

Exhibit G Data Share Agreement Instructions

Bidder must complete the following prior to returning to HCA:

Page 1:

Receiving Party Name

Receiving Party DBA (if applicable)

Receiving Party Address

Receiving Party Contact Name, Title (Contract Manager)

Receiving Party Contact Telephone

Receiving Party Contact Email Address

Receiving Party Signature / Printed Name and Title / Date Signed

Page 12:

Section 12, Legal Notices – Receiving Party Legal Notices Address


	Data Share Agreement RFP 2516 – Managed Care Dental Procurement		HCA Contract Number:
			Receiving Party Contract Number: _____
This Data Share Agreement (DSA) is made by and between the state of Washington Health Care Authority (HCA) and the party whose name appears below (Receiving Party)			
<i>Receiving Party Name</i>		<i>Receiving Party doing business as (DBA)</i>	
<i>Receiving Party Address</i>		<i>Receiving Party Contact Name, Title (Contract Manager)</i>	
<i>Receiving Party Contact Telephone</i>		<i>Receiving Party Contact Email Address</i>	
<i>HCA Program</i>		<i>HCA Division/Section</i>	
Managed Care Dental Program		MPOI / CS	
<i>HCA Contact Name, Title (Contract Manager)</i>		<i>HCA Contact Address</i>	
Jennifer Coiteux, Business Operations Manager		626 8th Avenue SE, PO Box 45502 Olympia, WA 98504-5502	
<i>HCA Contact Telephone</i>		<i>HCA Contact Email Address</i>	
		hcacontracts@hca.wa.gov	
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 HCA only upon signature by HCA.			
<i>Receiving Party Signature</i>		<i>Printed Name and Title</i>	<i>Date Signed</i>
<i>HCA Signature</i>		<i>Printed Name and Title</i>	<i>Date Signed</i>

Table of Contents

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

Schedule 1: Description of Shared Data

Exhibit A: Data Security Requirements

Exhibit B: User Agreement on Non-Disclosure of Confidential Information

Exhibit C: Certification of Disposition

1. Background

Washington Health Care Authority (HCA) currently provides comprehensive dental benefits for adults and children (including orthodontia for children age 20 and under) through fee-for-service (FFS) payment to enrolled dental providers. In fiscal year 2016, HCA had 2.1 million clients eligible for dental services. Of those, approximately 800,000 clients accessed some type of dental care, a 38.2% utilization rate.

As legislatively mandated by the passage of SSB 5883, Section 213(1)(c), HCA began the process of issuing a procurement to solicit proposals from Managed Care Entities (MCEs) interested in developing and implementing a Managed Care Dental program for eligible Medicaid clients beginning January 1, 2019. Request for Proposal (RFP) 2516 was released May 3, 2018.

The goals of the Apple Health Managed Care Dental Program are to: 1) facilitate better access to care and improved oral health outcomes for Medicaid Enrollees; 2) retain innovative programs such as Access to Baby and Child Dentistry program (ABCD) and Oral Health Connections Pilot Project that improve access and care, and develop new programs that improve access to care and dental outcomes; 3) increase the dental provider network, particularly for adults; and 4) establish a program to reduce emergency room visits for dental purposes.

Receiving Party submitted a Letter of Intent to bid, as directed in RFP 2516.

2. Purpose of the DSA

The purpose of this Data Share Agreement (DSA) is to identify, describe and protect the Medicaid data being provided by HCA to the Receiving Party. The purpose for sharing the Data is for the Receiving Party to be able to complete Bidder's Proposal for the Managed Care Dental Program RFP 2516.

Data provided will only be used to in Bidder's Proposal to RFP 2516, in regards to sections 3.3, Network Adequacy (Pass/Fail); 3.4, Network Adequacy (Scored); and 3.8, Cost Proposal.

3. Justification and Authority for Data Sharing

The Data to be shared under this DSA are necessary to comply with SSB 5883, Section 213(1)(c).

SSB 5883, Section 213(1)(c) directs HCA to competitively procure and contract with licensed dental health plans or managed health care plans for dental care services.

Receiving Party is a Covered Entity, as defined in 45 C.F.R. § 160.103.

