State of Washington
Department of Corrections

DOC K11966
OCO K197
Data Share Agreement

This Data Share Agreement is made and entered into by and between the Washington State Department of Corrections, hereinafter referred to as the "Department" or "WADOC," and the Office of the Corrections Ombuds, located at 302 Sid Snyder Ave. S.W., Olympia, WA 98501, hereinafter referred to as "OCO" or "Requestor," each a "Party" and collectively the "Parties."

I. PURPOSE, USE OF DATA, DATA TRANSMISSION

1. **PURPOSE:**
   a. The purpose of this Data Share Agreement (hereinafter referred to as the "Agreement," or "DSA") is to provide the Requestor with access to all Department data to the Requestor that is necessary to facilitate the duties of the Ombuds as specified in RCW 43.06C. Methods of data delivery include, but are not limited to, paper records, portable devices, hard disk drives, optical disc drives, and access to WADOC online platforms. Read only access is provided to the Offender Management Network Information (OMNI), to allow OCO access to basic data on incarcerated individuals. Access is also provided to On-Base, to allow OCO to access grievance information on incarcerated individuals. The OMNI and On-Base applications, along with other DOC resources, will be through the DOC intranet portal, iDOC.

      No modification, either intentional or unintentional, shall be made by a member of the OCO to an incarcerated individual's records. Should any modification be necessary, the appropriate edits, changes, or alterations must be made by an authorized DOC staff member.

   b. Additional data involving mental health, sexually transmitted disease (STD), or substance abuse treatment will require a signed release of information waiver from the incarcerated individual. (See Attachment C – Health Information – specifically to be used for Mental Health and STD's release, and Attachment D - Substance Abuse).

   c. Access by the OCO will include access to Category 3, Confidential Data and Category 4 Data - Confidential Information Requiring Special Handling, based upon classification categories developed by the OCIO. (See Attachment A - Data Classification Guidelines).

   d. Data access does not include approval to conduct research and statistical analysis. These activities must go through the Washington State Institution Review Board (WSIRB) and DOC Research and Data Analytics (RDA) approval process. All WSIRB documentation must be submitted to DOC for record keeping purposes.

2. **AUTHORITY:** This information is shared to support efforts to assist in strengthening procedures and practices that lessen the possibility of actions occurring within the department of corrections that may adversely impact the health, safety, welfare, and rehabilitation of

incarcerated individuals, and that will effectively reduce the exposure of the department to litigation. (See RCW 43.06C.005).

3. **USE OF DATA:** Requestor must comply with the Washington State Office of the Chief Information Officer (OCIO), WADOC Information Technology security policies, standards, and requirements and with this Agreement, in its treatment of all data provided to Requestor by the Department.

   a. Requestor shall use all data provided by WADOC to Requestor, whether that data originated in WADOC or in another entity other than Requestor, in accordance with OCIO Standard 141.10 (the key requirements of which are contained in this Agreement) and in accordance with all other applicable state and federal laws.

4. **PERIOD OF AGREEMENT:** The term of this DSA shall begin the date of execution by the final Party, and extend through September 30, 2021, unless terminated sooner or extended as provided herein.

5. **DATA SHARE AGREEMENT MANAGERS**
   The Agreement Manager for each of the Parties shall be responsible for, and shall be the contact person for, all communications and reports regarding the performance of this Agreement.

   a. Agreement Manager for OCO: Joanna Carns, Director, Telephone: (360) 764-3168, Email: joanna.carns@gov.wa.gov
   b. Agreement Manager for DOC: Jeremy Barclay, Director of Engagement, Telephone: (360) 515-6661, Email: jeremy.barclay@doc.wa.gov

II. DATA SECURITY

1. **PROTECTION OF DATA:** All electronic data provided by WADOC shall be stored on an encrypted hard drive in a secure environment with access limited to the least number of staff needed to complete the purpose of this Agreement.

   a. **Workstation hard disk drives.** Data stored on local workstation hard disks will be encrypted with a FIPS approved cryptographic algorithm. Access will be restricted to authorized users by requiring logon to the local workstation using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards.

