



SHARED SERVICES
Information Security and Privacy Office
500 Summer Street NE, E-24
Salem, Oregon 97301-1097
Voice: (503) 945-6812



OHA Agreement Number 182234

State of Oregon
Security and Access Agreement

In compliance with the Americans with Disabilities Act, this document is available in alternate formats such as Braille, large print, audio recordings, Web-based communications and other electronic formats. To request an alternate format, please send an e-mail to dhs-oha.publicationrequest@state.or.us or call 503-378-3486 (voice) or 503-378-3523 (TTY) to arrange for the alternative format.

This Security and Access Agreement (Agreement) is between the State of Oregon, acting by and through the Oregon Health Authority (OHA) ("Agency") and Yamhill County Health & Human Services (Private Entity) hereinafter referred to as "PE."

Access to be granted under this Agreement relates to OHA's Health Policy and Analytics Division.

1. PURPOSE.

- 1.1. This Agreement defines the roles and responsibilities of Agency and PE when State of Oregon Data, networks, and systems are accessed by PE, and identifies the Data, Access, and Information Assets.
- 1.2. The terms and conditions of this Agreement govern PE's:
 - 1.2.1. Use of Data.
 - 1.2.2. Access to State of Oregon Information Assets and Systems.
- 1.3. PE needs the Access described in Exhibit A, Third Party Information System Access Request (MSC 0785), which is hereby incorporated into this Agreement by reference.

2. AUTHORITY.

- 2.1. Agency has authority to share access under Federal Certified Community Behavioral Health Clinic (CCBHC) Certification Criteria.
- 2.2. PE has authority to receive access under Federal Certified Community Behavioral Health Clinic (CCBHC) Certification Criteria.

Board Order No. 24-57

3. **TERM.** This Agreement is effective upon execution and (subject to periodic review by Agency) is effective unless terminated by either party in accordance with Section 11, Suspension or Termination.
4. **DEFINITIONS.** The following definitions apply to this Agreement.
 - 4.1. "Access" means the ability or the means necessary to read, communicate, or otherwise use State of Oregon Data, Network and Information Systems, and Information Assets.
 - 4.2. "Breach" means the acquisition, access, exposure, use, disclosure, of an Information Asset (such as Data) in a manner not in compliance with applicable law, rule, or policy, or data loss, misuse, or compromise.
 - 4.3. "Client Records" includes any client, applicant, or participant information regardless of the media or source, exchanged between the parties. Client Records may be for clients of Agency, PE, both, or another entity.
 - 4.4. "Data" means information created, transmitted, and stored pursuant to this Agreement, including metadata, personal information, and Client Records.
 - 4.5. "Incident" means the attempted or successful unexpected or unwanted unauthorized access, use, disclosure, modification, or destruction of any Network and Information System or Information Asset. An Incident is an observable, measurable occurrence that is a deviation from expected operations or activities. An incident may be a Breach, failure to protect a User's identification (ID), or theft of computer equipment that uses or stores any de-identified Data.
 - 4.6. "Individual Access Request (IAR)" refers to the Agency's form used to authorize a User, identify the User's job assignment, and the required access to Network and Information System(s). It generates a unique alpha/numeric code used to access the Agency's Network and Information Systems.
 - 4.7. "Information Asset(s)" refers to all information provided through the Agency, regardless of the source, which requires measures for security and privacy. Includes Data.
 - 4.8. "Network and Information System(s)" or "Systems" means the State of Oregon's computer infrastructure which provides personal communications, Data, and Information Assets, regional, wide area, and local networks, and the internetworking of various types of networks.
 - 4.9. "User" means any individual (authorized or unauthorized) who Accesses the Network and Information Systems or Information Assets through PE's Access under this Agreement. Authorized Users each have an assigned unique log-on identifier.
5. **AMENDMENTS.** Other than as allowed under this section, the parties may amend this Agreement only via a written amendment executed by both parties that clearly recites

the parties' understanding and intent to amend the Agreement, and clearly and with specificity describes the terms to be amended or supplemented.