To allow Receiving Party, who is a Bidder on RFP 2516, access to the information necessary to provide HCA with an adequate network, and competitive, actuarially sound rates based on HCA assumptions, and current dental utilization and population data.

4. Definitions

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

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

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

“Client” means an individual who is eligible for or receiving Medicaid services.

“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 0, *Data Classification*, which includes, but is not limited to, Personal Information and Protected Health Information. For purposes of this DSA, Confidential Information means the same as “Data.”

“Contract Administrator” means the individual designated to receive legal notices and to administer, amend, or terminate this DSA.

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

“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.”

“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.

“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 CFR Parts 160 and Part 164.

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

“Protected Health Information” or “PHI” means information that relates to the provision of health care to an individual; the past, present, or future physical or mental health or condition of an

individual; or past, present or future payment for provision of health care to an individual. 45 CFR 160 and 164. PHI includes demographic information that identifies the individual or about which there is reasonable basis to believe, can be used to identify the individual. 45 CFR 160.103. PHI is information transmitted, maintained, or stored in any form or medium. 45 CFR 164.501. PHI does not include education records covered by the Family Educational Right and Privacy Act, as amended, 20 USC 1232g(a)(4)(b)(iv).

“ProviderOne” means the Medicaid Management Information System, which is the State’s Medicaid payment system managed by HCA.

“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.

“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

The Data to be shared is set out in attached Schedule 1: *Description of Shared Data*.

The Data will be provided one time, through SFT. HCA will provide access to Receiving Party.

6. Data Classification

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

The Data that is the subject of this DSA is classified as indicated below:

☒ Category 1 – Public Information

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

☒ Category 2 – Sensitive Information

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

☐ Category 3 – Confidential Information

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

- a. Personal Information about individuals, regardless of how that information is obtained;
- b. Information concerning employee personnel records;
- c. Information regarding IT infrastructure and security of computer and telecommunications systems;

☒ Category 4 – Confidential Information Requiring Special Handling

Confidential information requiring special handling is information that is specifically protected from disclosure by law and for which:

- a. Especially strict handling requirements are dictated, such as by statutes, regulations, or agreements;
- b. Serious consequences could arise from unauthorized disclosure, such as threats to health and safety, or legal sanctions.

7. Constraints on Use of Data

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

- 7.2. 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 sections 2, Purpose of the Data Sharing, and 3, Justification and Authority for Data Sharing. Any analysis, use, or reporting that is not within the Purpose of this DSA is not permitted without HCA's prior written consent.
- 7.3. Any disclosure of Data contrary to this DSA is unauthorized and is subject to penalties identified in law.
- 7.4. 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 this DSA as described in Section 2, *Purpose of the Data Sharing*.
- a. Receiving Party must identify:
 - i. Those persons or classes of persons in its workforce who need access to PHI to carry out their duties; and
 - ii. 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.
 - b. 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 Section 2, *Purpose of the Data Sharing*, of this DSA.

8. Security of Data

8.1. 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.

8.2. Data Security Standards

Receiving Party must comply with the Data Security Requirements set out in Exhibit A and the Washington OCIO Security Standard, 141.10 (<https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets>.) The Security Standard 141.10 is hereby incorporated by reference into this DSA.

8.3. Data Disposition

Upon request by HCA, 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, Section 5 *Data Disposition*, except as required to be maintained for compliance or accounting purposes.

Receiving Party will provide written Certification of Disposition, Exhibit C, upon request by HCA.

9. Data Confidentiality and Non-Disclosure

9.1. Data Confidentiality.

The Receiving Party will not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this DSA for any purpose that is not directly connected with the purpose and justification of this DSA, as set out in Sections 1 and 3 above, except: (a) as provided by law; or (b) with the prior written consent of the person or personal representative of the person who is the subject of the Confidential Information.

9.2. Non-Disclosure of Data

The Receiving Party must ensure that all 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. The Receiving Party will 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 or Subcontractor who will access the Data signs the *User Agreement on Non-Disclosure of Confidential Information*, Exhibit B hereto. The Receiving Party will retain the signed copy of the *User Agreement on Non-Disclosure of Confidential Information* 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 HCA upon request.

