Washington State Health Care Authority	**Data Share Agreement Three Party Agreement for PRISM Access**	HCA Contract Number: K8262 Receiving Party Contract Number: DSHS Contract # 2491-56969 Kitsap Contract # KC-202-26

THIS DATA SHARE AGREEMENT is made by and between the Washington State Health Care Authority (HCA), Washington State Department of Social and Health Services (DSHS) and Kitsap County (Receiving Party).

RECEIVING PARTY NAME		RECEIVING PARTY DOING BUSINESS AS (DBA)		
Kitsap County		Kitsap County Area Agency on Aging Division of Aging and Long-Term Care (ALTC)		
RECEIVING PARTY ADDRESS 611 Division St, MS-5	STREET	CITY Port Orchard	STATE WA	ZIP CODE 98366
RECEIVING PARTY CONTACT Stacey Smith	RECEIVING PARTY TELEPHONE (360) 337-5624	RECEIVING PARTY E-MAIL ADDRESS sasmith@kitsap.gov		
DISCLOSING PARTY NAME DSHS Research and Data Analysis Division		DISCLOSING PARTY DOING BUSINESS AS (DBA)		
DISCLOSING PARTY ADDRESS 1115 Washington St SE	STREET	CITY Olympia	STATE WA	ZIP CODE 98504
DISCLOSING PARTY CONTACT Tiffany Maples	DISCLOSING PARTY TELEPHONE (360) 902-0749	DISCLOSING PARTY E-MAIL ADDRESS tiffany.maples2@dshs.wa.gov		

HCA PROGRAM (DISCLOSING PARTY) Data Acquisition, Transformation, and Analytics	HCA DIVISION/SECTION Strategy, Policy and Innovation
HCA CONTACT NAME AND TITLE Bailey McDonald, Management Analyst	HCA CONTACT ADDRESS Health Care Authority 626 8th Avenue SE Olympia, WA 98504
HCA CONTACT TELEPHONE (360) 725-1031	HCA CONTACT E-MAIL ADDRESS bailey.mcdonald@hca.wa.gov

CONTRACT START DATE	CONTRACT END DATE	TOTAL MAXIMUM CONTRACT AMOUNT
Date of Execution	December 31, 2027	0.00

PURPOSE OF CONTRACT:

The purpose of this Data Share Agreement (DSA) is to provide pertinent client-level Medicaid and Medicare Data to those Receiving Party staff and Subcontractors with a need- to-know client-level Data in order to coordinate, improve quality and manage services for their Medicaid Clients.

The parties signing below warrant that they have read and understand this DSA and have authority to execute this DSA. This DSA will be binding on a Party only upon signature by all Parties.

RECEIVING PARTY SIGNATURE	PRINTED NAME AND TITLE	DATE
	Oran Root, Chair	4/13/26
DISCLOSING PARTY SIGNATURE Signed by: Amel Alsalman	PRINTED NAME AND TITLE Amel Alsalman Procurement Program Contracts Manager	DATE 4/28/2026
HCA SIGNATURE DocuSigned by: Andria Howerton F2EF77E93FBC4D7...	PRINTED NAME AND TITLE Andria Howerton HCA Deputy Contracts Administrator	DATE 4/17/2026

TABLE OF CONTENTS

1. Background

HCA and DSHS work together to encourage care coordination and quality improvement activities for Medicaid clients across Medicaid health care delivery systems (medical, behavioral health and long-term care services and supports). DSHS and HCA also sponsor and/or support quality improvement initiatives that require providing client-level data in hardcopy and/or electronic form to AAAs and/or AAA Subcontractors. This Data Share Agreement (DSA) outlines the requirements for use of client level Medicaid and Medicare data emanating from both HCA and DSHS for care coordination and quality improvement purposes.

HCA is designated the single state Medicaid entity by the federal government, Centers for Medicare and Medicaid Services (CMS). CMS requires a data share agreement incorporating their data use requirements for use of Medicare data between the single state Medicaid entity and direct Medicaid subcontractors, in order to use client-level CMS Medicare data for care coordination and quality improvement purposes. The *Medicare Data Use Requirements Documents* are attached in Exhibit E.

HCA is responsible for ProviderOne, Washington's federally certified Medicaid Management Information System (MM IS) that provides information on Client eligibility, managed care and fee-for service medical claims Data, Client-related correspondence, prior authorizations for Medicaid Clients receiving Medicaid (Title XIX) personal care services or other home and community services, as well as Provider scheduling and payment Data, which vendors of Specialized / Durable Medical Equipment have a Core Provider Agreement with HCA, and which Providers are taking Medicaid Clients.

DSHS is responsible for PRISM, a secure web-based clinical decision support tool integrating HCA, DSHS and Medicare data that shows administrative and assessment data for each Medicaid client and is organized to identify care coordination opportunities.

DSHS contracts with Area Agencies on Aging (AAAs), local organizations that develop and promote services and options to maximize independence for elders, adults with disabilities, and family caregivers, to provide case management services to Medicaid Clients. AAAs further subcontract with local governmental and non-profit organizations to provide services to Medicaid Clients.

2. Purpose of the DSA

The purpose of this Data Share Agreement (DSA) is to provide pertinent client-level Medicaid and Medicare Data to those Receiving Party staff and Subcontractors with a need- to-know client-level Data in order to coordinate, improve quality and manage services for their Medicaid Clients.

3. Justification for Data Sharing

The Data to be accessed under this DSA is necessary for Receiving Party to provide care coordination and quality improvement and case management services for individuals receiving Medicaid services. In order to effectively administer services, the Receiving Party must have access to Client Data, and to certain HCA and DSHS information systems, specifically ProviderOne and PRISM.

4. Definitions

"Agencies" means either the state of Washington Department of Social and Health Services (DSHS) or the state of Washington Health Care Authority ("HCA") or both of them and includes any division, section, office, unit, officers or other officials lawfully representing DSHS or HCA.

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

"Business Associate" means a Business Associate as defined in 45 C.F.R. § 160.103, who performs or assist 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, Subcontracts, third party contractors, volunteers, or directors.

"Business Associate Agreement" or **"BAA"** means the HIPAA Compliance section of this DSA, Section 17, and includes the Business Associate provisions required by the U.S. Department of Health and Human Services, Office for Civil Rights.

"Breach" means the acquisition, access, use, or disclosure of Data in a manner not permitted under law, including but not limited to the HIPAA Privacy Rule which compromises the security or privacy of the Protected Health Information, with the exclusions and exceptions listed in 45 C.F.R. 164.402.

"C.F.R." means the Code of Federal Regulations. All references in this DSA to C.F.R. chapters or sections will include any successor, amended, or replacement regulation. The C.F.R. may be accessed at http://www.ecfr.gov/cgi-bin/ECFR?page=browse

"Client" means an individual who is eligible for or receiving services through HCA program(s).

"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 8, *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 HCA individual designated to receive legal notices and to administer, amend, or terminate this DSA.

"Contract Manager" means the individual identified in the table below who will provide oversight of the activities conducted under this DSA.

"Covered Entity" means HCA, which is a Covered Entity as defined in 45 C.F.R. § 160.103, in its conduct of covered functions by its health care components.

"Data" means the information that is disclosed or exchanged as described by this DSA. For purposes of this DSA, Data means the same as "Confidential Information," "Personal Information," and "Protected Health Information" or "PHI."

"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.

"Disclosed Data" means Data that has been released, transferred, made accessible, or divulged in any other manner of information outside the entity holding the information.