   b. **Network server disks.** Data stored on hard disks mounted on network servers and made available through shared folders will be encrypted with a FIPS approved cryptographic algorithm. Access to the data will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. Data on disks mounted to such servers must be located in an area which is accessible only to authorized personnel, with access controlled

through use of a key, card key, combination lock, or comparable mechanism. Backup copies must be encrypted if recorded to removable media.

c. **Optical disc drives.** OCO will use and store data provided by WADOC on optical discs (e.g. CDs, DVDs, Blu-Rays) in local workstation optical disc drives which will not be transported out of a secure area. The method of this data transmission will be encrypted with a FIPS approved cryptographic algorithm. When not in use, such discs must be locked in a drawer, cabinet or other container to which only authorized users have the key combination, or mechanism required to access the contents of the container. Workstations which access WADOC Data on optical disks must be located in an area which is accessible only to authorized individuals, with access controlled though use of key, card key, combination lock, or comparable mechanism.

   Optical discs (e.g. CDs, DVDs, Blu-Rays) in drives or other devices attached to a network - This data will be encrypted with a FIPS approved cryptographic algorithm. Access to data on these discs will be restricted to authorized users through the use of access control lists which will grant access only after the authorized user has authenticated to the network using a unique user ID and complex password or other authentication mechanisms which provide equal or greater security, such as biometrics or smart cards. The optical discs must be located in an area which is accessible only to authorized individuals, with access controlled through use of a key, card key, combination lock, or comparable mechanism.

d. **Paper documents.** Any paper records must be protected by storing the records in a secure area which is only accessible to authorized individuals. 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.

e. **Portable devices.** Within this Agreement, portable devices include, but are not limited to handhelds/PDAs, Ultramobile PCs, flash memory devices (e.g. USB flash drives, personal media players), portable hard disks, and laptop/notebook computers. Portable media includes, but is not limited to optical media (e.g., CD's, DVD's, Blu-Rays), magnetic media (e.g., floppy disks, Zip or Jaz disks or drives,) or flash media (e.g., Compact Flash, SD Card, MMC).

   Requestor is authorized to store WADOC Data on portable devices or media so long as the data shall be given the following protections:

   i. Encrypt the data with a FIPS approved cryptographic algorithm.

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

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

iv. Physically protect the portable device(s) and/or media by keeping them in locked storage when unused; using check-in/check-out procedures when device or other media is being shared; taking frequent inventories of media, and access to media by users.

v. When being transported outside of a secure area, portable devices and media with confidential WADOC Data must be under the physical control of Requestor's staff with authorization to access the data.

2. **SAFEGUARDS AGAINST UNAUTHORIZED USE AND RE-DISCLOSURE OF DATA:** Requestor shall exercise due care to protect all data from unauthorized physical and electronic access. Both Parties shall establish and implement the following minimum physical, electronic and managerial safeguards for maintaining the confidentiality of information provided by either Party pursuant to this Agreement:

i. Access to information provided by WADOC will be restricted to only those authorized staff, officials, and agents of the Parties who need it to perform their official duties in the performance of the work requiring access to the information as detailed in this Agreement and/or contract which this Agreement concerns.

ii. Requestor will store the information in an area that is safe from access by unauthorized persons during work hours as well as non-work hours, or when otherwise not in use.

iii. Requestor will design, implement and maintain an information security program designed to meet at least an industry standard ability to protect the information in a manner that prevents unauthorized persons from retrieving the information by means of computer, remote terminal or other means.

iv. Requestor shall take precautions to ensure that only authorized personnel and agents are given access to on-line files containing confidential or sensitive data.

v. Requestor shall take due care and take reasonable precautions to protect WADOC Data from unauthorized physical and electronic access. Both Parties will strive to meet or exceed the requirements of the State of Washington's policies and standards for data security and access controls to ensure the confidentiality, availability, and integrity of all data accessed.

III. DATA SEGREGATION

1. When it is not feasible or practical to segregate WADOC Data from non-WADOC Data, then both the WADOC Data and the non-WADOC Data with which it is commingled must be protected as described in this Agreement.