9.3. Penalties for Unauthorized Disclosure of Data

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

The Receiving Party accepts full responsibility and liability for any noncompliance by itself, its employees, and its Subcontractors with these laws and any violations of the DSA.

10. Public Disclosure

Receiving Party acknowledges that HCA is subject to the Public Records Act (Chapter 42.56 RCW). This DSA will be a "public record" as defined in Chapter 42.56 RCW. Any documents submitted to HCA by Receiving Party may also be construed as "public records" and therefore subject to public disclosure.

11. Data Shared with Subcontractors

The Receiving Party will not enter into any Subcontract without the express, written permission of HCA, which will approve or deny the proposed contract in its sole discretion. If Data access is to be provided to a Subcontractor under this DSA, the Receiving Party must include all of the Data security terms, conditions and requirements set forth in this 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 for any breach in the performance of the Receiving Party's responsibilities.

12. Data Breach Notification and Obligations

The Breach or potential compromise of Data shared under this DSA must be reported to the HCA Privacy Officer at PrivacyOfficer@hca.wa.gov within one (1) business days of discovery. The Receiving Party must also take actions to mitigate the risk of loss and comply with any notification or other requirements imposed by law or HCA including but not limited to RCW 42.56.590.

13. HIPAA Compliance

The Receiving Party must perform all of its duties, activities, and tasks under this DSA in compliance with HIPAA, the HIPAA Rules, and all applicable regulations as promulgated by the U.S. Department of Health and Human Services, Office for Civil Rights, as applicable.

Within ten (10) business days, Receiving Party must notify the HCA Privacy Officer at PrivacyOfficer@hca.wa.gov of any complaint, enforcement, or compliance action initiated by the Office for Civil Rights based on an allegation of violation of HIPAA or the HIPAA Rules and must inform HCA of the outcome of that action. Receiving Party bears all responsibility for any penalties, fines, or sanctions imposed against Receiving Party for violations of HIPAA or the HIPAA Rules and for any sanction imposed against its Subcontractors or agents for which it is found liable.

14. 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.

15. 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 the written assumption of the Receiving Party's obligations by the third party.

16. Dispute Resolution

The parties will use their best, good faith efforts to cooperatively resolve disputes and problems that arise in connection with this DSA. Both parties will continue without delay to carry out their respective responsibilities under this DSA while attempting to resolve any dispute. When a genuine dispute arises between HCA and the Receiving Party regarding the terms of this DSA or the responsibilities imposed

herein and it cannot be resolved between the parties' Contract Managers, either party may initiate the following dispute resolution process.

- 16.1. The initiating party will reduce its description of the dispute to writing and deliver it to the responding party (email acceptable). The responding party will respond in writing within five (5) Business Days (email acceptable). If after five (5) additional Business Days the parties have not resolved the Dispute, it will be submitted to the HCA Director, who may employ whatever dispute resolution methods the Director deems appropriate to resolve the dispute.
- 16.2. A party's request for a dispute resolution must:
 - a. Be in writing;
 - b. Include a written description of the dispute;
 - c. State the relative positions of the parties and the remedy sought;
 - d. State the Contract Number and the names and contact information for the parties;
- 16.3. This dispute resolution process constitutes the sole administrative remedy available under this DSA. There is no right under this DSA to an adjudicative proceeding under the Administrative Procedure Act.

17. 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.

18. 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.

19. Incorporated Documents and Order of Precedence

- 19.1. Each of the documents listed below is, by this reference, incorporated into this DSA as though fully set forth herein.
 - a. Schedule 1 – Description of Shared Data.
 - b. Exhibit A – Data Security Requirements.
 - c. Exhibit B – User Agreement on Non-Disclosure of Confidential Information.
 - d. Section 4 of OCIO 141.10, *Securing Information Technology Assets Standards: Data Security* ([https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets.](https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets))
- 19.2. 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.

20. Inspection

No more than once per quarter during the term of this DSA and for six (6) years following termination or expiration of this DSA, HCA 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.