"Disclosing Party" refers to either HCA, DSHS, or both, when engaged in the Disclosure of Data to Receiving Party, and includes the entities owners, members, officers, directors, partners, trustees, employees, and Subcontractors and their owners, members, officers, directors, partners, trustees, and employees.

"Disclosing Parties" means both HCA and DSHS when both HCA-supplied and DSHS-supplied Data is disclosed to Receiving Party. It may also mean both HCA and DSHS collectively when jointly owned Data (generated by PRISM) is Disclosed to Receiving Party, and includes the entities' owners, members, officers, directors, partners, trustees, employees, and Subcontractors and their owners, members, officers, directors, partners, trustees, and employees.

"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.

"DSHS" means the state of Washington Department of Social and Health Services (DSHS), and the section unit or other entity of DSHS as defined below, and any of the officers or other officials lawfully representing those part of DSHS defined below.

"Electronic Protected Health Information" or **"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 C.F.R. § 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 amended 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 C.F.R. 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 C.F.R. § 164.502(g).

"Limited Data Set(s)" means a data set that meets the requirements of 45 C.F.R. §§ 164.514(e)(2) and 164.514(e)(3).

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

"Party" or "Parties" refers to one or more of the signatories to this DSA. The term "the Parties" refers to all signatories: HCA, DSHS, and Receiving Party.

"Permissible Use" means only those uses authorized in this DSA and as specifically defined herein.

"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 (including or excluding zip code), telephone numbers, social security numbers, driver's license numbers, credit card numbers, any other identifying numbers, and any financial identifiers.

"PRISM" means the Predictive Risk Intelligence System. which is a DSHS-secure web-based predictive modeling and clinical decision support tool that tracks medical, behavioral health, and long-term care service data, using it to predict an enrollee's twelve-month medical services utilization.

"PRISM Administrator" means the RDA employee with designated responsibility for activating, monitoring, reviewing, and terminating access to PRISM.

"PRISM Lead" means the Receiving Party employee who will act as liaison with the PRISM Administrator for purposes of validating business need for PRISM access and registering/ deactivating PRISM accounts, for training content regarding PRISM navigation, use of data, and privacy and security, and for any audits under this DSA.

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

"Protected Health Information" or **"PHI"** 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 past, present or future payment for provision of health care to an individual. 45 C.F.R. 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 C.F.R. 160.103. PHI is information transmitted, maintained, or stored in any form or medium. 45 C.F.R. 164.501. PHI does not include education records covered by the Family Educational Right and Privacy Act, as amended, 20 USC 1232g(a)(4)(B)(iv).

"RCW" means the Revised Code of Washington. All references in this DSA to RCW chapters or sections will 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 DSA, and includes the entity's owners, members, officers, directors, partners, trustees, employees, and Subcontractors and their owners, members, officers, directors, partners, trustees, and employees.

"Security Awareness Program" or **"SAP"** means a formal program with the goal of training users on how to recognize potential security vulnerabilities, exploits and threats to an organization's information technology infrastructure, along with how to avoid situations that may put an organization's Data at risk.

"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 a person or entity that is not in the employment of the Receiving Party, who is performing services or 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 DSA to USC chapters or sections will include any successor, amended, or replacement statute. The USC may be accessed at http://uscode.house.gov/

"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 DSA to WAC chapters or sections will include any successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at: http://apps.leg.wa.gov/wac/.

5. Description of Data to be Shared / Data Licensing Statements

Data Licensing Statements are the written statements that determine the following issues, at a minimum:

a. Identification of the purpose of the file;

b. Identification of costs (if any)

c. Identification of transmission method; and

d. Identification of the file layout.

There must be at least one Data Licensing Statement attached hereto, but more than one Data Licensing Statement may be included or incorporated into this DSA at different times. Each Data Licensing Statement is incorporated into this DSA by using the same Attachment reference letter (A) and then further marking it with sequential identifying numbers (A1, A2, A3).

6. PRISM Access Requirements

6.1. The Receiving Party must access PRISM through SecureAccessWashington (SAW), or through another method of secure access approved by HCA and DSHS.

6.2. The Receiving Party must identify a PRISM Lead who will act as a liaison with the PRISM Administrator for purposes of validating business needs for PRISM access and registering/deactivating PRISM accounts, for training content regarding PRISM navigation, use of data, privacy and security, and for any audits under this DSA.

6.3. PRISM Access Contact Information:

RECEIVING PARTY PRISM Lead		**PRISM Administrator**	
Name:	Adeanne Hume	Name:	Pierre Katona
Title:	Case Management Supervisor	Title:	PRISM Administrator

Address:	Division of Aging and LTC 614 Division St. MS-5 Port Orchard, WA 98366	Address:	1115 Washington St SE Olympia, WA 98504
Phone:	(360) 337-5700	Phone:	(360) 902-0809
Email:	ahume@kitsap.gov	Email:	PRISM.admin@dshs.wa.gov

6.4. The Receiving Party may change its PRISM Lead contact information or appoint one or more backups for the PRISM Lead role by written notice to the PRISM Administrator (email acceptable).

6.5. The PRISM Lead will notify the PRISM Administrator within five (5) business days whenever an Authorized User who has access to the Data is no longer employed by the Receiving Party or whenever an Authorized User's duties change such that they no longer require access to the Data.

6.6. Periodically and annually, the PRISM Administrator will send the PRISM Lead a spreadsheet of Receiving Party's current PRISM Authorized Users. The PRISM Lead must confirm the business need for continued PRISM access for the Authorized Users, verify that the required annual training is up to date, update the information in the spreadsheet as required, and return the updated spreadsheet to the PRISM Administrator within thirty (30) days of receipt.

6.7. The Receiving Party access to PRISM is tracked and monitored. The PRISM Administrator has the right at any time to suspend or terminate access privileges for unusual or potentially unauthorized activity, to conduct audits of PRISM access and use, and to investigate possible violations of this Agreement and/or violations of federal and state laws and regulations governing access to Personal Information and Protected Health Information.

6.8. The PRISM Administrator does not allow shared user IDs and passwords for use with Confidential Information or to access PRISM. The Receiving Party shall ensure that only Authorized Users access and use PRISM, use only their own user ID and password to access PRISM, and do not allow employees, agents or Subcontractors who are not authorized to borrow a user ID or password to access any systems.

6.9. No Receiving Party Subcontractors will be allowed access to PRISM under this DSA.

7. System Access Request Process

The Receiving Party may request to view PRISM information under this DSA for up to ten (10) Authorized Users with a need to know who will be performing activities related to case management and care coordination for older adults on Receiving Party's caseloads.

PRISM Access for the Receiving Party's Authorized Users may be requested in two ways as outlined in section 7.1 (Option A) and 7.2 (Option B) below. When the Receiving Party's

user base increases to more than twenty (20) users, Receiving Party must migrate as soon as possible to Option B.

7.1. Option A: Submit a complete PRISM Access Request Form.

7.1.1 The prospective user must fill out *User Registration Information* section of the PRISM Access Request Form in Exhibit C and sign the *User Agreement and Non-Disclosure of Confidential Information* page.

7.1.2 The PRISM Lead must complete the *Requesting Organization* section of the PRISM Access Request Form and sign as the *Authorizing Signature.*

7.1.3 Once the PRISM Access Request Form is completed, the PRISM Lead must email a PDF copy of the signed form to the PRISM Administrator

7.2. Option B: Submit evidence of completion of an online Learning Management System (LMS) training course with electronic attestation to the terms of the PRISM Access Request Form.

