Washington State Health Care Authority	**Data Share Agreement**	HCA Contract Number: KXXXX Receiving Party Contract Number: _____

This Data Share Agreement ("Agreement" or "DSA") is made by and between the state of Washington Health Care Authority ("HCA") and the party whose name appears below, ("Receiving Party")

Receiving Party Name	*Receiving Party doing business as (DBA)*
Receiving Party Address	*Receiving Party Contact Name, Title*
Receiving Party Contact Telephone	*Receiving Party Contact Email Address*

HCA Program	*HCA Division/Section*
HCA Contact Name, Title	*HCA Contact Address*
	626 8th Avenue SE, PO Box 45564 **Olympia, WA 98504-5564**
HCA Contact Telephone	*HCA Contact Email Address*

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

Receiving Party Signature	*Printed Name and Title*	*Date Signed*
HCA Signature	*Printed Name and Title*	*Date Signed*
	Melanie Anderson, Contracts Administrator	

Table of Contents

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

Schedule 1: Description of Shared Data

Exhibit A: Data Security Requirements
Exhibit B: User Agreement on Non-Disclosure of Confidential Information

Purpose of the DSA

The purpose of this Data Share Agreement (DSA) is to identify, describe and protect the HCA data to be provided to the Receiving Party for the Receiving Party to be used for purposes of carrying out the activities necessary to respond to RFP No. K-1807.

In order to evaluate unit cost levels, the HCA requires the Receiving Party to download a "Pricing Summary" file from Milliman FTP, which provides the Receiving Party historical paid claims data. The Receiving Party will input their unit cost levels and provide detailed pricing database files.

Justification and Authority for Data Sharing

The Data to be shared under this DSA are necessary for the Receiving Party to properly respond to HCA RFP No. K-1807 and are justified by CFR 164.514(e).

Definitions

"Agency" means the state of Washington Health Care Authority ("HCA") and includes any division, section, office, unit, officers or other officials lawfully representing HCA.
"Agreement" means this Data Share Agreement that is the entire written agreement between HCA and the Receiving Party with respect to the subject matter of this agreement and includes all documents attached or incorporated by reference.
"Authorized User" means an individual or individuals with an authorized business need to access HCA's Confidential Information under this Agreement.
"Breach" means the unauthorized acquisition, access, use, or disclosure of Data shared under this Agreement that compromises the security, confidentiality or integrity of the Data.
"CFR" means the Code of Federal Regulations. All references in this Data Share Agreement to CFR chapters or sections shall include any successor, amended, or replacement regulation. The CFR may be accessed at http://www.ecfr.gov/cgi-bin/ECFR?page=browse
"Client" means an individual who is eligible for or receiving federal or state funded 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 Agreement
"Contract Manager" means the individual identified on the cover page of this DSA who will provide oversight of the activities conducted under this DSA.
"Data" means the information that is disclosed or exchanged as described by this Data Share Agreement (DSA). For purposes of this DSA, Data means the same as "Confidential Information."
"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.
"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 USCA 1232g(a)(4)(b)(iv).
"ProviderOne" means the Medicaid Management Information System that is the State's Medicaid payment system managed by HCA.
"RCW" means the Revised Code of Washington. All references in this Agreement to RCW chapters or sections shall include any successor, amended, or replacement statute. Pertinent RCW chapters can be accessed at: http://apps.leg.wa.gov/rcw/.
"Regulation" means any federal, state, or local regulation, rule, or ordinance.
"Receiving Party" means the entity that is identified on the cover page of this DSA and is a party to this Agreement, and includes the entity's owners, members, officers, directors, partners, trustees, employees, and Subcontractors and their owners, members, officers, directors, partners, trustees, and employees.
"Sensitive Information" means information that is not specifically protected by law, but should be limited to official use only, and protected against unauthorized access.
"Subcontract" means any separate agreement or contract between the Receiving Party and an individual or entity ("Subcontractor") to perform any duties that give rise to a business requirement to access the Data that is the subject of this DSA.
"Subcontractor" means any separate agreement or contract between the Receiving Party and an individual or entity ("Subcontractor") to provide services or perform any duties that give rise to a business requirement to access the Data that is the subject of this DSA.
"USC" means the United States Code. All references in this Data Share Agreement to USC chapters or sections shall include any successor, amended, or replacement statute. The USC may be accessed at http://uscode.house.gov/
"Use" includes the sharing, employment, application, utilization, examination, or analysis, of Data.
"WAC" means the Washington Administrative Code. All references in this Agreement to WAC chapters or sections shall include any successor, amended, or replacement regulation. Pertinent WAC chapters or sections can be accessed at: http://apps.leg.wa.gov/wac/.

