Washington State Health Care Authority	**CONTRACT AMENDMENT For HARPS Services**	HCA Contract No.: K6914 Amendment No.: 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)**
North Sound Behavioral Health Administrative Services Organization, LLC	North Sound BH ASO
CONTRACTOR ADDRESS 2021 East College Way, Suite 101 Mount Vernon, WA 98273	**CONTRACTOR CONTRACT MANAGER** Name: Margaret Rojas Email: margaret_rojas@nsbhaso.org
AMENDMENT START DATE July 1, 2023	**CONTRACT END DATE** June 30, 2024

Prior Maximum Contract Amount	**Amount of Increase**	**Total Maximum Compensation**
$707,380	$0	$707,380

WHEREAS, HCA and Contractor previously entered into a Contract for Housing Support Services, and;

WHEREAS, HCA and Contractor determined that data sharing connected to providing services within the context of this Contract necessitated additional contract language, and;

WHEREAS, HCA determined that a clarification was needed in the Fidelity Review section of the Statement of Work, and;

WHEREAS, HCA and Contractor wish to amend the Contract pursuant to Section 4.4 to add a Data Share Agreement and to modify Subsection 3.3.1.2, Fidelity Review, of the Statement of Work;

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

1. Section 3, Incorporation of Documents and Order of Precedence, is amended to read as follows:

3.8 INCORPORATION OF DOCUMENTS AND ORDER OF PRECEDENCE

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:

3.8.1 Applicable Federal and State of Washington statutes and regulations;

3.8.2 Recitals;

3.8.3 Attachment 7: Data Share Agreement;

3.8.4 Special Terms and Conditions;

3.8.5 General Terms and Conditions;

3.8.6 Attachment 4: SAMHSA Award Terms;

3.8.7 Attachment 5: Federal Compliance, Certifications and Assurances;

3.8.8 Attachment 6(s): Federal Subaward Information;

3.8.9 Attachment 1(s): Statement(s) of Work;

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

2. Attachment 1, Statement of Work, Section 3, Work Expectations, Subsection 3.3, Participation in Trainings, Conference Calls and Program Meetings, Subsection 3.3.1, Trainings, Subsection 3.3.1.2, Fidelity Review, is amended in its entirety to read as follows:

   3.3.1.2 Fidelity Review. HCA will also include Contractor in the facilitation of an actual Fidelity Review of another agency. Contractor will send a minimum of one (1) FTE from the HARPS team to attend the Fidelity Review Training.

3. Attachment 7, Data Share Agreement, is added hereto and incorporated herein.

4. Effective Date. The execution of this Contract constitutes a ratification of the earlier agreement between the parties, the terms and conditions of which are contained herein. Accordingly, upon signature of both parties, this Contract is effective retroactive to July 1, 2023, regardless of the date of execution, and continues through June 30, 2024, unless terminated sooner as provided herein.

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

6. 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
DocuSigned by: Margaret Rojas 18B07DE7EA53449...	Margaret Rojas Assistant Director	10/26/2023
HCA SIGNATURE	**PRINTED NAME AND TITLE**	**DATE SIGNED**
DocuSigned by: Andria Howerton F2EF77E93FBC4D7...	Andria Howerton Deputy Contracts Administrator	10/26/2023

ATTACHMENT 7
Data Share Agreement

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

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

1.1. Identification of the purpose of the file;

1.2. Identification of costs (if any);

1.3. Identification of transmission method; and

1.4. Identification of the file layout.

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

2. Data Classification

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

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

2.1. ☐ 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.

2.2. ☐ 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.

2.3. ☐ 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;

2.4. ☒ 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.

3. Constraints on Use of Data/Limited License

3.1. 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.

3.2. For Limited Data Sets, Contractor agrees to not attempt to re-identify individuals in the Data shared or attempt to contact said individuals.

3.3. If 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.

3.4. 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.

3.5. 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).

3.6. Derivative Data Product Review and Release Process.

A. 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, approval, or notification of additional review time needed provided to Receiving Party within 10 business days. HCA reserves the right to extend the review period as needed for approval or denial.

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

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

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

A. Receiving Party must identify:

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

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

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

4. 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.

5. Security of Data

5.1. 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.

5.2. Data Security Standards

Contractor must comply with the Data Security Requirements set out in Attachment B and the Washington OCIO Security Standard, 141.10 (https://ocio.wa.gov/policies/141-securing-information-technology-assets/14110-securing-information-technology-assets.)