7.2.1 The Receiving Party may sponsor and maintain an online interactive LMS course that provides training in the appropriate use of PRISM and requires the prospective user's electronic attestation to the terms of the *User Agreement and Non-Disclosure of Confidential Information* as a condition for course completion.

7.2.2 The prospective user's supervisor is responsible for ensuring the employee has completed the required LMS IT Security and HIPPA training before enrolling in the LMS course described in 7.2(a) above. By approving an employee for this training, the supervisor affirms that the employee has completed the prerequisite training and meets the requirements of an Authorized User.

7.2.3 The PRISM Lead will file and retain the LMS training completion report for each prospective user and submit a request for PRISM access to the PRISM Administrator.

7.3. The PRISM Administrator will review the submitted registration information to assure appropriateness of the request. Once appropriateness is confirmed, the PRISM Administrator will activate the PRISM account and send logon instructions to the new Authorized User.

8. Data Classification

The State classifies data into categories based on the sensitivity of the data pursuant to the security policies and standards promulgated by Washington Technology Solutions (WaTech). See the WaTech Data Classification Standard at: https://watech.wa.gov/sites/default/files/2023-12/Data%20Classification%20Standard_Approved_2023.pdf, and which is hereby incorporated by reference.

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:

e. Personal Information about individuals, regardless of how that information is obtained;

f. Information concerning employee personnel records;

g. 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:

h. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements;

i. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

9. Constraints on Use of Data/Limited License

9.1. HCA discloses Data to DSHS for use by PRISM, and that data is used for multiple purposes pursuant to an existing, separate agreement. HCA hereby grants DSHS a limited right to further disclose relevant, HCA-supplied Data that is stored and used by PRISM to Receiving Party, according to the terms of this DSA, and Attachment A1, Receiving Party PRISM Licensing Statement, for use by Receiving Party in the provision of health care services to Receiving Party clients.

9.2. DSHS supplies Data to PRISM, which further generates Data based on both HCA-supplied and DSHS-supplied Data. Subject to the terms and conditions of the DSA, as well as those set forth in Attachment A1, Receiving Party PRISM Data Licensing Statement, DSHS grants Receiving Party access to PRISM, and a limited license to access both HCA-supplied Data and DSHS-supplied and PRISM generated Data, for certain permissible uses as stated in this DSA and Receiving Party PRISM Data Licensing Statement.

9.3. No ownership rights or interests in either HCA-supplied Data, in DSHS-supplied Data, or in DSHS-HCA jointly owned Data generated by PRISM is vested in, or transferred to, Receiving Party.

9.4. Data shared under this DSA includes data protected by 42 C.F.R. Part 2. In accordance with 42 C.F.R. § 2.32, this Data has been disclosed from records protected by federal confidentiality rules (42 C.F.R. Part 2). The federal rules prohibit Receiving Party from making any further disclosure(s) of the Data that identifies a patient as having or having had a substance use disorder (SUD) either directly, by reference to publicly available information, or through verification of such identification by another person unless further disclosure is expressly permitted by the written consent of the individual whose information is being disclosed or as otherwise permitted by 42 C.F.R. Part 2. A general authorization for the release of medical or other information is NOT sufficient for this purpose (42 C.F.R. § 2.31). The federal rules restrict any use of the SUD data to investigate or prosecute with regard to a crime any patient with a substance use disorder, except as provided at 42 C.F.R. §§ 2.12(c)(5) and 2.65.

9.5. This DSA does not constitute a release of the Data for the Receiving Party's discretionary use. Receiving Party must use the Data received or accessed under this DSA only to carry out the purpose and justification of this DSA as set out in the Data Licensing Statement(s). Any analysis, use, or reporting that is not within the Purpose of this DSA is not permitted without the Disclosing Parties' prior written consent.

9.6. This DSA does not constitute a release for Receiving Party to share the Data with any third parties, including Subcontractors, even if for authorized use(s) under this DSA, without the third party release being approved in advance by HCA and Disclosing Party and identified in the Data Licensing Statement(s), unless the third party is entitled to Data pertaining to a particular patient to whom the third party is providing health care services, or unless the third party is otherwise required by law to have access to the Data. Should Receiving Party Disclose Data it obtains pursuant to this DSA, it must document such Disclosures and must provide a report of such Disclosures (in a format that anonymizes PHI) to the PRISM Administrator upon request.

9.7. Derivative Data Product Review and Release Process. All reports derived from Data shared under this DSA, produced by Receiving Party that are created with the intention of being published for or shared with external customers (Data Product(s)) must be sent to HCA and DSHS for review of usability, data sensitivity, data accuracy, completeness, and consistency with HCA standards prior to disclosure. This review will be conducted, and response of suggestions, concerns, or approval provided to Receiving Party within 10 business days. Receiving Party will adhere to HCA Small Numbers Standards, Exhibit B. HCA, DSHS, and Receiving Party may agree to individual Permissible Use exceptions to the Small Numbers Standards in writing (email acceptable).

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

9.9. The Receiving Party must comply with the Minimum Necessary Standard, which means that Receiving Party will use the least amount of PHI necessary to accomplish the Purpose of sharing as described in Attachment A1, *et seq.*: Receiving Party PRISM Data Licensing Statement(s).

9.9.1 Receiving Party must identify:

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

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

9.9.2 Receiving Party must implement policies and procedures that limit the PHI disclosed to such persons or classes of persons to the amount reasonably necessary to achieve the purpose of the disclosure, in accordance with the attached Data Licensing Statement(s).

10. Data Modification(s)

Any modification to the Purpose, Justification, Description of Data to be Shared/Data Licensing Statement(s), and Permissible Use, is required to be approved by the Disclosing Party or Disclosing Parties through HCA's Data Request Process and by sending the requested modification to the DSHS Contract Administrator. Receiving Party must notify HCA's Contract Manager and DSHS Contract Manager of any requested changes to the Data elements, Use, records linking needs, research needs, and any other changes from this DSA, immediately to start the review process. HCA and DSHS will conduct a joint review of proposed modifications. Approved changes will be documented in an Amendment to the DSA.

11. Security of Data

11.1. Security Awareness Program

The Receiving Party must have a Security Awareness Program. This program must:

a. Be issued biennially, or more frequently, for all Receiving Party's employees or Subcontractors whose roles are associated with the Data contemplated in this DSA; and

b. At HCA's request, Receiving Party will provide documentation demonstrating its Security Awareness Program and associated training.

11.2. Data Protection

The Receiving Party must protect and maintain all Confidential Information gained by reason of this DSA 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.

11.3. Data Security Standards

a. Receiving Party must comply with the Data Security Requirements set out in Exhibit A and all WaTech Security Policies and Standards. See WaTech Security Policies and Standards at: https://watech.wa.gov/policies. All WaTech Security Policies and Standards are hereby incorporated by reference into this DSA.

b. Receiving Party must have a policy regarding monitoring and enforcement of the Data protection requirements specific in this DSA.

11.4. Data Disposition and Retention

a. Receiving Party will dispose of Disclosed Data in accordance with this section.

b. Upon request by a Disclosing Party, or at the end of the DSA term, or when no longer needed, Confidential Information/Data must be disposed of as set out in Exhibit A, *Data Security Requirements*, Section 5 *Data Disposition,* except as required to be maintained for compliance or accounting purposes. Receiving Party will provide written certification to the Disclosing Parties of disposition using Exhibit D, *Certification of Destruction/Disposition of Confidential Information*.

c. For the purpose of this section, "fiscal year" means the 12-month period of July 1 to June 30. Claims Data will not be kept or maintained beyond 10 years after the end of the fiscal year in which the claim is dated. Client Data, not including Claims Data, will not be kept or maintained beyond 10 years from the date received from the Disclosing Parties. DSHS-provided Client Data and PRISM-generated Data will not be kept or maintained beyond 10 years from the date received. Any other Data will not be kept or maintained beyond 10 years from the date received from the Disclosing Parties. At that time Data and derivative Data Products must be disposed of in accordance with subsection b.