2. If Requestor or its agents detect a compromise or potential compromise of the security such that this data may have been accessed or disclosed without proper authorization, Requestor shall give notice to WADOC within one (1) business day of discovering the compromise or potential compromise. Requestor shall take corrective action as soon as

practicable to eliminate the cause of the breach and shall be responsible for ensuring that appropriate notice is made to those individuals whose data may have been improperly accessed or disclosed.

IV. DATA CONFIDENTIALITY

1. Requestor acknowledges the personal or confidential nature of the information and agrees that their staff and contractor staff with access shall comply with all laws, regulations, and policies that apply to protection of the confidentiality of the data. Requestor is responsible for informing all these entities that they must abide by the data security provisions within this Agreement and within any amendments, attachments, or exhibits within this Agreement. Requestor acknowledges that the failure to meet the requirements of the preceding sentence may result in the Requestor not protecting the data as articulated within this Agreement, which is grounds for termination of this Agreement.

   a. **Non-Disclosure of Data**

      i. Individuals will access data gained by reason of this Agreement only for the purpose of this Agreement.

      ii. Access is limited to the OCO staff who require it as a function of their position and have read and signed Attachment B, Statement of Confidentiality and Non-Disclosure.

      iii. The OCO shall immediately terminate OCO staff access to OMNI, On-Base, iDOC, and any other confidential WADOC data when the staff persons' job function changes and access is no longer needed.

      iv. OCO staff with access to OMNI, On-Base, or any other confidential Department data, must read and sign Attachment B as required in IV(1.) (a)(ii), or failure to do so shall be grounds for termination of the DSA.

      v. Data to a user to whom WADOC has not received a signed Statement of Confidentiality and Non-Disclosure may, at WADOC's discretion, be cause for terminating the Agreement**.**

      vi. WADOC may, at its reasonable discretion, disqualify at any time any person authorized to access confidential information by or pursuant to this Agreement. Notice of disqualification shall be in writing and shall terminate a disqualified person's access to any information provided by WADOC pursuant to this Agreement immediately upon delivery of notice to Requestor. Disqualification of one or more persons by WADOC does not affect other persons authorized by or pursuant to this Agreement.

V. USE OF DATA

1. Requestor agrees to dispose of the data pursuant to Section VI "DISPOSITION OF DATA" after the work that required the data has been completed or upon the expiration of the one (1) year period from the date obtained, whichever occurs first, or as otherwise required by law.[1]

2. This Agreement does not constitute a release of the data for Requestor's discretionary use, but may be accessed only to carry out the responsibilities specified herein. Any ad hoc analyses or other use of the data not specified in this Agreement is not permitted without the prior written agreement of WADOC. Requestor shall not disclose, transfer, or sell any such information, except as provided by law or this Agreement. Requestor shall maintain the confidentiality of all data and other information gained by reason of this Agreement.

3. Requestor is not authorized to update or change any WADOC Data, and any updates or changes shall be cause for immediate termination of this Agreement.

4. Neither Washington State nor WADOC guarantees the accuracy of the data provided. All risk and liabilities of use and misuse by Requestor employees or agents of information provided pursuant to this Agreement are understood and assumed by Requestor.

5. WADOC Data cannot be re-disclosed or duplicated unless specifically authorized in this Agreement, or by law.[2]

6. When required, the OCO shall contact the Washington State Institutional Review Board (WSIRB) for research or data analysis approval.

7. The requirements in this section shall survive the termination or expiration of this Agreement or any subsequent agreement intended to supersede this DSA.

VI. DISPOSITION OF DATA

1. Unless otherwise required, Requestor shall dispose of the data received from WADOC immediately upon expiration or termination of the Agreement or as provided by law.

2. Acceptable destruction methods for various types of media include:

    a. For paper documents containing confidential or sensitive information, a contract with a recycling firm to recycle confidential documents is acceptable, provided the contract ensures that the confidentiality of the data will be protected. Such documents may also be destroyed by on-site shredding, pulping, or incineration.

