


**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

	Data Share Agreement [Name of System]		HCA Contract Number: KXXX
			Receiving Party Contract Number: _____
<i>This Data Share Agreement ("Agreement" or "DSA") is made by and between the state of Washington Health Care Authority ("HCA") and the party whose name appears below, ("Receiving Party")</i>			
Receiving Party Name		Receiving Party doing business as (DBA)	
Receiving Party Address		Receiving Party Contact Name, Title	
Receiving Party Contact Telephone		Receiving Party Contact Email Address	
HCA Program		HCA Division/Section	
HCA Contact Name, Title		HCA Contact Address	
		<i>626 8th Avenue SE, PO Box 4xxxx Olympia, WA 98504-xxxx</i>	
HCA Contact Telephone		HCA Contact Email Address	
<i>The parties signing below warrant that they have read and understand this Agreement, and have authority to execute this Agreement. This Agreement shall be binding on HCA only upon signature by HCA.</i>			
Receiving Party Signature	Printed Name and Title	Date Signed	
HCA Signature	Printed Name and Title	Date Signed	
	<i>Melanie Anderson, Contracts Administrator</i>		

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

Table of Contents

1. Purpose of the DSA.....	3
2. Justification for Data Sharing	3
3. Definitions.....	3
4. Authority to Access Data.....	5
5. Description of Data to be Shared	5
6. Data Classification.....	6
7. Constraints on Use of Data	6
8. Security of Data.....	7
9. Data Confidentiality and Non-Disclosure	7
10. Data or Systems Access	8
11. Public Disclosure Requests.....	9
12. Data Shared with Subcontractors	9
13. HIPAA Compliance.....	9
14. Non PHI Data Breach Notification	13
15. Amendments and Alterations	13
16. Assignment.....	13
17. Dispute Resolution	13
18. Entire Agreement	14
19. Governing Law and Venue.....	14
20. Incorporated Documents and Order of Precedence	14
21. Inspection	14
22. Insurance.....	14
23. Legal Notices.....	15
24. Maintenance of Records	15
25. Responsibility	15
26. Severability	15
27. Survivability	15
28. Term and Termination	16
29. Waiver	16
30. Signatures and Counterparts	16
1. Definitions.....	18
2. Data Transmitting	18
3. Protection of Data.....	18
4. Protection of Data Stored on Portable Devices or Media	20
5. Data Segregation	20
6. Data Disposition	21

Exhibit A: Data Security Requirements

Exhibit B: Receiving Party User Agreement on System Usage and Non-Disclosure of Confidential Information

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

1. Purpose of the DSA

The purpose of this Data Share Agreement (DSA) is to provide (enter detailed description of the DSA purpose).

Example: The data must be used for analysis purposes only to prepare required annual business summaries published by Receiving Party.

2. Justification for Data Sharing

The Data to be shared under this DSA is necessary for Receiving Party to (enter detailed explanation of why the data is needed).

3. Definitions

Note: Please carefully read the definitions and ensure they are applicable to the DSA. Can be deleted or added as deemed necessary for the final DSA.

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

“Agreement” means this Data Share Agreement that is the entire written agreement between HCA and the Receiving Party and includes all documents attached or incorporated by reference.

“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.”

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

“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.

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

“**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

[Enter the specific RCW, WAC, Bill, etc that allows access to the data by the other entity and a summary description of that statute. This information to be provided by the party receiving the data.]

pursuant to the authority granted by one or more of the following, RCW 39.34, RCW 70.47 and 45 CFR 164.512(k)(6).

Example:

RCW 74.39A.090 mandates that DSHS contract with Area Agencies on Aging (AAA's) to provide case management services to individuals receiving Medicaid personal care services and to reassess and reauthorize these individuals for Medicaid personal care services or other home and community services as defined by the statute. Also, in accord with Section 2703 of the Patient Protection and Affordable Care Act of 2010, and the State Plan Amendments of July 1 and October 1, 2013, Washington has established the Health Home community based program to provide intensive care coordination services to high-cost, high-need Medicaid and Medicaid/Medicare beneficiaries to ensure that services delivered are integrated and coordinated across medical, mental health, chemical dependency and long term care services and supports. In order to effectively administer these programs and services, the AAA's must have access to client data, and to the ProviderOne and PRISM systems.

