Receiving Party must provide written notice of such to HCA within one (1) Business Day of Receiving Party's receipt of such notice.

By requiring insurance herein, HCA does not represent that coverage and limits will be adequate to protect Receiving Party. Such coverage and limits will not limit Receiving Party's liability under the indemnities and reimbursements granted to HCA in this Agreement.

23. Legal Notices

23.1 The notices required in Sections 13 *HIPAA Compliance* and Section 14 *Non-PHI Data Breach Notification*, are required to be given as provided in Subsection 13.1 above.

23.2 The Points of Contact and process for System access requests are identified in Section 10 above.

23.3 Any other notice or demand or other communication required or permitted to be given under this DSA or applicable law will be effective only if it is in writing and signed by the applicable party, properly addressed, and either delivered in person, or by a recognized courier service, or deposited with the United States Postal Service as first-class mail, postage prepaid certified mail, return receipt requested, to the parties at the addresses provided in this section.

23.3.1 To Receiving Party at:

WSALPHO
Jaime Bodden
206 Tenth Avenue SE
Olympia, Washington 98501-1311

23.3.2 To HCA at:

Contract Administrator
Division of Legal Services
Health Care Authority
PO Box 42702
Olympia, Washington 98504-2702

Notices will be effective upon receipt or four (4) Business Days after mailing, whichever is earlier. The notice address and information provided above may be changed by written notice given as provided above.

24. Maintenance of Records

The Receiving Party must maintain records related to compliance with this Agreement for six (6) years after expiration or termination of this Agreement. HCA or its designee will have the right ot access those records during that six-year period for the purposes of auditing.

25. Responsibility

HCA and the Receiving Party will each be responsible for their own acts and omissions and for the acts and omissions of their agents and employees. Each party to this Agreement must defend, protect, and hold harmless the other party, or any of the other party's agents, from and against any loss and all claims, settlements, judgments, costs, penalties, and expenses, including reasonable attorney fees, arising from any willful misconduct or dishonest, fraudulent, reckless, unlawful, or negligent act or omission of the first party, or agents of the first party, while performing under the terms of this Agreement, except to the extent that such losses result from the willful misconduct, or dishonest, fraudulent, reckless, unlawful, or negligent act or omission on the part of the second party. Each party agrees to promptly notify the other party in writing of any claim and provide the other party the opportunity to defend and settle the claim.

26. Severablility

The provisions of this Agreement are severable. If any provision of this Agreement is held invalid by any court, that invalidity will not affect the other provisions of this Agreement and the invalid provision will be considered modified to conform to the existing law

27. Survivability

The terms and conditions contained in this Agreement that by their sense and context are intended to survive the expiration or other termination of this Agreement must survive. Surviving terms include, but are not limited to: *Constraints on Use of Data, Security of Data, Systems Access, Data Confidentiality and Non-Disclosure of Data, HIPAA Compliance, Non PHI Data Breach Notification, Dispute Resolution, Inspection, Maintenance of Records,* and *Responsibility*.

28. Term and Termination

28.1 Term. This Agreement will begin on October 15, 2015 or date of execution, whichever is later, and continue through August 15, 2016 unless terminated sooner, as provided in this Section.

HCA, at its sole discretion, may extend this MOU for two (2) additional one-year periods unless terminated sooner as provided herein.

28.2 Termination for Convenience. Either HCA or the Receiving Party may terminate this Agreement for convenience with thirty (30) days' written notice to the other. However, once Data is accessed by the Receiving Party, this Agreement is binding as to the confidentiality, use and disposition of all Data received as a result of access, unless otherwise agreed in writing.

28.3 Termination for Default. HCA may terminate this Agreement for default, in whole or in part, by written notice to the Receiving Pary, if HCA has a reasonable basis to believe that the Receiving Party has: (1) failed to perform under any provision of this Agreement; (2) violated any law, regulation, rule, or ordinance applicable to this Agreement; and/or (3) otherwise breached any provision or condition of this Agreement.

Before HCA terminates this Agreement for default, HCA will provide the Receiving Party with written notice of its noncompliance with the Agreement and provide the Receiving Party a reasonable opportunity to correct its noncompliance. If the Receiving Party does not correct the noncompliance within the period of time specified in the written notice of noncompliance, HCA may then terminate the Agreement. HCA may terminate the Agreement for default without such written notice and without opportunity for correction if HCA has a reasonable basis to believe that a Client's health or safety is in jeopardy. The determination of whether or not the Receiving Party corrected the noncompliance will be made by HCA, in its sole discretion.

29. Waiver

Waiver of any breach or default on any occasion shall not be deemed to be a waiver of any subsequent breach or default. Any waiver shall not be construed to be a modification of the terms and conditions of this Agreement.