[1] OCO is subject to RCW 40.14, regarding the Preservation and Destruction of Public Records, and relevant records retention schedules.
[2] OCO is subject to RCW 43.06C.060, regarding the disclosure of information and records.

b. For paper documents containing confidential information requiring special handling, recycling is not an option. These documents must be destroyed by on-site shredding, pulping, or incineration.

c. If confidential or sensitive information has been contained on optical discs (e.g. CDs, DVDs, Blu-ray), the data recipient shall either destroy by incinerating the disc(s), shredding the discs, or completely defacing the readable surface with a coarse abrasive.

d. If confidential or sensitive information has been stored on magnetic tape(s), the data recipient shall destroy the data by degaussing, incinerating or crosscut shredding.

e. If data has been stored on server or workstation data hard drives or similar media, the data recipient shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying disk(s).

f. If data has been stored on portable media (e.g. floppies, USB flash drives, portable hard disks, or similar disks), the data recipient shall destroy the data by using a "wipe" utility which will overwrite the data at least three (3) times using either random or single character data, degaussing sufficiently to ensure that the data cannot be reconstructed, or physically destroying the media.

VII. ON-SITE OVERSIGHT

Requestor agrees that WADOC shall have the right at any time during the term of the Agreement, during normal business hours and upon reasonable written notice, to monitor and review OCO data access to ensure that the data is being protected as required under the DSA.

VIII. WAIVER

A failure by either Party to exercise its rights under this Agreement shall not preclude that Party from subsequent exercise of such rights and shall not constitute a waiver of any other rights under this Agreement unless stated to be such in a writing signed by an authorized representative of the Party and attached to the original Agreement.

IX. DISPUTES

In the event that a dispute arises under this Agreement, it shall be determined by a Dispute Board in the following manner: Each Party to this Agreement shall appoint one member to the Dispute Board. The members so appointed shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall review the facts, agreement terms, and applicable statutes and rules and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the Parties hereto. As an alternative to this process, either of the Parties may

request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

X. AMENDMENTS AND ALTERATIONS TO THIS AGREEMENT

With mutual consent, WADOC and Requestor may amend this Agreement at any time, provided that the amendment is in writing and signed by authorized staff of each of the Parties.

XI. SEVERABILITY

If any provision of this Agreement or any provision of any document incorporated by reference shall be held invalid, such invalidity shall not affect the other provisions of this Agreement which can be given effect without the invalid provision, if such remainder conforms to the requirements of applicable law and the fundamental purpose of this Agreement, and to this end, the provisions of this Agreement are declared to be severable.

XII. INDEPENDENT CAPACITY

The employees or agents of each Party who are engaged in the performance of this Agreement shall continue to be employees or agents of that Party and shall not be considered for any purpose to be employees or agents of the other Party.

XIII. ASSIGNMENT

The work to be provided under this Agreement, and any claim arising thereunder, is not assignable or delegable by either Party in whole or in part, without the express prior written consent of the other Party, which consent shall not be unreasonably withheld.

XIV. GOVERNANCE

This Agreement is entered into pursuant to and under the authority granted by the laws of the state of Washington and any applicable federal laws. The provisions of this Agreement shall be construed to conform to those laws.

In the event of an inconsistency in the terms of this Agreement, or between its terms and any applicable statute or rule, the inconsistency shall be resolved by giving precedence in the following order:

a. Applicable state and federal statutes and rules;
b. Purpose, Section I(1) of this DSA; and
c. Any other provisions of the Agreement, including materials incorporated by reference.

XV. SIGNATURES

THIS DATA SHARE AGREEMENT, consisting of nine (9) pages and four (4) attachments, is executed by the persons signing below who warrant that they have the authority to execute the Agreement.

OFFICE OF THE CORRECTIONS OMBUDS	**DEPARTMENT OF CORRECTIONS**
_____	_____
(Signature)	(Signature)
_____	Debra J. Eisen
(Printed Name)	(Printed Name)
_____	Contracts Administrator
(Title)	(Title)
_____	_____
(Date)	(Date)

Approved as to Form: This Contract format was approved by the Office of the Attorney General.
Approval on file.

ATTACHMENT B

STATEMENT OF CONFIDENTIALITY AND NON-DISCLOSURE BETWEEN WASHINGTON DEPARTMENT OF CORRECTIONS AND OFFICE OF THE CORRECTIONS OMBUDS

Before you are allowed to access the data, you are required to sign the following statement: As an employee or agent of Requestor, I have access to information provided by the State of Washington, Department of Corrections (WADOC). This information is confidential, and I understand that I am responsible for maintaining this confidentiality. I understand that the information may be used solely for the purposes of work under the above referenced Agreement.