5. Description of Data to be Shared

NOTE: *Include a description of the data that is requested, including data elements, time frames and format of the data, as necessary. Specify if the data provided can be linked to other data and under what conditions, as necessary. Also specify whether the data will actually be provided to the Receiving Party, or whether they will just access the data.*

Example: *Data shared will include the data contained in HCA's agency's internal database that is described in this Agreement and will be updated through an automated process that runs daily on a server operated at . . .).*

Data to be shared includes:

- Data Element [enter data elements]
- Time Frame [enter time frame]
- Format of the Data [enter format for the data exchange]

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

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:

Check the appropriate box(es)

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.

Note: If the data includes PHI, Contractor will be required to complete a Business Associate Agreement (BAA).

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 **[identify the purpose(s)]** 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 ad hoc analyses or other use of the Data is not permitted without 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.

If Applicable

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

- 7.5. 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 must be reviewed and approved by HCA prior to publication or presentation.

If Applicable

- 7.6. Receiving Party is **not** authorized to update or change any data in the [enter SYSTEM name], and any updates or changes will be cause for immediate termination of this Agreement.

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:

- a) Allowing access only to staff that have an authorized business requirement to view the Confidential Information.
- b) 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*.

9. Data Confidentiality and Non-Disclosure

9.1. Data Confidentiality.

The Receiving Party shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Data Share Agreement for any purpose that is not directly connected with the purpose and justification of this DSA 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

- a) Employee Instruction. The Receiving Party shall 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 DSA before gaining access to the Data identified herein. The Receiving Party shall also instruct and make any new employee aware of the use restrictions and protection requirements of this DSA before they gain access to the Data.
- b) [Optional] Annual Reminder. Receiving Party shall provide an annual reminder to staff of the use restrictions and protection requirements of this DSA.
- c) User Agreement on System Usage and Non-Disclosure of Confidential Information. 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 shall retain the original *User Agreement on System Usage and Non-Disclosure of Confidential Information* on file for a minimum of six years and shall make the document available to HCA upon request.

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

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

NOTE: *Include a description of how the data will be accessed.*

If DSA is not about access to a system, describe how the data will be supplied to the Receiving Party.

Example: *Data access will be via terminal emulation software to be loaded on the appropriate Contractor staff workstations. HCA will grant access permissions required to access the data defined above.*

Example: *The Receiving Party may request access for specific users with a need to know to view Data in the Identify System(s) under this DSA. The access request must be signed by the requester's manager and sent by the Receiving Party's Point of Contact to the HCA Point of Contact, as identified below. Subcontractors may request access for specific users with a need to know to view Data in the identified System(s) by signing the access request and sending it to the Receiving Party to send to the HCA Point of Contact. HCA will accept access requests only from the Receiving Party.*

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 _____

Address _____

Telephone: _____

E-mail: _____

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 _____

Address _____

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

Telephone: _____

E-mail: _____

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

Use only if the Receiving Party is a public entity subject to Chapter 42.56 RCW.

If the Receiving Party receives a public records request under Chapter 42.56 RCW for any Data subject to this DSA, Receiving Party agrees to notify and discuss the request with the HCA Public Disclosure Officer prior to disclosing the requested records. The HCA Public Disclosure Officer can be contacted at PublicDisclosure@hca.wa.gov. The Receiving Party further agrees to provide the HCA with a minimum of ten (10) business days to initiate legal action to secure a protective order under RCW 42.56.540.

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

Use this section only if not entering into a separate Business Associate Agreement.

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:

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

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 shall 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:
- a) **Duty to Protect PHI.** Business Associate shall protect PHI from, and shall 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.
 - b) **Minimum Necessary Standard.** Business Associate shall 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).
 - c) **Disclosure as Part of the Provision of Services.** Business Associate shall only Use or disclose PHI as necessary to perform the services specified in this Agreement or as required by law, and shall 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.
 - d) **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.
 - e) **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.
 - f) **Impermissible Use or Disclosure of PHI.** Business Associate shall 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 shall mitigate, to the extent practicable, any harmful effect resulting from the impermissible Use or disclosure.
 - g) **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 shall 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

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

Business Associate do not end the violation, Business Associate shall terminate the Subcontract, if feasible.

