ORIGINAL

Washington State Health Care Authority	CONTRACT AMENDMENT	HCA Contract No.: K5893 Amendment No.: 1 WHATCOM COUNTY CONTRACT NO. 202205001-1

THIS AMENDMENT TO THE CONTRACT is between the Washington State Health Care Authority and the party whose name appears below, and is effective as of the date set forth below.

CONTRACTOR NAME	**CONTRACTOR doing business as (DBA)**
Whatcom County Corrections	
CONTRACTOR ADDRESS Public Safety Building, 311 Grand Ave Bellingham, WA 98225	**CONTRACTOR CONTRACT MANAGER** Name: Wendy Jones Email: wjones@co.whatcom.wa.us

AMENDMENT START DATE	**AMENDMENT END DATE**	**CONTRACT END DATE**
July 1, 2022	June 30, 2023	June 30, 2023
Prior Maximum Contract Amount	**Amount of Increase**	**Total Maximum Compensation**
$149,839	**$180,291**	**$330,130**

WHEREAS, HCA and Contractor previously entered into a Contract to develop and implement or expand the MOUD in Jails program, and;

WHEREAS, HCA and Contractor wish to amend the Contract pursuant to Section 4.3, *Amendments* to extend the term, add additional funds, incorporate work expectations and deliverables for the new term, and incorporate a Data security requirements;

NOW THEREFORE, the parties agree the Contract is amended as follows:

1. **Section 3.2. TERM**. The term of this contract is extended through June 30, 2023.

2. **Section 3.3. COMPENSATION**. The maximum compensation is increased by **$180,291** for new Total Maximum Compensation of **$330,130**.

3. **Schedule A-1, Statement of Work** is attached and incorporated herein to reflect work expectations and deliverables for the period July 1, 2022 through June 30, 2023.

4. **Attachment 1, Confidential Information Security Requirements** is hereby replaced in its entirety with **Attachment 1, Data Use Security and Confidentiality**, attached hereto.

5. **Attachment 2, Data Security Requirements** is attached and incorporated herein.

6. **Attachment 3, HCA Small Numbers Standards** is attached and incorporated herein.

7. **Attachment 4, Certificate of Destruction** is attached and incorporated herein.

8. **Section 3.7, Incorporation of Documents and Order of Precedence** is amended to include the new attachments included in this Amendment and shall now read as follows:

Each of the documents listed below is by this reference incorporated into this Contract. In the event of an inconsistency, the inconsistency will be resolved in the following order of precedence:

a. Applicable Federal and State of Washington statutes and regulations;

b. Recitals

c. Special Terms and Conditions;

d. General Terms and Conditions;

e. Attachment 1: Data Use Security and Confidentiality;

f. Attachment 2: Data Security Requirements;

g. Attachment 3: HCA Small Numbers Standards

h. Attachment 4: Certificate of Destruction

i. Schedule A: Statement of Work;

j. Exhibit A: HCA RFA #2021HCA42 for Medication for Opioid Use Disorder (MOUD) in Jails Program, dated December 29, 2021;

k. Exhibit B: *Contractor's Response* dated January 20, 2022; and

l. Any other provision, term or material incorporated herein by reference or otherwise incorporated.

9. This Amendment will be effective July 1, 2022 ("Effective Date").

10. All capitalized terms not otherwise defined herein have the meaning ascribed to them in the Contract.

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

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

CONTRACTOR SIGNATURE	PRINTED NAME AND TITLE	DATE SIGNED
Please see signature page attached		
HCA SIGNATURE DocuSigned by: Rachelle Amerine [illegible]	PRINTED NAME AND TITLE Rachelle Amerine Contracts Administrator	DATE SIGNED 8/19/2022

WHATCOM COUNTY:

Recommended for Approval:

08/22/22

Bill Elfo, Sheriff Date

Approved as to form:

Approved via email 8.17.22 (BR)

Brandon Waldron, Prosecuting Attorney Date

Approved:

Accepted for Whatcom County:

By: Satpal Sidhu

Satpal Singh Sidhu, Whatcom County Executive

STATE OF WASHINGTON)
) ss
COUNTY OF WHATCOM)

On this 14th day of September, 2022, before me personally appeared Satpal Singh Sidhu, to me known to be the Executive of Whatcom County, who executed the above instrument and who acknowledged to me the act of signing and sealing thereof.