- I have been informed and understand that all information related to this DSA (Data Share Agreement) is confidential and may not be disclosed to unauthorized persons. I agree not to divulge, transfer, sell, or otherwise make known to unauthorized persons any information contained in this system.

- I also understand that I am not to access or use this information for my own personal information, but only to the extent necessary and for the purpose of performing my assigned duties as an employee of *Requestor* under this Agreement.

- I agree to abide by all federal and state laws and regulations regarding confidentiality and disclosure of the information related to this DSA.

	Employee **I have read and understand the above Notice of Nondisclosure of information.**	**Supervisor** **The employee has been informed of their obligations including any limitations, use or publishing of confidential data.**
Signature		
Printed Name		
Organization		
Job Title		
Email Address		
Date		

State of Washington
Department of Corrections

DOC K11966
OCO K197
Amendment No. 1

This Amendment is made by the Washington State Department of Corrections, hereinafter referred to as "Department" or "WADOC" and the Office of the Corrections Ombuds, hereinafter referred to as "OCO," for the purpose of amending the above-referenced Contract, heretofore entered into between the Department and Contractor. The Department and the OCO may be referred to individually as a "Party" or collectively the "Parties" to this Amendment.

WHEREAS the purpose of this Amendment is to provide additional details as to the OCO's use and disclosure of sensitive Department information.

NOW THEREFORE, in consideration of the terms and conditions contained herein, or attached and incorporated and made a part hereof, the Department and OCO agree as follows:

Section V, Use of Data, is amended with the following:

8. The OCO agrees that the following WADOC records contain uniquely sensitive information and shall be subject to special use and disclosure restrictions:

   a. Mortality Review Committee Reports and other records created for and maintained as part of the Department's Coordinated Quality Improvement Program (CQIP). Records created and maintained for CQIP are subject to strict disclosure limitations set forth in RCW 43.70.510.

   b. Records disclosing the identity of confidential informants (CIs). These records could endanger informants and undermine effective law enforcement and are protected under RCW 42.56.240(1)-(2).

   c. Fixed camera surveillance video. Nondisclosure of video surveillance recordings is essential to effective law enforcement and the Department is therefore authorized to withhold such video from disclosure. *See Fischer v. Washington State Department of Corrections*, 160 Wn. App. 722 (2011).

   d. Audio recordings of telephone calls made through the call system mandated by RCW 9.73.095(2). State law limits access to phone recordings to the superintendent or designee and allows further disclosure only to safeguard the orderly operation of the facility, in response to a court order, or in the prosecution or investigation of any crime. See RCW 9.73.095(3). The Department therefore strictly limits access to these recordings.

   Accordingly, with respect to these records, the Parties agree:

   a. The Department will conspicuously label all CQIP, CI, surveillance video, and call recording files "Confidential – Not Subject to Further Disclosure" when producing such records to the OCO.

   b. The OCO shall strictly limit disclosure of these records, and the protected information in them, to paid OCO employees who have a need to access the information for OCO investigation purposes, except as provided by law.

   c. The OCO shall store the information at least as securely as OCO's own records to avoid unauthorized disclosure and prevent access by persons other than paid OCO employees, and the OCO shall promptly report to the Department any unauthorized disclosures.

d. The OCO shall maintain the records as required by chapter 40.14 RCW and other applicable law.

Additions to this text are shown by underline and deletions by ((~~strikeout~~)). All other terms and conditions remain in full force and effect. The effective date of this Amendment is **January 1, 2020.**

THIS AMENDMENT, consisting of two (2) pages is executed by the persons signing below who warrant that they have the authority to execute the Amendment.

OFFICE OF CORRECTIONS OMBUDS	**DEPARTMENT OF CORRECTIONS**
	
(Signature)	(Signature)
	Debra J. Eisen
(Printed Name)	(Printed Name)
	Contracts Administrator
(Title)	(Title)
	April 2, 2020
(Date)	(Date)

Approved as to Form: This Amendment format was approved by the office of the Attorney General.
Approval on file.