12. Data Confidentiality and Non-Disclosure

12.1. Data Confidentiality

The Receiving Party will not use, publish, transfer, sell, or otherwise disclose any Confidential Information gained by reason of this DSA for any purpose that is not directly connected with the purpose, justification, and Permissible Use of this DSA, as set out in the attached Data Licensing Statement(s), 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 Data.

12.2. Non-Disclosure of Data

The Receiving Party must ensure that all Authorized Users, including employees or Subcontractors, who will have access to the Data described in this DSA (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. For avoidance of doubt, the Receiving Party must 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.

The Receiving Party will ensure that each employee who will access the Data signs or provides an electronic attestation to the User Agreement on Non Disclosure of Confidential Information on the PRISM Access Request form, as outlined in Section 7, System Access Request Process. The Receiving Party will retain the signed copy of the User Agreement on Non-Disclosure of Confidential Information or the LMS training completion report in each employee's personnel file for a minimum of six years from the date the employee's access to the Data ends. The documentation must be available to the Disclosing Parties upon request.

12.3. 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 C.F.R. Part 160 and Part 164; Confidentiality of Alcohol and Drug Abuse Patient Records, 42 C.F.R., Part 2; and Safeguarding Information on Applicants and Beneficiaries, 42 C.F.R. 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 by itself, its employees, and its Subcontractors with these laws and any violations of the DSA.

13. Public Disclosure

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 Party (HCA, DSHS, or both) that owns the Data as outlined in Attachment A1 (HCA's Public Disclosure Officer or DSHS's Public Records Officer) within five (5) business days and to follow the procedure set out in this section before disclosing any records.

The Receiving Party must provide a copy of the records with proposed redactions to HCA and/or DSHS when they are available and ready. HCA and/or DSHS 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 and/or DSHS's concerns or proposed changes, Receiving Party must notify HCA and/or DSHS of that disagreement and provide HCA and/or DSHS with a minimum of fifteen (15) business days to obtain a restraining order or injunction under RCW 42.56.540 before disclosing any records.

The HCA Public Disclosure Officer can be contacted at PublicDisclosure@hca.wa.gov. The DSHS Public Records Office can be contacted at DSHSPublicDisclosure@dshs.wa.gov.

14. Data Shared with Subcontractors

The Receiving Party will not enter into any Subcontract without the express, written permission of HCA and DSHS, which will jointly approve or deny the proposed subcontract in their sole discretion. If Data access is to be provided to a Subcontractor under this DSA it will only be for the Permissible Use authorized by HCA and DSHS and the Receiving Party must include all of the Data security terms, conditions and requirements set forth in this DSA in any such Subcontract. In no event will the existence of the Subcontract operate to release or reduce the liability of the Receiving Party to HCA and DSHS for any breach in the performance of the Receiving Party's responsibilities.

15. Audit

15.1. At HCA's or DSHS's request or in accordance with WaTech Security Policies and Standards, Receiving Party shall obtain audits covering Data Security and Permissible Use. Receiving Party may cover both the Permissible Use and the Data Security Requirements under the same audit, or under separate audits. The term, "independent third-party" as referenced in this section means an outside auditor that is an independent auditing firm.

15.2. Data Security audits must demonstrate compliance with Data Security standards adopted by WaTech, and as set forth in Exhibit A, Data Security Requirements. At a minimum, audit(s) must determine whether Data Security policies, procedures, and controls are in place to ensure compliance with all Data Security Requirements set forth herein and as required by state and federal law.

15.3. Permissible Use Audits must demonstrate compliance with Permissible Use standards as set forth in this DSA and each Attachment A. Audit(s) must determine whether Permissible Use policies, procedures, and controls are in place to ensure compliance with all Permissible Use requirements in this DSA.

15.4. HCA and DSHS may monitor, investigate, and audit the use of Personal Information received by Receiving Party through this DSA. The monitoring and investigating may include the act of introducing data containing unique but false information (commonly referred to as "salting" or "seeding") that can be used later to identify inappropriate use or disclosure of Data.

15.5. During the term of this DSA and for six (6) years following termination or expiration of this DSA, HCA and DSHS will have the right at reasonable times and upon no less than five (5) business days prior written notice to access the Receiving Party's records and place of business for the purpose of auditing, and evaluating the Receiving Party's compliance with this DSA and applicable laws and regulations.

16. Data Breach Notification and Obligations

16.1. The Breach or potential compromise of Data shared under this DSA must be reported to the HCA Privacy Officer at PrivacyOfficer@hca.wa.gov and the DSHS Privacy Officer at DSHSPrivacyOfficer@dshs.wa.gov within one (1) business day of discovery.

16.2. If the Breach or potential compromise of Data includes PHI, and the Receiving Party does not have full details, it will report what information it has and provide full details within 15 business days of discovery. To the extent possible, these reports must include the following:

a. The identification of each individual whose PHI has been or may have been improperly accessed, acquired, used, or disclosed;

b. The nature of the unauthorized Use or disclosure, including a brief description of what happened, the date of the event(s), and the date of discovery;

c. A description of the types of PHI involved;

d. The investigative and remedial actions the Contractor or its Subcontractor took or will take to prevent and mitigate harmful effects and protect against recurrence;

e. Any details necessary for a determination of the potential harm to Clients whose PHI is believed to have been Used or disclosed and the steps those Clients should take to protect themselves; and

f. Any other information HCA reasonably requests.

16.3. 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 and DSHS including but not limited to 45 C.F.R. Part 164 Subpart D; RCW 42.56.590; RCW 19.255.010; or WAC 284-04-625.

16.4. If notification must, in the judgement of HCA and DSHS, must be made Receiving Party will further cooperate and facilitate notification to necessary individuals, to the U.S. Department of Health and Human Services (DHHS) Secretary, and to the media. At HCA's discretion, Receiving Party may be required to directly perform notification requirements, or if HCA and/or DSHS elects to perform the notifications, Receiving Party must reimburse HCA for all costs associated with notification(s).

16.5. Receiving Party is responsible for all costs incurred in connection with a security incident privacy Breach, or potential compromise of Data, including:

a. Computer forensics assistance to assess 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;

b. Notification and call center services for individuals affected by a security incident or privacy Breach, including fraud prevention, credit monitoring, and identify theft assistance; and

c. Regulatory defense, fines, and penalties 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).

16.6. Any breach of this section may result in termination of the DSA and the demand for return or disposition, as described in Section 11.4, of all HCA Data.

16.7. Receiving Party's obligations regarding breach notification survive the termination of this DSA and continue for as long as Receiving Party maintains the Data and for any Breach or potential compromise, at any time.

17. HIPAA Compliance

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

17.1. HIPAA Point of Contact. The point of contact for the Receiving Party for all required HIPAA-related reporting and notification communications from this Section 17, *HIPAA Compliance*, and all required Data Breach notification communications from Section 16, *Data Breach Notification and Obligations*, is:

HCA Privacy Officer

Washington State Health Care Authority
626 8th Avenue SE
Olympia, WA 98504-2700
Telephone: (360) 725-1116
E-mail: PrivacyOfficer@hca.wa.gov

When it receives any report, notice or communication from Receiving Party, HCA will promptly notify DSHS at:

DSHS Privacy Officer
Department of Social and Health Services
1115 Washington Street SE
PO Box 45115
Olympia, WA 98504-5115
Telephone: (360) 902-7802
Email: DSHSPrivacyOfficer@dshs.wa.gov

17.2. Compliance. Business Associate must perform all DSA 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, as applicalbe.