SUZANNE M MILDNER
NOTARY PUBLIC
STATE OF WASHINGTON
Commission # 89905
APPOINTMENT EXPIRES DECEMBER 31, 2023

Suzanne M. Mildner

NOTARY PUBLIC in and for the State of Washington,
Suzanne M. Mildner, printed name.
residing at Bellingham. My
commission expires 12-31-22.

SCHEDULE A-1
Statement of Work
July 1, 2022-June 30, 2023

1. **Purpose.** To provide medication for opioid use disorder (MOUD) in jails to incarcerated individuals who present with an opioid use disorder (OUD). To support a full MOUD program which includes the following: an OUD assessment, discussion of MOUD options between the incarcerated individual and provider, initiation prior to the onset of withdrawal or continuation of MOUD, release and reentry planning to include connection with continued treatment, same day release appointment when possible or MOUD to bridge patient until next appointment and naloxone upon release. Reentry planning may also include assisting the incarcerated individual with sign-up of Medicaid, reestablishing Medicaid and connection with the Managed Care Organizations (MCOs).

   Health Equity - This project also intends to address inequities in OUD treatment and recovery services by providing medically necessary treatment for opioid use disorder to incarcerated individuals. MOUD in jails programs should understand cultural barriers and whenever possible, provide culturally appropriate services and recognize the need for inclusion of people with lived experiences in the development of the MOUD in jails programs. Additionally, this project intends to identify stigma and educate staff to ensure ongoing collaboration and openness to change.

2. **Performance Work Statement.** The Contractor shall ensure funds are responsibly used towards the MOUD program in the jail/jails and provide the core components or a progressive plan to achieve the core components which include:
   a. FDA approved medication for opioid use disorder (MOUD) must be available and offered to all incarcerated individuals who present with OUD at intake. Individuals with OUD may decline MOUD at any time, but ongoing discussions on MOUD may be offered.
   b. Methadone, buprenorphine, naltrexone should all be offered unless: (a) an opioid treatment program (OTP) is not within reasonable driving distance from the jail, in which case the jail is not required to offer methadone as an option; or (b) there is no available buprenorphine provider in the community to which the patient will likely release, in which case the jail is not required to offer buprenorphine as an option. Naltrexone may be provided in oral formulation while the patient is incarcerated, but injectable long-acting naltrexone must be offered as an option prior to release.
   c. MOUD must be continued for those who are already taking MOUD upon entering the facility, providing they wish to do so. MOUD is continued using the same medication, at the same dose unless ordered otherwise by the jail prescriber based on clinical need (documented in the patient's medical record) with the exception of injectable long-acting naltrexone which may be converted to an equivalent oral dose until just prior to release and the injectable form is restarted. Methadone may be transitioned to buprenorphine if the jail is not a licensed opioid treatment program (OTP) and the nearest OTP is not within reasonable driving distance from the jail. The presence of other illicit or controlled substances should not result in discontinuation of MOUD (consistent with the 2020 ASAM National Practice Guideline for the Treatment of Opioid Use Disorder).
   d. Assessing for risk of acute withdrawal must be done upon intake. In those instances when the individual is refusing to answer health care questions, their intake form will be flagged for medical to follow up as soon as is possible. Assessing for opioid use disorder (OUD) absent a risk of acute withdrawal must also be done, but it may be done after intake, as long as the delay does not impair the ability to begin treatment prior to release. The incarcerated individual must be educated on treatment choices and the process for continuation of access to MOUD, during incarceration, and upon release. (See resources for validated tool suggestions.)
   e. Individuals entering the facility who are physically dependent on opioids, must be offered MOUD treatment; withdrawal (including withdrawal using buprenorphine or methadone) is not acceptable unless the patient provides an informed refusal of treatment or the patient elects MOUD treatment with naltrexone, in which case withdrawal is clinically required. Use of other medications (clonidine, anti-emetics, anti-diarrheals, analgesics) may be used as adjuncts or may be used in

place of opioid agonist or partial agonist if the individual so chooses, but they may not be the only withdrawal treatment available.