21. Insurance

- 21.1. HCA certifies that it is self-insured under the State's self-insurance liability program, as provided by RCW 4.92.130, and will pay for losses for which HCA is found liable.
- 21.2. 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 upon request.
- 21.3. 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. Cyber Liability/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, 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 within one (1) Business Day of Receiving Party’s receipt of such notice.

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

22. Legal Notices

22.1. 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:

Attn:

Receiving Party:

Address:

Address:

City, State Zip:

- b. To HCA at:

Contract Administrator

Division of Legal Services

Health Care Authority

P. O. Box 42702

Olympia, Washington 98504-2702

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

23. 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 or its designee will have the right to access those records during that six-year period for purposes of auditing.

24. Responsibility

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

25. Severability

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.

26. 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, Security of Data, Data Confidentiality and Non-Disclosure of Data, HIPAA Compliance, Non PHI Data Breach Notification, Dispute Resolution, Inspection, Insurance, Maintenance of Records, and Responsibility.*

27. Term and Termination

- 27.1. Term. This DSA will begin on the date of execution and continue through December 31, 2020, unless terminated sooner as provided in this Section.
- 27.2. Termination for Convenience. HCA may terminate this DSA for convenience with thirty (30) calendar days' written notice to the other. 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.
- 27.3. Termination for Cause. HCA may terminate this DSA for default, in whole or in part, by written notice to the Receiving Party, if HCA has a reasonable basis to believe that the Receiving Party has: (1) failed to perform under any provision of this 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 terminates this DSA for default, HCA 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 may then terminate the DSA. HCA may terminate the DSA for default without such written notice and without opportunity for correction if HCA has a reasonable basis to believe that a Client's health or safety is in jeopardy. The determination of whether or not the Receiving Party corrected the noncompliance will be made by HCA, in its sole discretion.

28. 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.

29. 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.

Schedule 1: Description of Shared Data

HCA will provide the following Data to Receiving Party through SFT for use in Proposal development for HCA RFP 2516, Medicaid Managed Care Dental.

1. Dental Data Book

a. *Managed Care RFP Data Book* Narrative, including:

- i. Detailed information about specific components of the Washington dental program;
- ii. A description of the data and methodology underlying the Dental Data Book; and
- iii. Instructions for populating the cost proposal template.

b. *Attachment 1: Data Dictionary*. Defines the fields provided in supplemental data files along with crosswalk tables and other technical specifications used in summarizing data for the Dental Data Book. This includes technical information used to identify diabetics and pregnant women for targeted oral health initiatives.

c. *Attachment 2: Cost Model*. Actuarial cost models by region, aid category, and age/gender band. Services have been stratified into general classes covered under dental managed care, with additional service cost summarized for enhanced service payments that will be funded outside the risk-based capitation rates. Cost models are provided separately by provider setting, identifying services in a clinic (FQHC or tribal) and other services. Experience data within the cost models is not adjusted to reflect claims completion, trend, fee schedule changes, benefit policy changes, or other common adjustments.

d. *Attachment 3: Flat Data Files*. Contains annual and monthly membership and incurred claims information for calendar year 2016 and 2017. The annual files contain more detailed information about covered populations. The monthly files are to be used by Receiving Party/Bidder in developing claims completion estimates.

i. Claims by Year

1. Incurred Year (2016, 2017);

2. Age Band:

a. 0-20

b. 21-64

c. 65+

3. Category of Aid:

- a. Aged Blind Disabled (ABD)
 - b. Apple Health Adult Coverage (AHAC)
 - c. Community of Programs Entry System (COPES)
 - d. Developmental Disabilities Administration (DDA)
 - e. Family
 - f. Foster Care (FC)
 - g. State Children's Health Insurance Program (SCHIP)
4. Member Region (1-10);
 5. Member County;
 6. Clinic Encounter Claim (Y, N);
 7. Federally Qualified Health Clinic (FQHC)/Tribal Flag (FQHC, TRBL, NA);
 8. Dual Eligible (Y, N);
 9. Third-Party Liability (Y, N);
 10. Access to Baby and Child Dentistry (ABCD) Flag (Y, N);
 11. Nursing Facility (NF)/Alternative Living Facility (ALF) Place of Service (POS) (Y, N);
 12. Developmental Disability (DD) Flag (Y, N);
 13. American Indian/Alaska Native (AI/AN) Flag (Y, N);
 14. Pregnant Flag (Y, N);
 15. Diabetes Flag (Y, N);
 16. Class (Exclude, I, II, III, Other);
 17. Category of Service;
 18. Paid Amount;
 19. Utilization; and
 20. Third Party Liability (TPL) Cost Avoidance Amount.