17.3. 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 must protect PHI from, and will use appropriate safeguards, and comply with Subpart C of 45 C.F.R. Part 164, Security Standards for the Protection of Electronic Protected Health Information, with respect to electronic PHI, 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 DSA.

b. 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 DSA (45 C.F.R. § 164.514(d)(2) through (d)(5)).

c. 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 DSA or as required by law, and will not Use or disclose such PHI in any manner that would violate Subpart E of 45 C.F.R. 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 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 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 must report to the contact identified in subsection 17.1, in writing, all Uses or disclosures of PHI not provided for by this DSA within one business day of becoming aware of the unauthorized Use or disclosure of PHI, including Breaches of unsecured PHI as required at 45 C.F.R. § 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.

g. Failure to Cure. If HCA or DSHS learns of a pattern or practice of Business Associate that constitutes a violation of the Business Associate's obligations under the terms of this DSA and reasonable steps by the Business Associate do not end the violation, HCA and/or DSHS may terminate this DSA, 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 Business Associate do not end the violation, Business Associate must terminate the Subcontract, if feasible.

h. Termination for Cause. Business Associate authorizes immediate termination of this DSA by HCA or DSHS, if HCA or DSHS determines that Business Associate has violated a material term of this Business Associate Agreement. HCA and/or DSHS may, at their 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 must give reasonable access to PHI, its internal practices, records, books, documents, electronic data, and all other business information received from, or created or received by Business Associate on behalf of HCA and DSHS to the Secretary of DHHS and/or to HCA and DSHS for use in determining compliance with HIPAA privacy requirements.

j. Obligations of Business Associate Upon Expiration or Termination. Upon expiration or termination of this DSA for any reason, with respect to PHI received from HCA and/or DSHS, 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 and DSHS 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 C.F.R. Part 164, Security Standards for the Protection of Electronic Protected Health Information, with respect to electronic PHI 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 the 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 17.1, *Use and Disclosure of PHI*, that applied prior to termination; and

v. Return to HCA and DSHS 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 Business Associate under this section will survive the termination or expiration of this DSA.

17.4. Individual Rights

a. Accounting of Disclosures

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

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

iii. At the request of HCA or DSHS 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 years prior to the date on which the accounting was requested.

b. 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's and DSHS's obligations under 45 C.F.R. § 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 asks the Business Associate to respond to a request, the Business Associate must comply with the requirements in 45 C.F.R. § 164.524, Access of Individuals to Protected Health Information, on form, time, and manner of access. When the request is made by HCA or DSHS, the Business Associate will provide the records to HCA or DSHS within ten business days.

c. Amendment

i. If HCA or DSHS amends, in whole or in part, a record or PHI contained in an Individual's Designated Record Set and HCA or DSHS has previously provided the PHI or record that is the subject of the amendment to Business Associate, then HCA or DSHS will inform Business Associate of the

amendment pursuant to 45 C.F.R. § 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 DSHS or as necessary to satisfy HCA's and DSHS's obligations under 45 C.F.R. § 164.526, Amendment of Protected Health Information.

17.5. Subcontracts and other Third Party Agreements. In accordance with 45 C.F.R. §§ 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 DSA 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 C.F.R. §§ 164.314(a)(2)(i)(B) and 164.504(e)(5).

17.6. Obligations. To the extent the Business Associate is to carry out one or more of HCA's or DSHS's obligation(s) under Subpart E of 45 C.F.R. 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).

18. Amendments and Alterations

This DSA, 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 will sign an amendment.

19. Assignment

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

20. Dispute Resolution

20.1. The parties agree to work in good faith to resolve all conflicts at the lowest level possible. However, if the parties are not able to promptly and efficiently resolve, through direct informal contact, any dispute concerning the interpretation, application, or implementation of any section of this DSA, either party may reduce its description of the dispute in writing, and deliver it to the other party for consideration. Once received, the assigned managers or designees of each party will work to informally and amicably resolve the issue within five (5) business days. If managers or designees are unable to come to a mutually acceptable decision within five (5) business days, they may agree to issue an extension to allow for more time.

20.2. If the dispute cannot be resolved by the managers or designees, the issue will be referred through each Agency's respective operational protocols, to the Director of HCA ("Director"), the Disclosing Party's Agency Head, and the Receiving Party's Agency Head ("Agency Heads") or their deputies or designated delegates. Both parties will be responsible for submitting all relevant documentation, along with a

short statement as to how they believe the dispute should be settled, to the Director and Agency Head.

20.3. Upon receipt of the referral and relevant documentation, the Director and Agency Heads will confer to consider the potential options of resolution, and to arrive at a decision within fifteen (15) business days. The Director and Agency Heads may appoint a review team, a facilitator, or both, to assist in the resolution of the dispute. If the Director and Agency Heads are unable to come to a mutually acceptable decision within fifteen (15) business days, they may agree to issue an extension to allow for more time.

20.4. The final decision will be put in writing, and will be signed by both the Director and Agency Heads. If the DSA is active at the time of resolution, the parties will execute an amendment or change order to incorporate the final decision into the DSA. The decision will be final and binding as to the matter reviewed and the dispute will be settled in accordance with the terms of the decision.

20.5. If the Director and Agency Heads are uanble to come to a mutually acceptable decision, the parties will request intervention by the Governor, per RCW 43.17.330, in which case the governor may employ whatever dispute resolution methods that the governor deems appropriate in resolving the dispute.

20.6. Both parties agree that, the existence of a dispute notwithstanding, the parties will continue without delay to carry out all respective responsibilities under this DSA that are not affected by the dispute.

21. Entire Agreement

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

22. Governing Law and Venue

This DSA 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 DSA, jurisdiction is proper only in the Superior Court of Washington, and venue is proper only in Thurston County, Washington.

23. Incorporated Documents and Order of Precedence

23.1. Each of the documents listed below is, by this reference, incorporated into this DSA as though fully set forth herein.

a. Attachment A(s) – Data Licensing Statement.

b. Exhibit A – Data Security Requirements.

c. Exhibit B – HCA Small Numbers Standard.

d. Exhibit C – PRISM Access Request Form

e. Exhibit D - Certification of Destruction/Disposal of Confidential Information.

f. Exhibit E – Medicare Data Use Requirements Documents

g. WaTech Security Policies and Standards: https://watech.wa.gov/policies.

23.2. In the event of any inconsistency in this DSA, the inconsistency will be resolved in the following order of precedence:

a. Applicable federal and state statutes, laws, and regulations;

b. Sections of this DSA;

c. Attachments, Exhibits, and Schedules to this DSA.

24. Insurance

24.1. HCA and DSHS 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 they are found liable.

24.2. 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 will provide certificates of insurance to that effect to HCA or DSHS upon request.

24.3. Required Insurance or Self-Insured Equivalent

a. Commercial General Liability Insurance (CGL) covering the risks of bodily injury (including death), property damage, and contractual liability, with a limit of not less than $1 million per occurrence, $2 million aggregate.

b. Privacy Breach Response Coverage. For the term of this DSA 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 assess 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 penalties 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).

c. 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 DSA or of the beginning of DSA work.

ii. If coverage is canceled or non-renewed, and not replaced with another claims-made policy form with a retroactive date prior to the DSA effective

date, the Receiving Party must purchase "extended reporting" coverage for a minimum of 3 years after completion of DSA work.