f. Methadone and buprenorphine must be administered daily or more frequently. Alternate-day ("Balloon") dosing of buprenorphine may be used in rare cases based on a clinical need, the decision for which is arrived at jointly between the healthcare provider and patient and is well-documented in the patient's medical record.
g. Release planning and reentry coordination completed as soon as possible to ensure an effective plan is in place prior to release or in the event of an unexpected release of an incarcerated individual who needs continued treatment and services.
h. Provide at least 2 doses of naloxone and naloxone administration training to all incarcerated individuals with OUD upon release.
i. Schedule the first community appointment with a treatment facility, provided it is a planned release from custody.
j. Provide – in hand upon release and at no cost to the individual – sufficient doses of MOUD to bridge patient until scheduled MOUD follow-up appointment at community treatment facility (does not apply to patients treated with injectable MOUD).
    i. Individuals who are at risk of being released directly from court are informed, prior to going to court, that they may request to be transported back to the jail by staff to receive these medications prior to going home.
    ii. In situations where an appointment cannot be made, e.g., after-hours bail-out, resident is given enough medication to last until the next available appointment at the community treatment facility. If that date is unknown, the individual is given a minimum of a 7-day supply.
    iii. In situations where medications cannot be provided upon release, e.g., unscheduled release at a time when medical staff are not present in the jail, the individual is informed that he/she may either return to the jail in the morning to receive bridge medications or, if no medical staff are present the following day, will have a prescription for the same bridging medication called to a local pharmacy, at no cost to the individual.
k. Ensure policies and procedures are in place to mitigate medication diversion.

3. **Scope of Work Activities.**
    a. Whatcom County Jail will achieve the core components of the MOUD program through the following activities:
        i. Purchase of MOUD, buprenorphine. Purchasing and storage of all MOUD must follow the laws and rules pertaining to locked storage of controlled substances and any pharmacy or prescription laws.
        ii. Enter into a service agreement with Bellingham Comprehensive Treatment for the provision of Methadone for individuals who are incarcerated, and who have elected not to switch to either Buprenorphine or Naltrexone as an Opioid substitute.
        iii. Expansion of the MOUD program to the Corrections Bureau's Minimum-Security Work Center. This will involve the following additional costs:
            1. Hiring of an additional FTE RN (Registered Nurse) or LPN (Licensed Practical Nurse) through NWRC (Northwest Regional Council) for the administration of MOUD in both facilities. Federal and State regulations concerning licensure parameters will be followed.
            2. Purchase of additional supplies including, but not limited to, medication, drug testing materials, and education materials.
            3. Supplies for both the work center and the downtown jail and will include, but not limited to: drug testing materials, educational materials, and naloxone.
        iv. Information Technology assistance to develop reports or, ideally, interfaces between the Jail's (RMS) (Record Management System) and the EHR (Electronic Health Records). This may allow the pull of data points and cross-referencing information, simplifying data collection and reporting to the HCA. Absent the ability to electronically merge the data, we

anticipate coming to agreement with the HCA for the data that is most critical to support these programs, and using the custom reports created by IT.

v. Dedicated overtime funds to cover the costs of a corrections deputy at the downtown jail to assist the RN dispensing the MOUD.
vi. Increasing the number of individuals who may elect to use MOUD while in custody by lowering barriers to participation.
vii. Including additional information about the MOUD program in the Offender handbook. This will include, at minimum, the medications available and how to notify the JHP (Jail Health Program) of an interest in participating.
viii. Hiring a complex patient navigator who can assist in coordinating care for individuals who have comorbidities. This will include connections to housing, financial assistance such as Veterans services, congregate or assisted living options, etc.
ix. Continue our working relationship with the Lummi Nation's Chemical Addiction Recovery and Education program.
x. Work collaboratively with the University of Washington Addictions, Drug and Alcohol Institute (ADAI) technical assistance staff to identify training needs and participate in peer-to-peer and educational learning opportunities.

b. Whatcom County Jail is enhancing the current MOUD program with this funding. The improvements made will allow for staff to be more effective in improving the standard of care and implementation of the core components of this contract.