Description of Data to be Shared

The Data to be shared is set out in attached Schedule 1: Five (5) *Claims Pricing Files*
The Data will be provided *via a Milliman Secure FTP site. Milliman will provide access to the Receiving Party and will be shared one (1) time.*

Data Classification

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

Constraints on Use of Data

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

1.2. This Agreement 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 purposes described herein. Any ad hoc analyses or other use or reporting of the Data is not permitted without HCA's prior written consent.

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

Security of Data

1.4. Data Protection

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

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

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

1.5. Data Security Standards

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

1.6. 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 6 *Data Disposition,* except as required to be maintained for compliance or accounting purposes.

Data Confidentiality and Non-Disclosure

1.7. Data Confidentiality.

The Receiving Party shall not use, publish, transfer, sell or otherwise disclose any Confidential Information gained by reason of this Data Share Agreement for any purpose that is not directly connected with the purpose and justification of this DSA set out in Sections 0 and 0 above,nor shall it attempt to associate the Confidential Information with particular individuals or contact individuals who are the subject of the Confidential Information 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.

1.8. Non-Disclosure of Data

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

Each employee who will access the Data will be required to sign the *User Agreement on Non-Disclosure of Confidential Information*, Exhibit B hereto. The Receiving Party shall 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 yearsfrom the date the employee's access to the data ends. The documentation must be available to HCA upon request.

1.9. Penalties for Unauthorized Disclosure of Data

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

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

Public Disclosure

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

Data Shared with Subcontractors

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

Data Breach Notification and Obligations

1.10. The HCA Privacy Point of Contact for the Receiving Party for all reporting and notification communications required under this Section 0 *Data Breach Notifications and Obligation*s is*:*

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

1.11. **Breach Notification**.

a) In the event of a Breach of unsecured Data or disclosure that compromises the privacy or security of Data obtained from HCA or involving HCA Clients, including any use or disclosure that is not expressly permitted by this Agreement, Receiving Party must take actions to mitigate the risk of loss and must comply with the requirements of this Section.

b) Receiving Party must notify the contact identified in Subsection 1.10 by telephone and in writing (email acceptable) within five (5) business days of discovery of any acquisition, access, use or disclosure of the Data not allowed by the provisions of this Agreement or not required by law, or any potential Breach of security or privacy of Data by the Receiving Party or its Subcontractors or agents. If Receiving Party does not have full details at that time, it must report what information it has, and provide full details within 15 days after discovery.

c) Receiving Party will follow telephone or e-mail notification with a written (fax or email acceptable) explanation of the Breach, to include the following: date and time of the Breach, date Breach was discovered, location and nature of the Data, type of Breach, origination and destination of Data, Receiving Party unit and personnel associated with the Breach, detailed description of the Breach, anticipated mitigation steps, and the name, address, telephone number, fax number, and email of the individual who is responsible as the Receiving Party primary point of contact. Receiving Party will coordinate and cooperate with HCA to provide a copy of its investigation and other information requested by HCA, including advance copies of any required notifications for HCA's review before disseminating and verification of the dates notifications were sent.

1.12. Additional Notifications

If Receiving Party or any subcontractor or agent of Receiving Party actually makes or causes, or fails to prevent, a use or disclosure constituting a Breach, and if notification of that use or disclosure must (in the judgment of HCA) be made under the HIPAA Breach Notification Rule, or RCW 42.56.590 or RCW 19.254.010, or other law or rule, then:

a) HCA may choose to make any required notifications to the individuals, to the U.S. Department of Health and Human Services Secretary (DHHS) Secretary, and to the media, or direct Receiving Party to make them or any of them.

b) In any case, Receiving Party will pay the reasonable costs of notification to individuals, media, and governmental agencies and of other actions HCA reasonably considers appropriate to protect Clients (such as paying for regular credit watches in some cases).

c) Receiving Party will compensate Clients for harms caused to them by any Breach or possible Breach.

1.13. Receiving Party's obligations regarding breach notification survive the termination of this Agreement and continue for as long as Receiving Party maintains the Data and for any breach or possible breach at any time.