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

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

By requiring insurance herein, HCA and DSHS do 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 and DSHS in this DSA.

25. Legal Notices

25.1. 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:

Stacey Smith
Aging & Long Term Care Director
614 Division St., MS-5
Port Orchard, WA 98366

b. To HCA at:

Contract Administrator
Division of Legal Services
Health Care Authority
PO Box 42702
Olympia, Washington 98504-2702
contracts@hca.wa.gov

c. To DSHS at:

DSHS/Operations Support & Services
Attn: Central Contracts and Legal Services
PO Box 45811
Olympia, Washington 98504-5811

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.

26. Maintenance of Records

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

27. Responsibility

HCA, DSHS, 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. Receiving Party must defend, protect, and save HCA and DSHS harmless from and against any loss and all claims, settlements, judgments, costs, penalties, and expenses, including reasonable attorney fees, arising from any intentional or negligent acts or omissions while performing under the terms of this DSA. 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.

28. Severablility

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

29. Survival Clauses

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

30. Term and Termination

30.1. Term. This DSA will begin on date of execution and continue through December 31, 2027, unless terminated sooner as provided in this section. The DSA may be extended through mutual agreement by amendment.

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

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

Before HCA or DSHS terminates this DSA for default, HCA or DSHS will provide the Receiving Party with written notice of its noncompliance with the DSA 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 and/or DSHS may then terminate the DSA. HCA and/or DSHS may terminate the DSA for default without such written notice and without opportunity for correction if HCA or DSHS 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 and/or DSHS, in its or their sole discretion.

31. Waiver

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

32. Signatures and Counterparts

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

Attachment A1: KITSAP COUNTY ALTC PRISM Data Licensing Statement

1. Background

HCA and DSHS work together to determine eligibility and serve Medicaid clients through Medicaid health care delivery systems (medical, behavioral health and long-term care services and supports).

HCA is responsible for ProviderOne, Washington's federally certified Medicaid Management Information System (MMIS) that provides information on Client eligibility, managed care and fee-for-service medical claims Data, Client-related correspondence, prior authorizations for Medicaid Clients receiving Medicaid (Title XIX) personal care services or other home and community services, etc.

DSHS's Research and Data Analysis (RDA) Division is responsible for the Predictive Risk Intelligence System (PRISM), a secure web-based clinical decision support tool integrating HCA-supplied and DSHS-supplied Data that shows administrative and assessment data for each Medicaid Client and is organized to identify care coordination opportunities. The PRISM application is housed and administered in the DSHS Research and Data Analysis Division and along with the information it produces is jointly owned by DSHS's RDA Division and HCA. K492-1-14 is the Service Level Agreement between HCA and DSHS for the PRISM application.

PRISM draws health care information from ProviderOne, from the CARE Assessment and from billing records administered by the DSHS Home and Community Living Administration (HCLA), and from other sources. For purposes of this Agreement, HCA and DSHS HCLA are owners of Data put into PRISM.

2. Justification and Authority for Data Sharing

The Data to be shared under this DSA are necessary for the Receiving Party to perform activities that involve the provision, coordination, or management of Client health care and related services, which includes consultation with another provider and referral to another provider.

In addition the following statutes, state and federal rules provide authority for sharing this Data: RCW 39.34, Interlocal Cooperation Act; RCW 74.04.060(1)(b), Records, Confidential-Exceptions-Penalty, RCW 74.39A Long-Term Care Services Options; RCW 41.05, State Health Care Authority; RCW 70.02, Medical Records- Health Care Information Access and Disclosure, Chapter 388-71 WAC, Home and Community Services and Programs; 388-825 WAC, Developmental Disabilities Administration Service Rules; 45 CFR 164.512(k)(6), Uses and Disclosures for Specialized Government Functions, Covered Entities that are Government Programs Providing Public Benefits: and 45 CFR 164.506, Uses and Disclosures to carry out Treatment, Payment or Health Care Operations.

3. Purpose / Use / Description of Data

The purpose of this DSA is to provide terms and conditions under which HCA and DSHS will allow the restricted use of its Data to the Receiving Party, and under which the Receiving Party may receive and use the Data. This DSA ensures that HCA, DSHS, and jointly owned Data is provided, protected, and used only for purposes authorized by state and federal law governing such Data use.

The scope of this DSA only provides the Receiving Party with access and Permissible Use of Data; it does not establish an agency relationship or independent contractor relationship between HCA and the Receiving Party or DSHS and the Receiving Party.

4. Permissible Use:

Receiving Party may only use the Data for the purposes of facilitating case management and care coordination for aging adults in the Receiving Party's caseload to include, for example, the following treatment related activities:

a. To verify information when there is a question about the accuracy of reporting by Medicaid clients or their representatives.

b. To better support aging Medicaid clients by looking up medical diagnoses and medications, providers, and historical hospitalizations and ER visits.

5. Data Access:

The Parties will exchange Data as described below:

a. Method of Access/Transfer: PRISM system access as described in Sections 6 and 7 of this DSA.

b. Frequency of Data Access: As Needed

c. Costs: N/A

Data Elements: Receiving Party staff involved in care management activities for aging adults who are in the care of Receiving Party will use PRISM to access information about health service utilization (e.g., hospitalizations), treating providers, medications, and health service needs. Access to this Data will help Receiving Party staff support better health outcomes for Medicaid clients under their care.

DSHS's RDA maintains access control over substance use disorder (SUD) data covered by 42 C.F.R. Part 2 and has an authorization process for allowing users to access these data. When requesting SUD data in PRISM the User must attest they have authority (such as documented patient consent) to access SUD treatment information that may be protected under 42 CFR Part 2 by clicking OK within the pop-up box. SUD data are not displayed until a user has attested within PRISM that they are authorized to access this data.

The Receiving Party shall comply with the privacy, Data security, permitted Data usage requirements and Data use restrictions contained in Exhibit E, as follows:

a. Information Exchange Agreement between Center for Medicare and Medicaid Services Washington State Health Care Authority for Disclosure of Medicare Part D Data (CMS Agreement No. 2019-13) as pertains to Medicare Data provided to the Receiving Party.

b. Medicare Part D Data Use Agreement No. 21268, Agreement for Use of Center for Medicare and Medicaid Services Data Containing Individual Identifiers and addenda.

Exhibit A: Data Security Requirements

1. Definitions

In addition to the definitions set out in Section 1, *Definitions*, of the Data Share Agreement (DSA), the definitions below apply to this Exhibit.

"Hardened Password" means a string of characters containing at least three of the following character classes: upper case letters; lower case letters; numerals; and special characters, such as an asterisk, ampersand or exclamation point.

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

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

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

"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).

"Portable/Removable Devices" means any small computing device that can be transported, including but not limited to: handhelds/PDAs/Smartphones; Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players); and laptop/notebook/tablet computers. If used to store Confidential Information, devices should be Federal Information Processing Standards (FIPS) Level 2 compliant.

"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.

"Transmitting" means the transferring of data electronically, such as via email, SFTP, webservices, AWS Snowball, etc.

"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.

"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

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.