5.3. 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 B, 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 E, *Certification of Destruction/Disposition of Confidential Information*.

6. Data Confidentiality and Non-Disclosure

6.1. 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.

6.2. 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 employee 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 D hereto. The Contractor will retain the signed copy of the *User Agreement on Non-Disclosure of Confidential Information* in each employee's personnel file for a minimum of six years from the date the employee's access to the Data ends. The documentation must be available to HCA upon request.

6.3. 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.

7. Data Shared with Subcontractors

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 Attachment 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 Data Breach in the performance of the Contractor's responsibilities.

8. Audit

8.1. 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.

8.2. 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 B, *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.

8.3. 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.

8.4. 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.

8.5. 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.

9. Data Breach Notification and Obligations

9.1. The Data 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.

9.2. If the Data 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.

9.3. 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.

9.4. 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).

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

A. The reasonable costs of notification to individuals, media, and governmental agencies and of other actions HCA reasonably considers appropriate to protect HCA clients.

B. 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 Data Breach notification laws;

C. Notification and call center services, and other appropriate services (as determined exclusively by HCA) for individuals affected by a security incident or Data Breach, including fraud prevention, credit monitoring, and identify 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).

E. Compensation to HCA clients for harms caused to them by any Data Breach or possible Data Breach.

9.6. Any Breach of this section may result in termination of the Contract and the demand for return or disposition, as described in Section 6.3, of all HCA Data.

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

9.8. Data Breach Notification. Data Breach Notification and Obligations are detailed in Section 10.

9.9. Miscellaneous Provisions

A. Regulatory References. A reference in this Attachment to a section of HIPAA means the section as in effect or as amended.

B. Interpretation. Any ambiguity in this Attachment will be interpreted to permit compliance with the HIPAA.

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

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

10. Data Breach Response Insurance 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, Data Breach, or potential compromise of Data, including:

10.1. 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 Data Breach notification laws;

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

10.3. Data Breach resolution and mitigation services for individuals affected by a security incident or Data Breach, including fraud prevention, credit monitoring, and identity theft assistance; and

10.4. 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).

11. Survival Clauses

The terms and conditions contained in this Attachment that by their sense and context are intended to survive the expiration or other termination of this Attachment 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, Audit, HIPAA Compliance, Data Breach Notification and Obligations and Data Breach Response Coverage Requirements.*

Attachment A1: Data Licensing Statement

1. Background

The Contractor is providing services to people at risk of entering or recently discharging from a behavioral healthcare setting who don't otherwise qualify for Medicaid support. The data that the Contractor collects helps HCA monitor and track program activities.

2. Justification and Authority for Data Sharing

The Data to be shared under this Contract are necessary to comply with HIPAA rules.

3. Purpose / Use / Description of Data

The scope of this Attachment 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.

HCA is not sharing data with the Contractor. The Contractor is sharing client data with HCA.

4. Permissible Use: Contractor may only use the Data for the purposes as follows:

4.1. Monthly

4.1.1 Behavioral Health Data System (BHDS)

a. Contractor enters client data into the BHDS monthly.

b. HCA accesses client data for review.

c. HCA extracts data from BHDS and works with DBHR to determine which data points will be included (aggregate or otherwise) in a monthly report.

d. HCA reviews monthly report.

4.1.2 Monthly HARPS Participant Log

4.2 Quarterly - Contractor provides documents and spreadsheets to HCA.

5 Technical Design Specification (TDS), File Layout & Delivery Method

5.1 Data Elements from BHDS – manually entered by the Contractor into the database.

Element Name
County
Name
Age
Gender
Race

5.2 Data Elements from HARPS Monthly Participant Log – Contractor enters into spreadsheet, loads spreadsheet into MFT.

Element Name
Last Name
First Name
Client ProviderOne ID #
Client DOB
Date of First Contact w HARPS Program
Setting the person is discharging from or being diverted from (ex: Western State Hospital Discharge; Adult Behavioral Health System (ABHS) Diversion)

5.3 Data Elements from HARPS Quarterly Report Template. Report is in narrative format, using the following prompts, and is formatted into a Word document, and sent via email.