2. Non PHI Data Breach Notification

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

Amendments and Alterations

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

Assignment

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

Dispute Resolution

In the event that a dispute arises under this Agreement, the parties will make every effort to resolve the dispute informally and at the lowest level. If a dispute cannot be resolved informally a Dispute Board will determine resolution in the following manner:
(a) HCA will appoint one member to the Dispute Board and Receiving Party will appoint a second member. These first two members will select the third member;
(b) The Dispute Board will review the facts, DSA terms, and applicable statutes and rules and as quickly as reasonably possible, make a written determination of the dispute, including its analysis

and reasoning for the decision based on the application of the DSA terms, and applicable statutes and rules to the facts;
(c) Participation in this dispute process must precede any judicial or quasi-judicial action and will be the final administrative remedy available to the parties.

Entire Agreement

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

Governing Law and Venue

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

Incorporated Documents and Order of Precedence

2.1. Each of the documents listed below is, by this reference, incorporated into this Agreement 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

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

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

b) Sections of this Data Share Agreement;

c) Attachments, Exhibits and Schedules to this Data Share Agreement.

Inspection

No more than once per quarter during the term of this Agreement and for one (1) year following termination or expiration of this Agreement, HCA shall have the right at reasonable times and upon no less than 15 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 Agreement, and applicable laws and regulation.

Insurance

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

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

2.5. Required Insurance or Self-Insured Equivalent

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

Legal Notices

2.6. 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:

[Address of Receiving Party]

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.

Maintenance of Records

The Receiving Party shall maintain records related to compliance with this Agreement for six (6) years after expiration or termination of this Agreement.

Responsibility

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

Severablility

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

Survival Clauses

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

Term and Termination

2.7. Term. This Agreement shall begin on *November 17, 2016* or date of execution, whichever is later, and continue through *July 28, 2017* unless terminated sooner as provided in this Section.

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

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

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

Waiver

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

Signatures and Counterparts

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

Schedule 1: Description of Shared Data

Overview

In order to evaluate unit cost levels, we ask the Receiving Party to respond to the data request below. Milliman will be providing files for Receiving Party to populate. Please see section titled 'Specific Instructions' for details of the data request.

Specific Instructions

To complete the analyses of unit cost levels and the response for Exhibit 5.1, Admnistrative Fee Proposal, the Receiving Party must download a fourth file, "Pricing Summary.xls", from the Milliman FTP to input the unit cost level results.

The "Pricing Summary.xls" file is a summary the unit cost levels for five (5) files of historical paid claims:

A. Facility Inpatient.mdb
B. Facility Outpatient.mdb
C. Ambulatory surgery center.mdb
D. Professional.mdb (including M.D., D.O, and ARNP claims)
E. Ancillary Providers.mdb

Summary results of the claims pricing calculations, including total costs, must be input by the Receiving Party into the "Pricing Summary.xls" and uploaded to the Milliman FTP site along with the detailed pricing database files.

The claim files provided by the HCA include a historical sample of non-Medicare UMP Members. Each database file includes a query "Carrier Summary" which will summarize the pricing information into two (2) columns: "In Network Allowed Charges", and "Alternative Provider Allowed Charges". The Receiving Party will need to copy these two (2) columns into the excel file titled "Pricing Summary.xls", provided by the HCA through the Milliman FTP site.

The file "Pricing Summary.xls" calculates the total reported unit cost for each of the five (5) files based on the Receiving Party's populated values. Not all unit cost levels will be used in the evaluation and scoring of the Proposal. Unit cost levels should be reported based upon the date-of-service reported on the claim, and as specific to the type of provider and geographic location of the claim. The Receiving Party's response to the Exhibit 3, Provider Network, can address any possible improvements to the reported unit cost levels in future years or the level of disruption within the claim sample and the current networks.

Milliman will use the database files to validate the values populated by the Receiving Party the pricing summary and potentially perform a more detailed analysis of the files. The more detailed analysis may include understanding the likelihood of alternative provider utilization, or a comparison to current hospital discount performance. By responding to this request, the Receiving Party authorizes Milliman to use the data in such further analysis. **The HCA will *not* receive a copy of the detailed pricing files**. Any discrepancies discovered during validation will supersede the Bidder's populated pricing summary.