When transmitting HCA's Confidential Information via paper documents, the Receiving Party must use a Trusted System and must be physically kept in possession of an authorized person

3. Protection of Data

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

Data at Rest:

i. Data will be encrypted with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the data. Access to the Data will be restricted to Authorized Users through the use of access control lists, a Unique User ID, and a Hardened Password, or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Systems which contain or provide access to Confidential Information must be located in an area that is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

ii. Data stored on Portable/Removable Media or Devices:

(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 DSA. 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.

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.

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.

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.

Receiving Party must designate and be able to identify all computing equipment on which they store, process and maintain HCA Data. No Data at any time may be processed on or transferred to any portable storage medium. Laptop/tablet computing devices are not considered portable storage medium devices for purposes of this DSA provided it is installed with end-point encryption.

5. Data Disposition

Consistent with Chapter 40.14 RCW, Receiving Party shall erase, destroy, and render unrecoverable all HCA Confidential Data and certify in writing that these actions have been completed within thirty (30) days of the disposition requirement or termination of this DSA, whichever is earlier. At a minimum, media sanitization is to be performed according to the standards enumerated by NIST SP 800-88r1 Guidelines for Media Sanitization.

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.

6. Network Security

Receiving Party's network security must include the following:

Network firewall provisioning;

Intrusion detection;

Quarterly vulnerability assessments; and

Annual penetration tests.

7. Application Security

Receiving Party must maintain and support its software and subsequent upgrades, updates, patches, and bug fixes such that the software is, and remains secure from known vulnerabilities.

8. Computer Security

Receiving Party shall maintain computers that access Data by ensuring the operating system and software are updated and patched monthly, such that they remain secure from known vulnerabilities. Receiving Party computer device(s) must also be installed with an Anti-Malware solution and signatures updated no less than monthly.

9. Offshoring

Receiving Party must maintain all hardcopies containing Confidential Information only from locations in the United States.

Receiving Party may not directly or indirectly (including through Subcontractors) transport any Data, hardcopy or electronic, outside the United States unless it has advance written approval from HCA.

Exhibit B: HCA Small Numbers Standard

1. Background

It is the HCA's legal and ethical responsibility to protect the privacy of its clients and members. Publishing, sharing, or releasing data products that include small numbers creates two concerns: (1) As a reported number gets smaller, the risk of re-identifying an HCA client or member increases. This is especially true when a combination of variables is included in the data product to arrive at the small number (e.g. location, race/ethnicity, age, or other demographic information); and (2) Small numbers can also create questions around statistical relevance. When it comes to externally-shared data products, the need to know the exact value in a cell containing small numbers must be questioned.

Any external publication of data products derived in whole or in part from HCA data are to be compliant with both HIPAA and Washington State privacy laws. Data products are not to contain small numbers that could allow re-identification of individual beneficiaries. Category 1 data is information that can be released to the public. These products do not need protection from unauthorized disclosure but do need integrity and availability protection controls. Additionally, all contractors (state and private) that use HCA's data to produce derivative reports and data products are required to adhere to this standard as well.

As HCA moves away from traditional, static reports to a dynamic reporting environment (e.g. Tableau visualizations), it is easier for external data consumers to arrive at small numbers. Further, those external consumers have an increasing amount of their own data that could be used to re-identify individuals. As a result, more rigor and a consistent approach should be in place to protect the privacy of HCA's clients and members. Until now, some HCA data teams have elected to follow small numbers guidelines established by the Department of Health, which include examples of suppression methods for working with small numbers. HCA is now establishing its own standard but is planning to work with DOH and other agencies dealing with healthcare data to try and develop a consistent small numbers methodology at a statewide level.

This standard does not supersede any federal and state laws and regulations. Federal health organizations such as the Centers for Disease Control and Prevention (CDC) and the National Center for Health Statistics (NCHS) also maintain small numbers standards. HCA's federal oversight agency and funding partner, the Centers for Medicare and Medicaid Services (CMS) adopts suppression of any cell with a count of 10 or less.

2. HCA's Small Number Standard

There are no automatic exemptions from this standard (See Exception Request Process section below).

i. Standard applies for all geographical representations, including statewide.

ii. Exceptions to this standard will be considered on a case-by-case basis (see Exception Request Process section below for more information).

iii. Ensure that no cells with $0 < n < 11$ are reported ($0 < n < 11$ suppressed).

iv. Apply a marginal threshold of 1 - 10 and cell threshold of 1 - 10 to all tabulations ($0 < n < 11$ suppressed).

v. To protect against secondary disclosure, suppress additional cells to ensure the primary suppressed small value cannot be recalculated.

vi. Suppression of percentages that can be used to recalculate a small number is also required.

vii. Use aggregation to prevent small numbers but allow reporting of data. Age ranges are a very good example of where aggregation can be used to avoid small numbers but avoid suppressing data (see example below).

3. Small Numbers Examples

Example (Before Applying Standard)

Client Gender	County	Accountable Community of Health (ACH)	Statewide
Male	6	8	14
Female	11	15	26
TOTAL	17	23	40

Example (After Applying Standard)

Client Gender	County	ach	Statewide
Male	---[1]	---	14
Female	11	15	26
TOTAL	---	---	40

[1] In order to protect the privacy of individuals, cells in this data product that contain small numbers from 1 to 10 are not displayed.

The above examples show in order to comply with the standard, analysts must not only suppress directly those cells where n < 11, but also in this case secondary suppression is necessary of the county and ACH totals in order to avoid calculation of those cells that contained small numbers.

Example (Suppression with no aggregation)

Age Range	County	ach	Statewide
0-3	5 (would be suppressed)	8 (would be suppressed)	13 (would be suppressed)
4-6	7 (would be suppressed)	18	25 (would be suppressed)
	15	23	38
10-12	24	33	57
TOTAL	51 (would be suppressed)	82 (would be suppressed)	133

Example (Using aggregation instead of suppression)

Age Range	County	ach	Statewide
0-6	12	26	38
7-9	15	23	38
10-12	24	33	57
TOTAL	51	82	133

The above examples provide guidance for using aggregation to avoid small number suppression and still provide analytic value to the end user. Aggregation is an excellent method to avoid presenting information with many holes and empty values.

4. Exception Request Process

To request an exception to this standard, Receiving Party must do the following:

Send an e-mail to HCAData@hca.wa.gov containing the following information:

a. A copy of the data product, or a sample of the data product if sending the entire data products is not feasible due to size.

b. Rationale and reason for publishing the product containing small numbers.

c. Impact if the product is not published.

d. Intended audience for the data product.

e. Why aggregation is not an acceptable mitigation.

f. Requests are jointly reviewed by the HCA Privacy Officer and Data Governance Program Manager.

If the HCA Privacy Officer and Data Governance Program Manager deem necessary, the request will be escalated up through HCA's Data Utilization Committee for a final decision.

HCA's Data Governance Program Manager will inform requestor the final decision along with any necessary handling instructions for the product if it is allowed to be shared or posted.

Decisions for each exception will be documented on the HCA Data Governance Decision Log.

Those approved exceptions for publishing small numbers will be considered in future updates of this standard.

Exhibit C: PRISM Access Request

Washington State Department of Social & Health Services
Transforming lives

PRISM Access Request

Washington State Health Care Authority

An Organization may request access to PRISM for its employees or employees of Subcontractors (Users) under its Data Share Agreement (DSA) with DSHS and HCA. The Organization PRISM Lead reviews and completes the "Requesting Organization" section. The PRISM Access Request form must be signed by the PRISM Lead authorizing the request, which attests to the Users' business need for electronic Protected Health Information, and in the case of a Subcontractor User, attests that the contract with the Subcontractor includes a HIPAA Business Associate Agreement and Medicare data share language, as appropriate. The User completes the "User Registration Information" section below and signs the "User Agreement and Non- Disclosure of Confidential Information" page. The PRISM Lead then forwards the request to: PRISM.Admin@dshs.wa.gov. Upon review and acceptance, DSHS and HCA will grant the appropriate access permissions to the User and notify the PRISM Lead. Changes to Access for Users: The PRISM Lead must notify the PRISM Administrator within five (5) business days whenever a User with access rights leaves employment or has a change of duties such that the User no longer requires access. If the removal of access is emergent, please include that information with the request.