- 5.1. **Point of Contact Changes.** Each party will provide timely notification to the other of any change of its respective point(s) of contact, including any technical lead, and will name an interim or replacement person in any such notice. This Agreement will be deemed amended to include the updated information.
- 5.2. **Administrative Changes.** Either party may request updates to Exhibit A that are, in the sole discretion of Agency's Information Security and Privacy Office, administrative in nature and do not modify the mode of Access or type of Data by submitting a written request to the other party. Upon written authorization of both parties and subsequent written approval by Agency's Information Security and Privacy Office, Exhibit A will be deemed amended to include the updated information.

6. NOTIFICATIONS.

- 6.1. **Points of Contact.** The parties have designated their respective points of contact in Section 27, Signatures. The parties will facilitate direct communication between their points of contact. The parties will provide timely written notification to the other of any changes in point of contact information.
- 6.2. **Incident and Breach Notifications.** In the event PE or its subcontractors or agents discover or are notified of an Incident or a Breach, including a failure to comply with PE's confidentiality obligations, PE shall notify the Agency's point of contact, identified in Section 27, Signatures, of the Incident or Breach immediately, and in no event more than 24 hours following discovery or notification. If the State of Oregon determines that the Incident or Breach requires notification of Agency's clients, or other notification required by law, the State of Oregon will have sole control over the notification content, timing, and method, subject to PE's obligations under applicable law. Notwithstanding the foregoing, the parties acknowledge and agree that this section constitutes notice by PE to Agency of the ongoing existence and occurrence of security incidents that are "unsuccessful," such as "pings" on a firewall, and do not represent Incidents or Breaches.
- 6.3. **Requests for Data.** In the event PE receives a third-party request for Data, including any electronic discovery, litigation hold, or discovery searches, PE shall first give Agency notice and provide such information as may be reasonably necessary to enable the State of Oregon to protect its interests.
- 6.4. **Changes in Law.** Each party shall provide notice to the other of any change in law, or any other legal development, which may significantly affect its ability to perform its obligations under this Agreement.
- 6.5. **Notices.** Except as otherwise expressly provided in this Agreement, any communications between the parties or notices to be given under this Agreement must be given in writing to PE's point of contact, and in writing to Agency's point

of contact, or to such other addresses or numbers as either party may hereafter indicate pursuant to this Agreement.

- 6.5.1. Any communication or notice delivered by United States Postal Service, first class mail postage prepaid, will be deemed given five (5) calendar days after mailing.
- 6.5.2. Any communication or notice delivered by email will be deemed given when the recipient responds with a receipt, which may be auto-generated. To be effective against Agency, such email transmission must be confirmed by telephone notice to the Agency's point of contact (or delegate).
- 6.5.3. Any communication or notice by personal delivery will be deemed given when actually received by the appropriate point of contact (or delegate).

7. GRANT OF LICENSE.

- 7.1. **State Systems and Data.** Subject to PE's compliance with this Agreement, PE and its authorized Users are hereby granted a non-exclusive, non-transferable, and revocable authorization to access and use Network and Information Systems and Information Assets only in accordance with this Agreement and applicable laws, rules, and policies. PE and its Users shall not participate in any unauthorized transfer or sale of, create derivative works of, or in any way exploit the Data made available through this Agreement.
- 7.2. **Third Party Systems.** PE is responsible for the compliance of its employees, agents, and subcontractors with any third party licenses to which Access is subject.

8. DATA PRIVACY.

- 8.1. **Generally.** PE shall hold all Client Records and other information as to personal facts and circumstances obtained by PE on Agency's clients as confidential, in accordance with the standard of care applicable to the Client Records and shall not divulge any Client Records without the written consent of the client, the client's attorney, the responsible parent of a minor child, or the minor child's guardian except as required by this Agreement or applicable law.
- 8.2. **Accuracy of Data.** Data Accessed under this Agreement is from multiple sources and subject to change arising from numerous factors. Without limiting any other provision of this Agreement, neither party nor its vendors are responsible or liable under this Agreement for any claim related to the accuracy, content, currency, completeness, or delivery of any Data either provided or used by the parties.
- 8.3. **Limited Purposes.** PE shall limit the use or disclosure of Data concerning clients to persons directly connected with the Services and administration of this Agreement.