4. **Data Collection.**
   a. Participation requires performance monitoring activities, including requiring timely and accurate data reporting to the Health Care Authority, Division of Behavioral Health, and Recovery (HCA DBHR). Further evaluation, including on- and off-site data collection may be conducted by HCA DBHR or a third-party.
   b. The contractor will submit a monthly report, template provided by HCA DBHR, by the 10th day of the month with the following participant information, (identified as having a current OUD), for the previous month:
      i. Full name
      ii. Date of birth
      iii. Provider One #, SSN or another unique identifier
      iv. Date of booking
      v. Date MOUD started: continued or induction?
      vi. Date of release if applicable
      vii. Scheduled first MOUD appointment upon release
      viii. Which MOUD provided upon release
   c. Information will be collected via the Secure file Transfer (SFT) which HCA will assist with setting up. It will be shared with Research Data and Analysis (RDA) for evaluation purposes.

5. **Contract Management/Accounting.**
   a. Submit monthly invoices for payment.
   b. Attend monthly meetings with HCA DBHR program administrator to discuss project contract requirements, compliance, problem-solving and attend trainings.
   c. Contractor will cooperate with periodic site visits by the HCA DBHR program administrator or designee and make all relevant records and personnel available, provided all personnel making site visits will submit information in advance and pass a basic security background prior to the site visit. Additionally, all HCA personnel accessing will be asked to sign an acknowledgement that the Whatcom County Sheriff's Office/Corrections has a "No Hostage" policy.
   d. Submit a monthly report as detailed in the Deliverables Table with the invoice to the HCA DBHR program administrator.

FY2023 Contract Deliverables Table			
Activity	Deliverable	Due Date	Payment
Monthly progress reports	Report must include status of hiring staff, status of MOUD purchases and other supplies requested in the budget, core components (Section 2) being met or progress towards meeting the core components, barriers and successes, technical assistance and training participation, staff changes and additional information as needed.	Monthly: Reports due on the 10th of every month beginning with August 10, 2022.	$7,512.13 X 12 months = $90,145.50
Monthly Data Collection spreadsheet	Data spreadsheet filled out completely and shared via SFT.	Monthly: Due on the 10th of every month beginning with August 10, 2022.	$7,512.13 X 12 months = $90,145.50

6. **Billing and Payment.**
   a. This contract total is for **$180,291** and is for services rendered between July 1, 2022, and June 30, 2023.
   b. Invoice System. The Contractor shall submit invoices using State Form A-19 Invoice Voucher, or such other form as designated by HCA. Consideration for services rendered shall be payable upon receipt of properly completed invoices which shall be submitted to the program administrator, Rachel Meade, Rachel.meade@hca.wa.gov, by the Contractor monthly. The invoices shall describe and document to HCA's satisfaction a description of the work performed, activities accomplished, the progress of the project, and fees. Payments shall be in accordance with delivery and approval of deliverables as outlined in the Deliverables Table.
   c. Payment. Payment shall be considered timely if made by HCA within thirty (30) days after receipt and acceptance by HCA of the properly completed invoices. Payment shall be sent to the address designated by the Contractor on page one (1) of this Contract. HCA may, at its sole discretion, withhold payment claimed by the Contractor for services rendered if Contractor fails to satisfactorily comply with any term or condition of this Contract.
   d. Claims for payment submitted by the Contractor to HCA for amounts due and payable under this agreement that were incurred prior to the expiration date shall be paid by HCA if received by HCA within 90 days after the expiration date.
   e. HCA shall not reimburse the Contractor for any fees and expenses which exceed the maximum consideration of this contract.