Requesting Organization (to be completed by PRISM Lead)		
CONTRACTOR'S NAME	SUBCONTRACTOR'S NAME (IF APPLICABLE)	
CONTRACTOR'S STREET ADDRESS CITY STATEZIP CODE		
User Registration Information (to be completed by User)		
USER'S NAME (FIRST, MIDDLE, LAST)	USER'S JOB TITLE	
USER'S BUSINESS EMAIL ADDRESS	USER'S BUSINESS PHONE NUMBER (INCLUDE AREA CODE)	
Completion of HIPAA Training and IT Security Training in the past year:	DATE HIPAA TRAINING	DATE IT SECURITY TRAINING
If user will be completing Health Action Plans (HAPs), enter the date HAP training was completed:		DATE HAP TRAINING
PRISM USER'S SIGNATURE DATE	PRISM USER'S PRINTED NAME	
Authorizing Signature		

Protected Data Access Authorization The HIPAA Security rule states that every employee that needs access to electronic Protected Health Information (ePHI) receives authorization from an appropriate authority and that the need for this access based on job function or responsibility is documented. I, the undersigned PRISM Lead, verify that the individual for whom this access is being requested (User or Subcontractor User) has a business need to access this data, has completed the required HIPAA Privacy training and the annual IT Security training and has signed the required *User Agreement and Non-Disclosure of Confidential Information* included with this Access Request. This User's access to this electronic Protected Health Information (ePHI) is appropriate under the HIPAA Information Access Management Standard and the Privacy Rule. In addition, if applicable, this employee has been instructed on 42 Code of Federal Regulations (CFR) Part 2 that governs the use of alcohol and drug use information and is aware that this type of data must be used only in accordance with these regulations. I have also ensured that the necessary steps have been taken to validate the User's identity before approving access to confidential and protected information. If a Subcontractor is indicated, I attestthat the contract with the Subcontractor includes a HIPAA Business Associate Agreement, and where appropriate Medicare data share language.	
PRISM LEAD SIGNATURE DATE	PRISM LEAD NAME (PRINT)

User Agreement and Non-Disclosure of Confidential Information

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

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, RCW 70.02.020 and RC2.70.02.230) 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 Agreement and Assurance of Confidentiality

In consideration for DSHS and HCA granting me access to PRISM 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 DSHS or HCA systems and view DSHS or HCA Confidential Information.
3. Will not use or disclose any Confidential Information gained by reason of this Agreement for any commercial, personal, or research purpose, or any other purpose that is not directly connected with client care coordination and quality improvement.
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 DSHS and HCA systems User ID and password and not share them with anyone or allow others to use any DSHS or HCA system logged in as me.
10. Will not distribute, transfer, or otherwise share any DSHS 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, DSHS or 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.

User's Signature	
PRISM USER'S SIGNATURE DATE	PRISM USER'S PRINTED NAME

Exhibit D: Certification of Destruction/Disposal of Confidential Information

(To Be Filled Out and Returned to HCA and DSHS Upon Termination of DSA)

NAME OF RECEIVING PARTY:	DATA SHARE AGREEMENT (DSA) #:

_____ (Receiving Party) herby certifies that the data elements listed below or attached, received as a part of the data provided in accordance with DSA have been:

☐ DISPOSED OF/DESTROYED ALL COPIES

You certify that you returned or destroyed all identified confidential information received from HCA and DSHS, or created, maintained, or received by you on behalf of HCA and DSHS. You certify that you did not retain any copies of the confidential information received by HCA and DSHS.

Description of Information Disposed of/ Destroyed:

Date of Destruction: _____

Method(s) of destroying/disposing of Confidential Information:

Disposed of/Destroyed by:

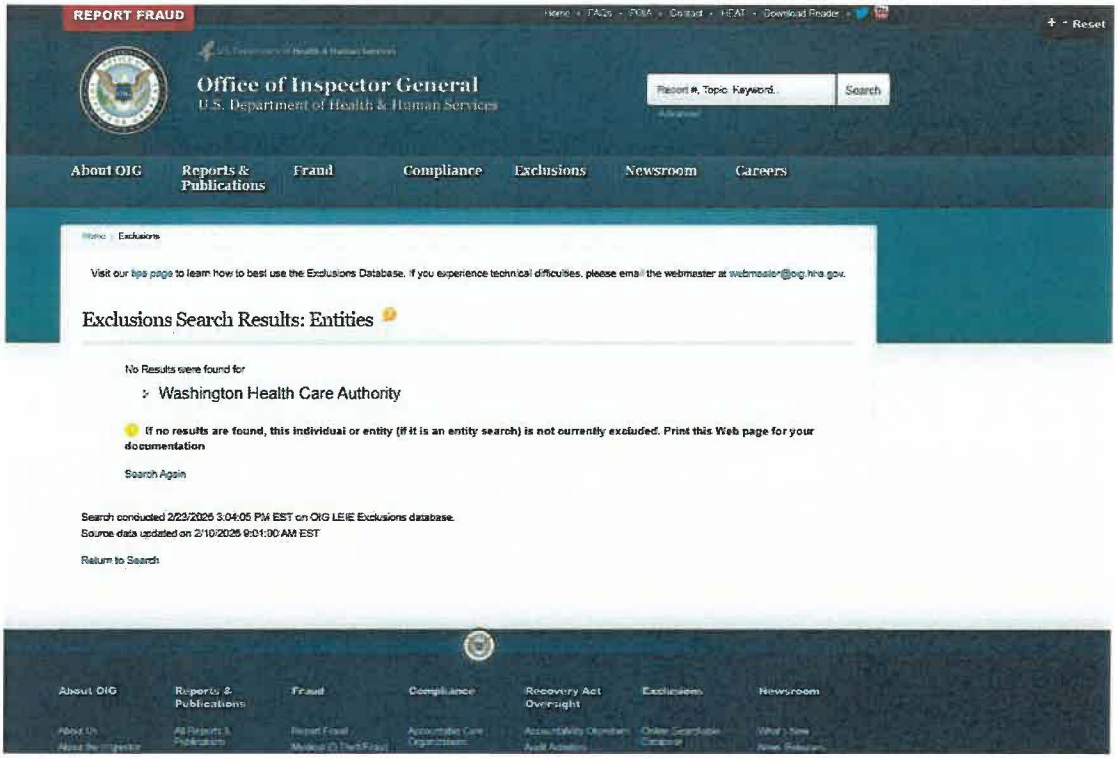
Signature	Date
Printed Name:	
Title:	

Exhibit E: Medicare Data Use Requirements Documents

Information Exchange Agreement between Center for Medicare and Medicaid Services Washington State Health Care Authority for Disclosure of Medicare Part D Data (CMS Agreement No. 2019-13) as pertains to Medicare Data provided to the Receiving Party.

Medicare Part D Data Use Agreement No. 21268, Agreement for Use of Center for Medicare and Medicaid Services Data Containing Individual Identifiers and addenda.

Washington State Health Care Authority



Washington State Department of Social and Health Services