ii. Claims by Month

1. Incurred Month (YYYYMM);
2. Paid Month;
3. Age Band:
 - a. 0-20
 - b. 21-64
 - c. 65+
4. Category of Aid:
 - a. Aged Blind Disabled
 - b. AHAC
 - c. COPES
 - d. DDA
 - e. Family
 - f. FC
 - g. SCHIP
5. Member Region (1-10);
6. Clinic Encounter Claim (Y, N);
7. FQHC/Tribal Flag (FQHC, TRBL, NA);
8. Dual Eligibility (Y, N);
9. Third-Party Liability (Y, N);
10. DD Flag (Y, N);
11. AI/AN Flag (Y, N);
12. Class (Exclude, I, II, III, Other);
13. Paid Amount;
14. Utilization; and
15. TPL Cost Avoidance Amount.

iii. Membership by Year:

1. Incurred Year (2016, 2017);
2. Age Band:
 - a. 0-20
 - b. 21-64
 - c. 65+
3. Category of Aid:
 - a. Aged Blind Disabled
 - b. AHAC
 - c. COPES
 - d. DDA
 - e. Family
 - f. FC
 - g. SCHIP
4. Member Region (1-10);
5. Member County;
6. Dual Eligible (Y, N);
7. Third-Party Liability (Y, N);
8. NF/ALF POS (Y, N);
9. DD Flag (Y, N);
10. AI/AN Flag (Y, N);
11. Pregnant Flag (Y, N);
12. Diabetes Flag (Y, N); and
13. Member Months.

iv. Membership by Month:

1. Incurred Month (YYYYMM);

2. Age Band:

a. 0-20

b. 21-64

c. 65+

3. Category of Aid:

a. Aged Blind Disabled

b. AHAC

c. COPES

d. DDA

e. Family

f. FC

g. SCHIP

4. Member Region (1-10);

5. Dual Eligible (Y, N);

6. Third-Party Liability (Y, N);

7. DD Flag (Y, N);

8. AI/AN Flag (Y, N); and

9. Member Months.

e. *Attachment 4: Cost Proposal Template.* Cost Proposal Template is to be completed by Receiving Party/Bidder in conjunction with an actuarial certification in support of proposed capitation rates to be paid effective January through December 2019. Instructions for completing this template are outlined in Section IV of the *Managed Care RFP Data Book* Narrative. Receiving Party/Bidder should review the entire document and attached workbook prior to completing the cost proposal template.

2. Provider Network Submission Files.

a. GeoRpt – Geo program

- b. *Enrollee File*. File containing Data on Medicaid Clients to enable Receiving Party to determine network adequacy, in accordance with RFP 2516, Sections 3.3 and 3.4.
 - i. Table_SID – unique, table assigned, client key;
 - ii. City – Client’s City;
 - iii. State – Client’s State;
 - iv. ZIP_Code – Client’s Zip Code;
 - v. County – Client’s County;
 - vi. Latitude – Client’s Latitude Coordinates;
 - vii. Longitude – Client’s Longitude Coordinates; and
 - viii. ZIP_4 – Client’s USPS mail route.
- c. *Provider Network Submission Workbook*;
- d. *Page Calculation Workbook*; and
- e. *Bidder’s Instructions*.

Exhibit A – Data Security Requirements

1. Definitions

In addition to the definitions set out in section 4, *Definitions*, of the Data Share Agreement (DSA), the definitions below apply to this Exhibit.