- 8.4. **Privacy Protections.** Data may include information, such as Client Records, subject to specific confidentiality protections under state or federal law. PE shall comply with laws and regulations applicable to the information to which PE has Access, including as specified in this Agreement.
- 8.5. **Training.** PE's employees, subcontractors, and agents who will be granted Access have received training on the privacy and security obligations relating to the Access, including on Client Records. PE shall provide periodic privacy and security training to its employees, subcontractors, and agents. This periodic training may include State of Oregon trainings available to third parties on security and use and disclosure of Data.

9. SECURITY REQUIREMENTS.

- 9.1. **Compliance with Laws, Regulations, and Policies.** PE and its employees, contractors, and agents shall comply with all applicable state and federal laws and regulations, and State of Oregon policies governing use and disclosure of Data (including Client Records) and Access, including as those laws, regulations, and policies may be updated from time to time. Applicable laws, regulations, and policies include but are not limited to:

- 9.1.1. Oregon's Statewide Information Security Standards
<https://www.oregon.gov/eis/cyber-security-services/Documents/2019StatewideInformationAndCyberSecurityStandardsV1.0.pdf>
- 9.1.2. Oregon's Statewide Information Security Plan,
<https://www.oregon.gov/eis/cyber-security-services/Documents/StatewideInformationSecurityPlan.pdf>
- 9.1.3. Oregon's Statewide Policies:
<https://www.oregon.gov/das/Pages/policies.aspx#IT>.
- 9.1.4. ODHS and OHA Privacy and Confidentiality administrative rules, OAR Chapter 407, Division 14, and OAR Chapter 943, Division 14.
- 9.1.5. The Oregon Consumer Information Protection Act, ORS 646A.600 through 646A.628, to the extent applicable.
- 9.1.6. The Health Insurance Portability and Accountability Act (HIPAA), including as amended by the Health Information Technology for Economic and Clinical Health ("HITECH") Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009, Public Law 111-5 ("ARRA"), and its implementing Privacy Rule and Security Rule, 45 CFR Parts 160 and 164[, to the extent PE receives Protected Health Information (as defined in HIPAA) in connection with this Agreement.

- 9.2. **Responsible for Compliance.** PE is responsible for the compliance of its employees, agents, and contractors with this Agreement and with any third-party licenses to which Access is subject.
- 9.3. **Subcontractors.** PE shall disclose its subcontractors acquiring Access to Data under this Agreement to the Agency's point of contact.
- 9.4. **Privacy and Security Measures.** PE represents and warrants it has established and will maintain privacy and security measures that meet or exceed the standards set in laws, rules, and regulations applicable to the safeguarding, security and privacy of all Information Assets, including Client Records, regardless of the media, and all Network and Information Systems. PE shall monitor, periodically assess, and update its security controls and risk to ensure continued effectiveness of those controls.
- 9.5. **Security Risk Management Plan.** PE shall ensure the level of security and privacy protection required in accordance with this Agreement is documented in a security risk management plan. PE shall make its security risk management plan available to the State of Oregon for review upon request.
- 9.6. **Audit Rights and Access.** PE shall maintain records in such a manner as to clearly document its compliance with and performance under this Agreement, and provide Agency, the Oregon Secretary of State, the federal government, and their duly authorized representatives, access to PE's officers, agents, contractors, subcontractors, employees, facilities and records for them to:
 - 9.6.1. Determine PE's compliance with this Agreement,
 - 9.6.2. Validate PE's written security risk management plan, or
 - 9.6.3. Gather or verify any additional information Agency may require to meet any state or federal laws, rules, or orders regarding Data.
 - 9.6.4. Access to facilities, systems, and records under this section will be granted following reasonable notice to PE. Records include paper or electronic form, system security logs, and related system components and tools (including hardware and software), required to perform examinations and audits, and to make excerpts and transcripts, including for data forensics.