Attachment 1

Data Use, Security, and Confidentiality

1. Definitions

In addition to the definitions set out in section 2, Definitions, of the Contract, the definitions below apply to this Schedule:

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

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

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

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

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

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

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

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

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

"Electronic Protected Health Information" or **"ePHI"** means Protected Health Information that is transmitted by electronic media or maintained in any medium described in the definition of electronic media at 45 C.F.R. § 160.103.

"HIPAA" means the Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191, as amended by the American Recovery and Reinvestment Act of 2009 ("ARRA"), Sec. 13400 – 13424, H.R. 1 (2009) (HITECH Act).

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

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

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

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

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

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

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

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

"Regulation" means any federal, state, or local regulation, rule, or ordinance.

"Contractor" means the entity that is identified on the cover page of this Contract and is a party to this Contract, 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 Contractor 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 Contract.

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

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

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

a. Identification of the purpose of the file;

b. Identification of costs (if any)

c. Identification of transmission method; and

d. Identification of the file layout.

Attachment 1A contains the Data Licensing Statement for this Contract

3. 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/141 10-securing-information-technology-assets. Section 4 is hereby incorporated by reference.)

The Data that is the subject of this Contract 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.

4. Constraints on Use of Data/Limited License

4.1. Subject to the Terms and Conditions of this Contract, HCA hereby grants Contractor a limited license for the access and Permissible Use of Data. This grant of access may not be deemed as providing Contractor with ownership rights to the Data. The Data being shared/accessed is owned and belongs to HCA.

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

regard to a crime any patient with a substance use disorder, except as provided at 42 C.F.R. §§ 2.12(c)(5) and 2.65.

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

4.4. This Contract does not constitute a release for Contractor to share the Data with any third parties, including Subcontractors, even if for authorized use(s) under this Contract, without the third party release being approved in advance by HCA and identified in the Data Licensing Statement(s).

4.5. Derivative Data Product Review and Release Process. All reports derived from Data shared under this Contract, produced by Contractor that are created with the intention of being published for or shared with external customers (Data Product(s)) must be sent to HCA for review of usability, data sensitivity, data accuracy, completeness, and consistency with HCA standards prior to disclosure. This review will be conducted and response of suggestions, concerns, or approval provided to Receving Party within 10 business days.

a. Small Numbers. Contractor will adhere to *HCA Small Numbers Standards*, Attachment 2. HCA and Contractor may agree to individual Permissible Use exceptions to the Small Numbers Standards, in writing (email acceptable).

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

5. Data Modification(s)

Any modification to the Purpose, Justification, Description of Data to be Shared/Data Licensing Statement(s), and Permissible Use, is required to be approved through HCA's Data Request Process. Contractor must notify HCA's Contract Manager of any requested changes to the Data elements, Use, records linking needs, research needs, and any other changes from this Contract, immediately to start the review process. Approved changes will be documented in an Amendment to the Contract.

6. Security of Data

6.1. Data Protection

The Contractor must protect and maintain all Confidential Information gained by reason of this Contract against unauthorized use, access, disclosure, modification or loss. This duty requires the Contractor 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.

6.2. Data Security Standards

Contractor must comply with the Data Security Requirements set out in Attachment 1 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 Contract.

6.3. Data Disposition and Retention

a. Contractor will dispose of HCA Data in accordance with this section.

b. Upon request by HCA, or at the end of the Contract term, or when no longer needed, Confidential Information/Data must be disposed of as set out in Attachment 1, Section 5 *Data Disposition,* except as required to be maintained for compliance or accounting purposes. Contractor will provide written certification to HCA of disposition using Attachment 4, *Certification of Destruction/Disposition of Confidential Information.*

7. Data Confidentiality and Non-Disclosure

7.1. Data Confidentiality.

The Contractor will not use, publish, transfer, sell, or otherwise disclose any Confidential Information gained by reason of this Contract for any purpose that is not directly connected with the purpose, justification, and Permissible Use of this Contract, as set out in the attached Data Licensing Statement(s) except: (a) as provided by law; or (b) with the prior written consent of the person or personal representative of the person who is the subject of the Data.