- h) 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.
- i) Consent to Audit. Business Associate shall 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.
- j) 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 shall:
 - 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.
- k) Survival. The obligations of the Business Associate under this section shall survive the termination or expiration of this Agreement.

13.4. Individual Rights.

- a) Accounting of Disclosures.
 - i. Business Associate shall 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 shall 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 shall 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 shall 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.

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

- b) Access
 - i. Business Associate shall 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's 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 shall 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.
- c) Amendment.
 - i. If HCA amend, in whole or in part, a record or PHI contained in an Individual's Designated Record Set and HCA have 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 shall 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 shall 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 shall 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.**
 - a) 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.
 - b) 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.
 - c) 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

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

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.

- d) 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.

- a) Regulatory References. A reference in this Agreement to a section in the HIPAA Rules means the section as in effect or amended.
- b) Interpretation. Any ambiguity in this Agreement shall be interpreted to permit compliance with the HIPAA Rules.

14. Non PHI Data Breach Notification

The compromise or potential compromise 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 law or HCA.

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:

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

(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

The laws of the State of Washington govern this Agreement. In the event of a lawsuit involving this Data Share Agreement, venue shall be 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.

- a) Exhibit A – Data Security Requirements
- b) Exhibit B - User Agreement on System Usage and Non-Disclosure of Confidential Information

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

- a) Applicable federal and state statutes, laws, and regulations;
- b) Sections of this Data Share Agreement;
- c) Attachments, Exhibits and Schedules to this Data Share Agreement.

21. Inspection

During the term of this Agreement and for one (1) year 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,

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

HCA, their elected and appointed officials, agents, and employees shall be named as additional insureds.

Note: *Consider the need for Cyber Liability Insurance*

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.
- a) To Receiving Party at:
- Name
Title
Address
- b) To HCA at:
- Contract Administrator
Division of Legal Services
Health Care Authority
P. O. 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 shall maintain records related to compliance with this Agreement for six (6) years after expiration or termination of this Agreement.

25. Responsibility

Each party to this Agreement shall be responsible for the negligence of its officers, employees, and agents in the performance of this Agreement.

26. Severability

The provisions of this Agreement are severable. If any provision of this Agreement is held invalid by any court, that invalidity shall not affect the other provisions of this Data Sharing Agreement and the invalid provision shall 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 shall 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.*

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

28. Term and Termination

28.1. Term. This Agreement shall begin on *[specify start date]* or date of execution, whichever is later, and continue through *[specify end date]* unless terminated sooner, as provided in this Section. **Optional** Thereafter this Agreement will automatically renew for subsequent one-year terms unless either HCA or the Receiving Party give thirty (30) days' advance written notice to the other of intent to terminate the Agreement.

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 Party, 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.

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 below 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 Security Requirements

DRAFT

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

Exhibit A – Data Security Requirements

1. Definitions

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

- a. “Hardened Password” means a string of at least eight 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.
- b. “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.
- c. “Transmitting” means the transferring of data electronically, such as via email.
- d. “Trusted Systems” means the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Data 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.
- e. “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 Transmitting

- a. When transmitting HCA’s Confidential Information electronically, including via email, the Data must be protected by:
 - a) Transmitting the Data within the State Governmental Network (SGN) or Receiving Party’s internal network; or
 - b) Encrypting any Data that will be transmitted outside the SGN or Receiving Party’s internal network with 128-bit Advanced Encryption Standard (AES) encryption or better. This includes transit over the public Internet.
- b. When transmitting HCA’s Confidential Information via facsimile (fax), the Receiving Party shall verify the fax recipient’s fax number and shall communicate with the intended fax recipient before transmission to ensure that the fax will be received only by the intended fax recipient.
- c. 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 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.