10. ACCESS TO AGENCY SYSTEMS.

- 10.1. **Review of User Requests.** If required for Access, Agency will review requests, including forms such as the IAR, and will:
 - 10.1.1. Notify PE of the approval or denial of its request for each User for whom Access has been requested;
 - 10.1.2. Provide any unique log-on identifier required for authorized individual Access;

- 10.1.3. Provide updates to approved inquiry processes and instructions to PE.
- 10.2. **PE's Responsibilities for User Accounts.** PE agrees to facilitate the completion any forms, such as the IAR, for each person for whom Access is requested.
 - 10.2.1. PE is responsible for all activities that occur through its Access, including for any acts related to a lost or stolen User ID or password.
 - 10.2.2. Except as otherwise specified or approved by Agency, neither PE nor its Users shall modify, alter, delete, or destroy any Information Asset.
 - 10.2.3. PE shall immediately notify Agency when a User, group of Users, or PE, no longer requires Access whether due to changes in duties or due to changes in PE's programs related to this Agreement.
 - 10.2.4. PE is responsible for ensuring account information for its Users is accurate, complete, and up to date.
- 10.3. **Security.** PE shall maintain security of equipment and hardware, and ensure the proper handling, storage and disposal of all State of Oregon or Agency Information Assets accessed, obtained, or reproduced by PE and its Users to prevent inadvertent destruction or loss.
- 10.4. **Prevention of Unauthorized Access.** PE shall not allow any Access to State of Oregon Network and Information Systems or Information Assets by its Users that is not authorized in accordance with this Agreement and applicable law, and shall implement and maintain safeguards to prevent unauthorized Access.
- 10.5. **Access from Outside the US and its Territories.** PE Access to the state network from outside the US and its territories is prohibited unless approved through the Geofencing Exception Request Process, ODHS|OHA 090-009-05.
 - 10.5.1. PE shall not allow use of any Information Asset in any country or in any manner prohibited by governing applicable law, rule, or policy.
- 10.6. **Authorized Access and Use Only.** No User may Access or use State of Oregon Network and Information Systems or Information Assets for any purpose other than those specifically authorized under this Agreement.
 - 10.6.1. Users shall not use Access to obtain or attempt to obtain Access or any Data not authorized or intentionally made available.
 - 10.6.2. The use and disclosure of any Data is strictly limited to the minimum information necessary for the purpose stated in Section 1 of this Agreement.
- 10.7. **Revocation or Termination of Access.** Breach, or wrongful use or disclosure of Data by PE or its Users, may cause the immediate revocation of the Access granted through this Agreement, in the sole discretion of Agency, or Agency may

specify a reasonable opportunity for PE to cure the unauthorized use or disclosure and end the violation, and terminate the Access if PE does not do so within the time specified by Agency. Legal actions also may be taken for violations of applicable regulations and laws.

- 10.8. **No Unauthorized Distribution.** PE shall not sell, make available, or provide Information Assets in any form to any other persons or organizations, and shall not use the Data for any purposes other than as allowed under this Agreement and applicable law.
- 10.9. **No Impairment.** PE shall not allow use of this Access in any manner which could damage, disable, overburden, or impair Network and Information Systems, or interfere with any other entity's use or benefit of Network and Information Systems.
- 10.10. **Prohibition on Data Mining.** PE shall not use any data-mining technology on Network and Information Systems for any non-authorized activity. For purposes of this requirement, "non-authorized activity" means the data mining or processing of data on Network and Information Systems, stored or transmitted for unrelated commercial purposes, advertising or advertising-related purposes, or for any other purpose other than security analysis that is not explicitly authorized in this Agreement.
- 10.11. **Incidents and Breaches.** PE shall comply, and shall cause its subcontractors to comply, with any requirements for identifying and addressing an Incident or Breach. This requirement applies regardless of whether the Incident or Breach was accidental or otherwise.