Database Fields included in each of the five (5) pricing files, supplied by the HCA:

A. Patient location (5-digit ZIP Code)
B. Provider tax ID
C. Tax ID Name
D. National Provider ID for Provider of Service
E. NPI Name
F. NPI or TIN ZIP Code (5-digit ZIP Code)
G. Claim number
H. Claim line number
I. Begin Service Date
J. End Service Date
K. Primary diagnosis code
L. Primary diagnosis code type (ICD 9 or ICD10)
M. Procedure code (HCFA revenue for facility, CPT or HCPCS for practitioner)

N. Procedure code modifier
O. Place of service code
P. DRG (for inpatient hospital claims)
Q. Milliman Global RVUs
R. Units
S. Provider/Specialty type code
T. Type of service code
U. Submitted or Billed Charges
V. Metropolitan Statistical Area (MSA)
W. Metropolitan Statistical Area Description for Grouping and Ordering

Key Elements to Be Addressed

To submit pricing, the Receiving Party is required to populate the following fields in each of the five (5) claims files, per the instructions below:

A. In Proposed Network Claim Indicator (as described below)
B. Allowed Charge 1 - after applying Network Unit Cost Levels under Method #1 as described below.
C. Alternative Provider Tax ID 2 (Method #2 as described in below)
D. Alternative NPI for Provider of Service 2 (Method #2 as described in below)
E. Alternative Provider Name 2 (Method #2 as described in below)
F. Alternative Provider 5 digit zip (Method #2 as described below)
G. Allowed Charge after Discount 2(Method #2 as described below)
H. Allowed Portion with FFS Contract – the percentage of allowed charge after discount that is under a Fee-for-Service (FFS) contract.

The pricing should be done based on contract provisions at the time and date-of-service, and not based on current or future contract negotiations. If the Bidder is unable to populate the discount pricing based on contracts in place for the service period of the sample, indicate the historical time period that the pricing is based on in the provider network narrative. The application of Network Unit Cost levels should be based upon existing provider contracts. The pricing should be done on a line by line basis and consistent with the actuarial standards of practice. If this basis cannot be followed, explain how the basis used compares to the estimation of line by line pricing.

The first step for populating the files relating to claims pricing is a determination if the servicing provider on the claim is in the current network. This designation will be noted by populating the “In-Network Claim” Indicator with a “Yes” **for those providers considered participating as of January 31, 2017**. For in-network claims the field “Allowed Charge 1” should reflect the level of unit cost for the servicing provider’s contract. **All attempts should be made to populate this amount field with a value as close as possible to what the actual allowed charges would be in the adjudication of the claim on January 31, 2017 for the date-of-service noted on the claim.**

For Out-of-network claims, the “In-Proposed Network Claim” Indicator populated with “No”, and the pricing should reflect two (2) methods:

For Method #1, assume Members do not change providers. Price these claims using the provider’s billed charges. Populate “Allowed Charge 1” after discount to be equal to submitted charges, reflecting no savings. For Method #2, assume that Members change to the closest in-network substitute provider who is accepting new patients and appropriate for the applicable service or treatment Populate “Allowed Charge 2” with the network unit cost levels to be the contracted cost for this claim.

For all Out-of-network claims additional information for the alternative provider used in Method #2 will need to be provided including Provider tax ID, name, and 5-digit zip. The query Carrier Summary will total the Allowed Charge 1 for the In-Network claims and Allowed Charge 2 for the claims where the servicing provider is out of network and an Alternative Provider is used. Once copied to the Pricing Summary workbook the discount and percentage of charges assumed to go through Alternative Providers.

For both In-Network and Out-of-Network claims, please populate he field “Allowed Portion with FFS Contract,” with the percentage of the actual allowed charges that are under a Fee-for-Service (FFS) contract.

Exhibit A- Data Security Requirements

Definitions

In addition to the definitions set out in Section 0 of the Data Share Agreement, the definitions below apply to this Exhibit.

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

b. "Secured Area" means an area to which only Authorized Users have access. Secured Areas may include buildings, rooms or locked storage containers (such as a filing cabinet) within a room, as long as access to the Confidential Information is not available to unauthorized personnel.

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

d. "Trusted Systems" means the following methods of physical delivery: (1) hand-delivery by a person authorized to have access to the Confidential Data with written acknowledgement of receipt; (2) United States Postal Service ("USPS") first class mail, or USPS delivery services that include Tracking, such as Certified Mail, Express Mail or Registered Mail; (3) commercial delivery services (e.g. FedEx, UPS, DHL) which offer tracking and receipt confirmation; and (4) the Washington State Campus mail system. For electronic transmission, the Washington State Governmental Network (SGN) is a Trusted System for communications within that Network.

e. "Unique User ID" means a string of characters that identifies a specific user and which, in conjunction with a password, passphrase, or other mechanism, authenticates a user to an information system.