7.2. Non-Disclosure of Data

The Contractor must ensure that all employees or Subcontractors who will have access to the Data described in this Contract (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 Contract before gaining access to the Data identified herein. The Contractor will also instruct and make any new employe aware of the use restrictions and protection requirements of this Contract before they gain access to the Data.

The Contractor will ensure that each employee or Subcontractor who will access the Data signs the *User Agreement on Non-Disclosure of Confidential Information*, Attachment 3 hereto. The Contractor will retair 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.

7.3. Penalties for Unauthorized Disclosure of Data

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

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

8. Data Shared with Subcontractors

The Contractor will not enter into any Subcontract without the express, written permission of HCA, which will approve or deny the proposed subcontract in its sole discretion. If Data access is to be provided to a Subcontractor under this Contract it will only be for the Permissible Use authorized by HCA and the

Contractor must include all of the Data security terms, conditions and requirements set forth in this Contract in any such Subcontract. In no event will the existence of the Subcontract operate to release or reduce the liability of the Contractor to HCA for any breach in the performance of the Contractor's responsibilities.

9. Audit

9.1. At HCA's request or in accordance with OCIO 141.10, Contractor shall obtain audits covering Data Security and Permissible Use. Contractor may cover both the Permissible Use and the Data Security Requirements under the same audit, or under separate audits. The term, "independent third-party" as referenced in this section means an outside auditor that is an independent auditing firm.

9.2. Data Security audits must demonstrate compliance with Data Security standards adopted by the Washington State Office of the Chief Information Officer (OCIO), and as set forth in Attachment 1, *Data Security Requirements*. At a minimum, audit(s) must determine whether Data Security policies, procedures, and controls are in place to ensure compliance with all Data Security Requirements set forth herein and as required by state and federal law.

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

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

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

10. Data Breach Notification and Obligations

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

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

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

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

c. A description of the types of PHI involved;

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

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

f. Any other information HCA reasonably requests.

10.3. The Contractor 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 45 C.F.R. Part 164 Subpart D; RCW 42.56.590; RCW 19.255.010; or WAC 284-04-625.

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

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

a. Computer forensics assistance to assess the impact of a Data Breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with Breach notification laws;

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

c. Regulatory defense, fines, and penalties from any claim in the form of a regulatory proceeding resulting from a violation of any applicable privacy or security law(s) or regulation(s).

10.6. Any breach of this section may result in termination of the Contract and the demand for return or disposition, as described in Section 7.3, of all HCA Data.

10.7. Contractor's obligations regarding breach notification survive the termination of this Contract and continue for as long as Contractor maintains the Data and for any Breach or potential compromise,

11. Privacy Breach Response Coverage Requirements

For the term of this Contract and 3 years following its termination or expiration, Contractor must maintain insurance to cover costs incurred in connection with a security incident, privacy Breach, or potential compromise of Data, including:

a. Computer forensics assistance to assess the impact of a Data Breach, determine root cause, and help determine whether and the extent to which notification must be provided to comply with Breach notification laws;

b. Notification and call center services for individuals affected by a security incident, or privacy Breach;

c. 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

d. 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).

12. Survival Clauses

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

Attachment 1A: Data Licensing Statement

1. Background

The state of Washington, acting by and through the Health Care Authority (HCA), issued a Request for Application (RFA) dated December 29, 2021, (Exhibit A) for the purpose of developing and implementing or continuing to expand Medication for Opioid Use Disorder (MOUD) in Jails Program in accordance with its authority under chapters 39.26 and 41.05 RCW. The resulting Statement of Work requires the jail to share specific Data with HCA regarding individuals with Opioid Use Disorder

2. Justification and Authority for Data Sharing

The Data to be shared under this DSA are necessary to comply with 2021 Engrossed Senate Bill 5476 and Engrossed Substitute Bill 5092 directing HCA to implement and enhance medication for Opioid Use Disorder in jail programs.