11. SUSPENSION OR TERMINATION.

- 11.1. This Agreement may be terminated at any time by written agreement of the parties.
- 11.2. This Agreement may be terminated by either party upon 30 calendar days' written notice to the other party.
- 11.3. Access and this Agreement may be terminated immediately upon written notice from PE if the Access is no longer needed by PE.
- 11.4. Access and this Agreement terminates immediately upon PE no longer being under contract.
- 11.5. Agency may immediately revoke the Access granted PE for PE's failure to comply with the requirements of this Agreement, via written notice to PE's point of contact. Agency may, to the extent it determines it is reasonable and able to do so, provide advance written notice to PE to cure any deficiency or breach under this Agreement.
- 11.6. Either party may terminate this Agreement, and Agency may modify Access, upon written notice if there are changes to or revised interpretations of federal or state

laws, rules, or regulations, or if either party has changes in policies that require such change.

12. RETURN OF INFORMATION ASSETS. Upon expiration or termination of this Agreement for any reason whatsoever, PE shall comply with its obligations under applicable law and this Agreement for the return of Agency's property, including:

12.1. Disposal. PE shall ensure the proper handling, storage and disposal of all State of Oregon or Agency's Information Assets accessed, obtained, or reproduced by PE and its Users to prevent inadvertent destruction or loss. PE shall ensure proper disposal of equipment and Information Assets when authorized use ends, consistent with PE's record retention obligations and obligations regarding Data under applicable law and this Agreement.

12.2. Sanitization. Except as necessary to meet its records maintenance and audit obligations under this Agreement, PE shall not retain any copies of State of Oregon or Agency's Data. PE shall notify Agency of any conditions that make returning all such Data not feasible. Upon Agency's written acknowledgement that returning all Data is not feasible, PE shall purge or destroy retained State of Oregon and Agency Data in all its forms in accordance with the most current version of NIST SP 800-88 (or other agreed-upon standard) and on request provide Agency with written certification of sanitization.

12.3. Protections. PE shall maintain protections required by law and this Agreement for any retained State of Oregon or Agency's Data for so long as PE (including through any subcontractor) retains it.

13. COSTS. Each party will bear its own costs related to the acquisition of all equipment, software, data lines or connections necessary for Access, unless otherwise agreed to by written agreement between the parties. Each party is responsible for securing compatible hardware, equipment, and software, and network connections.

14. DOCUMENTS; COMPLETE AGREEMENT. This Agreement consists of these terms and conditions and Exhibit A, in the form attached. This Agreement merges all prior and contemporaneous communications with respect to the matters described in this Agreement. Any ambiguity will be resolved to permit Agency to comply with applicable privacy and security laws and the State of Oregon's rules and policies interpreting those laws. In the event of any conflict between the requirements of applicable law, the terms and conditions of this Agreement and Exhibit A, the conflict will be resolved in that order.

15. WAIVER. No provision of this Agreement may be waived except by an agreement in writing signed by the waiving party. A waiver of any term or provision will not operate as a waiver of any other term or provision.

16. NO THIRD-PARTY BENEFICIARIES. Agency and PE are the only parties to this Agreement and are the only parties entitled to enforce its terms.

17. INDEMNIFICATION. INDEMNIFICATION. PE will indemnify, defend and hold harmless Agency, and Agency's directors, officers, agents and employees ("Indemnities'") from and against any claim, cause of action, liability, damage, cost or expense (including, without limitation, reasonable attorney's fees and court costs) arising out of or in connection with any unauthorized or prohibited use or disclosure including any Security Incident or Breach or any other violation of this Agreement by PE or any employee, subcontractor, or agent of PE.

18. ATTORNEYS' FEES. Neither party to this Agreement is entitled to obtain judgment from the other party for attorneys' fees incurred in any litigation between the parties. Except as specifically described for PE's indemnification obligations, neither party may obtain judgment from the other party for attorneys' fees incurred in the defense of any claim asserted by a third party.

19. REMEDIES.

19.1. In the event PE is in breach of this Agreement, Agency may, at its option, pursue any or all of the remedies available to it under this Agreement and at law or in equity, including, but not limited to suspension or termination of this Agreement. Agency's remedies are cumulative to the extent the remedies are not inconsistent, and Agency may pursue any remedy or remedies singly, collectively, successively or in any order whatsoever.

19.2. In the event Agency is in breach of this Agreement, PE's sole remedy will be to terminate this Agreement. In no event will Agency be liable to PE for any expenses related to suspension or termination of this Agreement or for lost revenues.