1. Please describe procurement, hiring and implementation activities to date:
2. Describe staff development activities for this reporting period (including orientation and training). Please indicate: • Date(s)/duration of the training or meeting • Subject of the training or meeting • Discuss value/impact on the pilot project.
3. Discuss any other project activities or events, including meetings with local Continuums of Care, Coordinated Entry Programs, housing, and housing services providers meetings. • Date(s)/duration of the training or meeting • Subject of the training or meeting • Discuss value/impact on the pilot project.
4. The number of individuals discharged from the state psychiatric hospitals (WSH and ESH) the HARPS team has enrolled this quarter?
5. The number of individuals discharged from the state psychiatric hospitals (WSH and ESH) the HARPS team has assisted in obtaining housing this quarter?
6. Number of landlord outreach and engagement contacts made by the HARPS Team this quarter?
7. Number of participants referred to DVR?
8. Number of participants referred to IPS Supported Employment Programs?
9. Number outreach activities to potential employers for program participants?
10. Number of enrolled individuals referred to other healthcare providers, including primary care, dental care, eye care?
11. Number of enrolled individuals referred to other community-based supports, such as long-term care services, meals on wheels, chore services, transportation assistance, shopping assistance or companion services?
12. Number of individuals enrolled that required modifications to their home to make it accessible?

13. Number of individuals currently receiving disability benefits?
14. Number of individuals assisted in applying for disability benefits?
15. Number of individuals enrolled that have no monthly income?
16. Number of individuals enrolled that have received a housing voucher?
17. Number of individuals enrolled receiving HEN or ABD?
18. Subsidies spent this quarter? GFS? GFS SUD?
19. Share a success story – do not use PHI

Attachment B: Data Security Requirements

1. Definitions

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

1.1. **"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.

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

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

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

1.2. **"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).

1.3. **"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.

1.4. **"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.

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

1.6. **"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.

1.7. **"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

2.1. 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.

2.2. 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:

3.1. **Data at Rest:**

3.1.1 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.

3.1.2 Data stored on Portable/Removable Media or Devices:

3.1.2.1 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.

3.1.2.2 HCA's data must not be stored by the Contractor on Portable Devices or Media unless specifically authorized within the Contract. If so authorized, the Contractor must protect the Data by:

a. Encrypting with NIST 800-series approved algorithms. Encryption keys will be stored and protected independently of the data;

b. Control access to the devices with a Unique User ID and Hardened Password or stronger authentication method such as a physical token or biometrics;

c. Keeping devices in locked storage when not in use;

d. Using check-in/check-out procedures when devices are shared;

e. Maintain an inventory of devices; and

f. Ensure that when being transported outside of a Secured Area, all devices with Data are under the physical control of an Authorized User.

3.2. **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 Contract 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.

4.1. HCA's Data must be kept in one of the following ways:

4.1.1 on media (e.g. hard disk, optical disc, tape, etc.) which will contain only HCA Data; or

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

4.1.3 in a database that will contain only HCA Data; or

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

4.1.5 when stored as physical paper documents, physically segregated from non-HCA Data in a drawer, folder, or other container.

4.2. 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.

4.3. 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 Contract provided it is installed with end-point encryption.

5. Data Disposition

5.1. 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 Contract, 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.

5.2. 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:

6.1. Network firewall provisioning;

6.2. Intrusion detection;

6.3. Quarterly vulnerability assessments; and

6.4. 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

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

9.2. 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 C: 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:

2.1 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 contain sensitive information and should not be shared or published.

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

2.3 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:

6.1 There are no automatic exemptions from this standard

6.2 (See Exception Request Process section below)

6.3 Standard applies for all geographical representations, including statewide.

6.4 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).

6.5 Ensure that no cells with 0 < n < 11 are reported (0 < n < 11 suppressed)

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

6.7 (0 < n < 11 suppressed).

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

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

6.10 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

7.1 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

7.2 Example (After Applying Standard)

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

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

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

7.3 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

7.4 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 D: User Agreement on Non-Disclosure of Confidential Information

(To Be Signed by Each Individual User with Access to Confidential HCA Data)

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

Confidential Information

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

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

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

Regulatory Requirements and Penalties

State laws (including, but not limited to, RCW 74.04.060, RCW 74.34.095, and RCW 70.02.020) and federal regulations (including, but not limited to, HIPAA Privacy and Security Rules, 45 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.

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

Attachment E: Certification of Destruction/Disposal of Confidential Information

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

NAME OF CONTRACTOR:	CONTRACT #:

_____ (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 destroyed, and returned if requested by HCA, 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 and/or Return:

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

Disposed of/Destroyed by:

Signature	Date
Printed Name:	
Title:	