Data Transmitting

a. When transmitting HCA's Confidential Information electronically, including via email, the Data must be protected by:

   i. Transmitting the Data within the State Governmental Network (SGN) or Receiving Party's internal network; or

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

b. HCA's Confidential Information will not be transmitted via facsimile (fax).

c. When transmitting HCA's Confidential Information via paper documents, the Receiving Party must use a Trusted System.

Protection of Data

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

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

b. **Network server disks.** Data stored on hard disks mounted on network servers and made available through shared folders. Access to the Data will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has authenticated to the network using a Unique User ID and Hardened Password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area that is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

   Data Destruction: For HCA's Confidential Information stored on network disks, deleting unneeded Data is sufficient as long as the disks remain in a Secured Area and otherwise meet the requirements listed in the above paragraph. Destruction of the Data as outlined in Section 6: *Data Disposition* of this Exhibit may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

c. **Removable Media, including Optical discs (CDs or DVDs) in local workstation optical disc drives and which *will not be transported out of a secure area***. Confidential Information provided by HCA on removable media, such as optical discs or USB drives, which will be used in local workstation optical disc drives or USB connections will be encrypted with 128-bit AES encryption or better. When not in use for the contracted purpose, such discs must be locked in a drawer, cabinet or other container to which only Authorized Users have the key, combination or mechanism required to access the contents of the container. Workstations that access Confidential Information on optical discs must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. **Optical discs (CDs or DVDs) in drives or jukeboxes attached to servers and which *will not be transported out of a secure area*.** Confidential Information provided by HCA on optical discs which will be attached to network servers will be encrypted with 128-bit AES encryption or better. Access to Data on these discs will be restricted to Authorized Users through the use of access control lists which will grant access only after the Authorized User has been authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on discs attached to such servers must be located in an area which is accessible only to authorized personnel, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

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

Protection of Data Stored on Portable Devices or Media

HCA's Data must ***not*** be stored by the Receiving Party on portable devices or media unless specifically authorized within the Data Share Agreement. If so authorized, the Receiving Party must protect the Data as provided in this Section 4.
Portable devices are any small computing device that can be transported, including but are not limited to: handhelds/PDAs/phones; Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players); and laptop/notebook/tablet computers.
Portable media means any Data storage device that can be detached or removed from a computer and transported, including but not limited to: optical media (e.g. CDs, DVDs); magnetic media (e.g. floppy disks, tape, Zip or Jaz disks); USB drives; or flash media (e.g., CompactFlash, SD, MMC).
For Data stored on Portable devices or media, Receiving Party must:

f. Encrypt the Data with a key length of at least 128 bits using an industry standard algorithm, such as AES;

g. Ensure that portable devices such as flash drives are Federal Information Processing Standards (FIPS) Level 2 compliant;

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

i. Manually lock devices whenever they are left unattended and set devices to lock automatically after a period of inactivity, if this feature is available. The maximum period of inactivity is 20 minutes.

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

   i. Keeping them in locked storage when not in use;
   ii. Using check-in/check-out procedures when they are shared;
   iii. Maintaining an inventory; and
   iv. Ensuring that when being transported outside of a Secured Area, portable devices and media with Data are under the physical control of an Authorized User.

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 no non-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 no non-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.

Data Disposition

When the Confidential Information is no longer needed, except as noted in **Error! Reference source not found.**, the Data must be returned to HCA or destroyed. Media on which Data may be stored and associated acceptable methods of destruction are as follows:

Data stored on:	Will be destroyed by:
Server or workstation hard disks, or Removable media (e.g. floppies, USB flash drives, portable hard disks, Zip or similar disks)	Using a "wipe" utility which will overwrite the Data at least three (3) times using either random or single character Data, or Degaussing sufficiently to ensure that the Data cannot be reconstructed, or Physically destroying the disk
Paper documents with Category 3 and higher Data	Recycling through a contracted firm provided the contract with the recycler assures that the confidentiality of Data will be protected.
Paper documents containing confidential information requiring special handling (e.g. protected health information)	On-site shredding by a method that renders the Data unreadable, pulping, or incineration
Optical discs (e.g. CDs or DVDs)	Incineration, shredding, or cutting/breaking into small pieces.
Magnetic tape	Degaussing, incinerating or crosscut shredding

Exhibit B- Non-Disclosure Agreement

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 (Agreement).

Confidential Information

"Confidential Information" means information that is exempt from disclosure to the public or other unauthorized persons under Chapter 42.56 RCW or other federal or state laws. Confidential Information includes, but is not limited to, Protected Health Information and Personal Information. 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