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

- 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 that is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- (1) **Data Destruction:** 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 the above paragraph. Destruction of the Data as outlined in Section 5: *Data Disposition* of this Exhibit may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.
- c. **Removable Media, including Optical discs (CDs or DVDs) in local workstation optical disc drives and which *will not be transported out of a secure area*.** Confidential Information provided by HCA on removable media, such as optical discs or USB drives, which will be used in local workstation optical disc drives or USB connections will be encrypted with 128-bit AES encryption or better. When not in use for the contracted purpose, such discs must be locked in a drawer, cabinet or other container to which only Authorized Users have the key, combination or mechanism required to access the contents of the container. Workstations that access Confidential Information on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.
- d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers and which *will not be transported out of a secure area*.** Confidential Information provided by HCA on optical discs which will be attached to network servers will be encrypted with 128-bit AES encryption or better. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has been authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached 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.
- e. **Paper documents.** Any paper records containing Confidential Information must be protected by storing the records in a secure 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.
- f. **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. Receiving Party shall have established and documented termination procedures for existing staff with access to the Data. These procedures must be provided upon request. The Receiving Party will notify HCA's Point of Contact within five (5) business days whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Receiving Party, and whenever an Authorized User's duties change such that the user no longer requires access. (See Section 10 of the Agreement, *Data or Systems Access*)
- g. **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. Receiving Party shall have established and documented termination procedures for existing staff with access to the

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

Data. These procedures must be provided upon request. Receiving Party will notify HCA's Point of Contact within five (5) business days whenever an Authorized User in possession of such credentials is terminated or otherwise leaves the employ of the Receiving Party and whenever an Authorized User's duties change such that the user no longer requires access. (See Section 10 of the Agreement, *Data or Systems Access*)

4. Protection of Data Stored on Portable Devices or Media

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 as provided in this Section 4.

Portable devices are any small computing device that can be transported, including 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.

Portable 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); magnetic media (e.g. floppy disks, tape, Zip or Jaz disks); USB drives; or flash media (e.g., CompactFlash, SD, MMC).

- c. For Data stored on Portable devices or media, Receiving Party must
 - a. Encrypt the Data with a key length of at least 128 bits using an industry standard algorithm, such as AES;
 - b. Ensure that portable devices such as flash drives are FIPS Level 2 compliant;
 - c. Control access to the devices with a unique user ID and password or stronger authentication method such as a physical token or biometrics;
 - d. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. The maximum period of inactivity is 20 minutes.
 - e. 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;
 - c) Maintaining an inventory; and
 - d) Ensuring that when being transported outside of a Secured Area, portable devices and media with Data are under the physical control of an Authorized User.

5. 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:
 - a) on media (e.g. hard disk, optical disc, tape, etc.) which will contain no non-HCA Data; or
 - b) in a logical container on electronic media, such as a partition or folder dedicated to HCA's Data; or
 - c) in a database that will contain no non-HCA Data; or
 - d) within a database and will be distinguishable from non-HCA Data by the value of a specific field or fields within database records; or
 - e) When stored as physical paper documents, physically segregated from non-HCA Data in

**ATTACHMENT 2
DRAFT DATA SHARE AGREEMENT**

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.

6. Data Disposition

When the Confidential Information is no longer needed, except as noted in 3.b(1) above, the Data must be returned to HCA or destroyed. 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 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 Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with Category 3 and higher Data	Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing confidential information requiring special handling (e.g. protected health information)	On-site 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

Exhibit B

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

User Agreement on *System Usage and 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 System Usage and Non-Disclosure of Confidential Information (Agreement).

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.

“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 ProviderOne, or other systems and the Confidential Information in those systems**, 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 HCA systems and Confidential Information.
3. Will not use or disclose any Confidential Information gained by reason of this Agreement for any commercial or personal purpose, research, or any other purpose that is not directly connected with client care coordination and quality improvement activities.
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 protect my HCA systems User ID and password and not share them with anyone or allow others to use any HCA system logged in as me.
10. Will not distribute, transfer, or otherwise share any HCA software with anyone.
11. 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.
12. Understand at any time, HCA may audit, investigate, monitor, access, and disclose information about my use of the systems and that my intentional or unintentional violation of the terms of this Agreement may result in revocation of privileges to access the systems, disciplinary actions against me, or possible civil or criminal penalties or fines.
13. 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