3. Purpose / Use / Description of Data

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

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

a. File Layout: The Parties will exchange Data using the mutually agreed upon file layouts below. The Parties may edit and/or change the *File Layout* as considered necessary.

   i. Method of Access/Transfer: Once an established Secure Data Transfer connection with the host computer at Contractor's location is confirmed, Contractor will provide Data listed in *File Layout* list below, to HCA.

   ii. Delivery Method: Secure File Transfer

   iii. Frequency of Data Delivery: Contractor will transmit Data monthly, by the 10th day of the month for the previous month.

   iv. Costs: N/A

Contractor will be sharing with HCA the following Data elements:

i. Full name

ii. Date of birth

iii. Provider One #, SSN or another unique identifier

iv. Date of booking

v. Date MOUD started: continued or induction?

vi. Date of release if applicable

vii. Scheduled first MOUD appointment upon release

viii. Which MOUD provided upon release

Attachment 2: Data Security Requirements

1. Definitions

In addition to the definitions set out in the Data Use, Security, and Confidentiality Schedule, the definitions below apply to this Attachment.

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.

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

   ii. 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 PCs, flash memory devices (e.g. USB flash drives, personal media players); and laptop/notebook/tablet computers. If used to store Confidential Information, devices should be Federal Information Processing Standards (FIPS) Level 2 compliant.

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 Contractor must use a Trusted System and must be physically kept in possession of an authorized person

3. Protection of Data

The Contractor 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.

i. 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 Contractor on Portable Devices or Media unless specifically authorized within the DSA. If so authorized, the Contractor 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 Contractor, 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

   i. in a logical container on electronic media, such as a partition or folder dedicated to HCA's Data; or

   ii. in a database that will contain only HCA Data; or

   iii. within a database and will be distinguishable from non-HCA Data by the value of a specific field or fields within database records; or

   iv. 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 Attachment.

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

5. Data Disposition

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

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 Attachment may be deferred until the disks are retired, replaced, or otherwise taken out of the Secured Area.

6. Network Security

Contractor's network security must include the following:

a. Network firewall provisioning;

b. Intrusion detection;

c. Quarterly vulnerability assessments; and

d. Annual penetration tests.

7. Application Security

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

8. Computer Security

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

9. Offshoring

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

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

Attachment 3: HCA Small Numbers Standard

1. Why do we need a Small Numbers Standard?

It is the Washington State Health Care Authority's (HCA) legal and ethical responsibility to protect the privacy of its clients and members. However, HCA also supports open data and recognizes the ability of information to be used to further HCA's mission and vision. As HCA continues down the path of Data Governance maturity, establishing standards such as this is key in helping HCA analysts and management meet the needs of external data requestors while maintaining the trust of our clients and members and complying with agency, state and federal laws and policies.

Publishing data products that include small numbers creates two concerns. As a reported number gets smaller, the risk of re-identifying an HCA client or member increases. This is especially true when a combination of variables are included in the data product to arrive at the small number (e.g. location, race/ethnicity, age, or other demographic information).

Small numbers can also create questions around statistical relevance. When it comes to publicly posting data products on HCA's internet site, or sharing outside the agency, the need to know the exact value in a cell that is less than 11 must be questioned.

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

2. Scope

HCA often uses Category 4 data to create summary data products for public consumption. This Standard is intended to define one of the requirements for a summary data product to be considered Category 1. Specifically, it is intended to define the level of suppression that must be applied to an aggregated data product derived from Category 4 data for the data product to qualify as Category 1. Category 1 products are data products that are shared external to the agency, in large part those products that are posted on HCA's Internet website (www.hca.wa.gov). The primary scope of this Standard is for those data products posted publicly (e.g. on the website), or, shared as public information.