30. Signatures and Counterparts

The signatures on page 2 of this document indicate agreement between the parties. The parties may execute this Agreement in multiple counterparts, each of which is deemed an original and all of which constitute only one agreement.

Exhibit A – Data Share Agreement

Data Security Requirements

Exhibit A – Data Security Requirements

1. Definitions

In addition to the definitions set out in section 3, *Definitions*, of the Data Share Agreement, the definitions below apply to this Exhibit.

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.

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

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

(c) 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. Data Transmission

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 Data

The Receiving Party agrees to store and protect Confidential Information as described:

a. **Data at Rest:**

(1) 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.

(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 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. Data Segregation

HCA's Data received under this DSA must be segregated or otherwise distinguishable from non-HCA Data. This is to ensure that when no longer needed by the Receiving Party, 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.

a. HCA's Data 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.

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

5. Data Disposition

When the Confidential Information is no longer needed, except as noted below, the Data 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).

a. For HCA's Confidential Information 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 3, 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.

Exhibit B – Data Share Agreement

User Agreement on System Usage
and
Non-Disclosure of Confidential Information

User Agreement on Non-Disclosure of Confidential Information

Your organization has entered into a Data Share Agreement with the state of Washington Health Care Authority (HCA) that will allow you access to data and records that are deemed Confidential Information as defined below. Prior to accessing this Confidential Information you must sign this *User Agreement on Non-Disclosure of Confidential Information.*

Confidential Information

“Confidential Information” means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information includes, but is not limited to, Protected Health Information and Personal Information. For purposes of the pertinent Data Share Agreement, Confidential Information means the same as “Data.”

“Protected Health Information” means information that relates to: the provision of health care to an individual; the past, present, or future physical or mental health or condition of an individual; or the past, present or future payment for provision of health care to an individual and includes demographic information that identifies the individual or can be used to identify the individual.

“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, driver license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

Regulatory Requirements and Penalties

State laws (including, but not limited to, RCW 74.04.060, RCW 74.34.095, and RCW 70.02.020) and federal regulations (including, but not limited to, HIPAA Privacy and Security Rules, 45 CFR Part 160 and Part 164; Confidentiality of Alcohol and Drug Abuse Patient Records, 42 CFR, Part 2; and Safeguarding Information on Applicants and Beneficiaries, 42 CFR Part 431, Subpart F) prohibit unauthorized access, use, or disclosure of Confidential Information. Violation of these laws may result in criminal or civil penalties or fines.

User Assurance of Confidentiality

In consideration for HCA granting me access to the Confidential Information that is the subject of this Agreement, I agree that I:

1. Will access, use, and disclose Confidential Information only in accordance with the terms of this Agreement and consistent with applicable statutes, regulations, and policies.
2. Have an authorized business requirement to access and use the Confidential Information.
3. Will not use or disclose any Confidential Information gained by reason of this Agreement for any commercial or personal purpose, or any other purpose that is not directly connected with this Agreement.
4. Will not use my access to look up or view information about family members, friends, the relatives or friends of other employees, or any persons who are not directly related to my assigned job duties.
5. Will not discuss Confidential Information in public spaces in a manner in which unauthorized individuals could overhear and will not discuss Confidential Information with unauthorized individuals, including spouses, domestic partners, family members, or friends.
6. Will protect all Confidential Information against unauthorized use, access, disclosure, or loss by employing reasonable security measures, including physically securing any computers, documents, or other media containing Confidential Information and viewing Confidential Information only on secure workstations in non-public areas.
7. Will not make copies of Confidential Information, or print system screens unless necessary to perform my assigned job duties and will not transfer any Confidential Information to a portable electronic device or medium, or remove Confidential Information on a portable device or medium from facility premises, unless the information is encrypted and I have obtained prior permission from my supervisor.
8. Will access, use or disclose only the “minimum necessary” Confidential Information required to perform my assigned job duties.
9. Will not distribute, transfer, or otherwise share any software with anyone.
10. Will forward any requests that I may receive to disclose Confidential Information to my supervisor for resolution and will immediately inform my supervisor of any actual or potential security breaches involving Confidential Information, or of any access to or use of Confidential Information by unauthorized users.
11. Understand at any time, HCA may audit, investigate, monitor, access, and disclose information about my use of the Confidential Information and that my intentional or unintentional violation of the terms of this Agreement may result in revocation of privileges to access the Confidential Information, disciplinary actions against me, or possible civil or criminal penalties or fines.
12. Understand that my assurance of confidentiality and these requirements will continue and do not cease at the time I terminate my relationship with my employer.

Signature

Print User’s Name	User Signature	Date
Jaime Bodden	DocuSigned by: Jaime Bodden EC3521C1809E460...	12/22/2017