- a. “Hardened Password” means a string of characters containing at least three of the following character classes: upper case letters; lower case letters; numerals; and special characters, such as an asterisk, ampersand or exclamation point.
 - 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.
- b. “Portable/Removable Media” means any Data storage device that can be detached or removed from a computer and transported, including but not limited to: optical media (e.g. CDs, DVDs); USB drives; or flash media (e.g. CompactFlash, SD, MMC).
- c. “Portable/Removable Devices” means any small computing device that can be transported, including but not limited to: handhelds/PDAs/Smartphones; Ultramobile PC’s, flash memory devices (e.g. USB flash drives, personal media players); and laptops/notebook/tablet computers. If used to store Confidential Information, devices should be Federal Information Processing Standards (FIPS) Level 2 compliant.
- d. “Secured Area” means an area to which only Authorized Users have access. Secured Areas may include buildings, rooms, or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.
- e. “Transmitting” means the transferring of data electronically, such as via email, SFTP, webservices, AWS Snowball, etc.
- f. “Trusted System(s)” means the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Information with written acknowledgement of receipt; (2) United States Postal Service (“USPS”) first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.
- g. “Unique User ID” means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase, or other mechanism, authenticates a user to an information system.

2. Data Transmission

- a. When transmitting HCA's Confidential Information electronically, including via email, the Data must be encrypted using NIST 800-series approved algorithms (<http://csrc.nist.gov/publications/PubsSPs.html>). This includes transmission over the public internet.
- b. When transmitting HCA's Confidential Information via paper documents, the Receiving Party must use a Trusted System.

3. Protection of Data

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

- a. Data at Rest:
 - 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.

- b. **Paper documents.** Any paper records containing Confidential Information must be protected by storing the records in a Secured Area that is accessible only to authorized personnel. When not in use, such records must be stored in a locked container, such as a file cabinet, locking drawer, or safe, to which only authorized persons have access.

4. Data Segregation

HCA's Data received under this DSA must be segregated or otherwise distinguishable from non-HCA Data. This is to ensure that when no longer needed by the Receiving Party, all of HCA's Data can be identified for return or destruction. It also aids in determining whether HCA's Data has or may have been compromised in the event of a security breach.

- a. HCA's Data must be kept in one of the following ways:
 - i. on media (e.g. hard disk, optical disc, tape, etc.) which will contain only HCA Data; or
 - ii. in a logical container on electronic media, such as a partition or folder dedicated to HCA's Data; or
 - iii. in a database that will contain only HCA Data; or
 - iv. within a database and will be distinguishable from non-HCA Data by the value of a specific field or fields within database records; or
 - v. when stored as physical paper documents, physically segregated from non-HCA Data in a drawer, folder, or other container.
- b. When it is not feasible or practical to segregate HCA's Data from non-HCA data, then both HCA's Data and the non-HCA data with which it is commingled must be protected as described in this Exhibit.

5. Data Disposition

When the Confidential Information is no longer needed, except as noted below, the Data must be returned to HCA or destroyed. Media are to be destroyed using a method documented within NIST 800-88 (<http://csrc.nist.gov/publications/PubsSPs.html>).

- a. For HCA's Confidential Information stored on network disks, deleting unneeded Data is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in Section 3, above. Destruction of the Data as outlined in this section of this Exhibit may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

User Agreement on Non-Disclosure of Confidential Information

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

Confidential Information

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

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

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

Regulatory Requirements and Penalties

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

User Assurance of Confidentiality

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

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

Signature

Print User’s Name	User Signature	Date

Certification of Destruction/Disposal of Protected Health Information (PHI)

NAME OF RFP BIDDER/RECEIVING PARTY:	RFP PROPOSAL DUE DATE: 6/29/2018	DATA SHARE AGREEMENT #:
DATE HCA DATA ACCESSED/SENT: ____/____/____	APPARENTLY SUCCESSFUL BIDDER (ASB) ANNOUNCEMENT DATE: 08/06/2018	

____ (RFP Bidder/Receiving Party) hereby certifies that the data which contains the protected health information (PHI) and received as a part of the Request for Proposal (RFP) 2516 has been:

☐

DISPOSED OF/DESTROYED ALL COPIES

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

Description of Information Disposed of/ Destroyed

Date of Destruction: ____/____/____

Method(s) of destroying/disposing of PHI: _____

Disposed of/Destroyed by: _____

Signature

Print Name

Title

____/____/____
Date