The following are examples of when this Standard **does not** apply to data products are:

a. Those shared directly with an external entity outside HCA, the Standard suppression of small numbers would not be required. However, you should notify the recipient that the data products contains sensitive information and should not be shared or published.

b. Those exchanged under a data share agreement (DSA) that will not be posted or shared outside the Contractor.

c. Those created for HCA-only internal use.

This standard does not supersede any federal and state laws and regulation.

3. Approach

In 2017, an impromptu workgroup was formed to tackle the issue of small numbers and determine what the general approach for handling data products that contain them would be. This initial effort was led by the agency's Analytics, Interoperability and Measurement (AIM) team who had an immediate need for guidance in handling and sharing of data products containing small numbers. The result of that work was a set of Interim Small Numbers Guidelines, which required suppression of cells containing values of less than 10. In addition, data products that contain small numbers are considered Category 2 under HCA's Data Classification Guidelines.

In spring 2018, a new cross-divisional and chartered Small Numbers Workgroup was formed to develop a formal agency standard. Representatives from each of the major HCA divisions that produce data and analytic products were selected. The charter, complete with membership, can be found here (available to internal HCA staff only). The Workgroup considered other state agency standards, and national standards and methods when forming this standard. The Workgroup also consulted business users and managers to determine the potential impact of implementing a small numbers suppression standard. All of this information was processed and used to form the HCA Small Numbers Standard.

4. State and National Small Numbers Standards Considered

When developing these standards, HCA reviewed other organizations' small numbers standards at both a state and federal level. At the state level, DOH recently published a revised Small Numbers Standard, which emphasizes the need for suppression for both privacy concerns and statistical relevance. HCA also convened a meeting of other state agencies to discuss their approach and policies (if any) around Small Numbers. Feedback from that convening was also taken into consideration for this Standard as well.

Federal health organizations such as the Centers for Disease Control and Prevention (CDC) and the National Center for Health Statistics (NCHS) also maintain small numbers standards. HCA's federal oversight agency and funding partner, the Centers for Medicare and Medicaid Services (CMS) adopts suppression of any cell with a count of 10 or less.

5. WA Health Care Authority Small Numbers Standard

Any HCA external publication of data products are to be compliant with both HIPAA and Washington State privacy laws. Data products are not to contain small numbers that could allow re-identification of individual beneficiaries. HCA analysts are to adhere to the following requirements when developing Category 1 data products for distribution and publication. Category 1 data is information that can be released to the public. These products do not need protection from unauthorized disclosure, but do need integrity and availability protection controls. Additionally, all contractors (state and private) that use HCA's data to produce derivative reports and data products are required to adhere to this standard as well. HCA's Contracts team will ensure that proper contractual references are included to this and all HCA Data Release and Publishing Standards. The requirements discussed herein are not intended for Category 2, Category 3, or Category 4 data products.

6. HCA's Small Number Standard:

a. There are no automatic exemptions from this standard

b. (See Exception Request Process section below)

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

d. Exceptions to this standard will be considered on a case-by-case basis (see *Exception Request Process* section later in this document for more information).

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

f. Apply a marginal threshold of 1 - 10 and cell threshold of 1 - 10 to all tabulations

g. (0 < n < 11 suppressed).

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

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

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

7. Small Numbers Examples

a. Example (Before Applying Standard)

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

b. Example (After Applying Standard)

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

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

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

c. Example (Suppression with no aggregation)

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

d. Example (Using aggregation instead of suppression)

Age Range	County	ach	Statewide
0-6	12	26	38
7-9	15	23	38

10-12	24	33	57
TOTAL	51	82	133

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

Attachment 4: Certification of Destruction/Disposal of Confidential Information

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

NAME OF CONTRACTOR:	DATA SHARE AGREEMENT (DSA) #:

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

☐ DISPOSED OF/DESTROYED ALL COPIES

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

Description of Information Disposed of/ Destroyed

Date of Destruction: _____

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

Disposed of/Destroyed by:

Signature	Date
Printed Name:	
Title:	