20. LIMITATION ON STATE OF OREGON LIABILITY. THE STATE IS NOT LIABLE UNDER THIS AGREEMENT FOR ANY CLAIM RELATING TO THE ACCESS, THE INFORMATION ASSETS, RELATED DOCUMENTATION, OR ANY LICENSE GRANTED TO SUPPORT PE'S ACCESS, UNDER ANY BREACH OF WARRANTY, CONTRACT, NEGLIGENCE, STRICT LIABILITY, OR ANY OTHER LEGAL OR EQUITABLE THEORY.

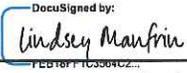
21. GOVERNING LAW; JURISDICTION; VENUE. This Agreement is governed by and construed in accordance with the laws of the state of Oregon without regard to conflicts of laws. The sole and exclusive jurisdiction and venue for actions related to the subject matter of this Agreement is the Circuit Court of the State of Oregon for Marion County. In the event a claim must be brought in federal court, the jurisdiction and venue for such action is the United States District Court for the District of Oregon. PE HEREBY CONSENTS TO THE PERSONAL JURISDICTION OF THESE COURTS, WAIVES ANY OBJECTION TO VENUE IN THESE COURTS, AND WAIVES ANY CLAIM THAT THESE COURTS ARE INCONVENIENT FORUMS. In no way may this section or any other term of this Agreement be construed as (i) a waiver by the State of Oregon of any form of defense or immunity, whether it is sovereign immunity, governmental immunity, immunity based on the Eleventh Amendment to the Constitution of the United States, or otherwise, or (ii) consent by the State of Oregon to the jurisdiction of any court.

- 22. COUNTERPARTS.** This Agreement may be executed in several counterparts, all of which when taken together constitute one agreement, notwithstanding that all parties are not signatories to the same counterpart. Each copy of the Agreement so executed constitutes an original.
- 23. BINDING EFFECT.** The persons signing below have the right and authority to execute this Agreement and no further approvals are necessary to create a binding agreement.
- 24. SEVERABILITY.** The parties agree that if any term or provision of this Agreement is declared by a court of competent jurisdiction to be illegal or in conflict with any law, the validity of the remaining terms and provisions will not be affected, and the rights and obligations of the parties will be construed and enforced as if the Agreement did not contain the particular term or provision held to be invalid.
- 25. FORCE MAJEURE.** A party will not be liable for nonperformance or delay in performance (other than of obligations regarding confidentiality) caused by any event beyond the reasonable control of such party, including but not limited to wars, hostilities, revolutions, riots, civil commotion, national emergency, strikes, lockouts, unavailability of supplies, epidemics, fire, flood, earthquake, force of nature, explosion, embargo, or any other Act of God, Internet, electric power or communications outage, or any law, proclamation, regulation, or ordinance of any court, government, or governmental agency.
- 26. SURVIVAL.** The provisions of this Agreement which by their nature survive termination do so survive. This Agreement applies to any Access by PE by its employees, agents, providers, and subcontractors following its termination.

27. SIGNATURES

The authorized representative of each party hereby acknowledges that he/she has read this Agreement, understands it, and agrees to be bound by its terms and conditions.

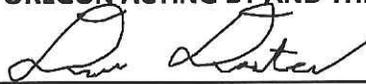
YAMHILL COUNTY HEALTH & HUMAN SERVICES:

By:  _____
Print Name: Lindsey Manfrin
Title: HHS Director Date: 2/26/2024

Point of Contact:

Printed Name and Title: Lindsey Manfrin
Organization Name: HHS Director
Mailing Address: 627 NE Evans Street, McMinnville, OR 97128
Physical Address: 627 NE Evans Street, McMinnville, OR 97128
Telephone: (503) 474-4917
Email: manfrinl@co.yamhill.or.us

STATE OF OREGON ACTING BY AND THROUGH ITS OREGON HEALTH AUTHORITY (OHA):

By:  _____
Print Name: Drew Docter
Title: Research Analyst Date: 2/26/2024

Point of Contact:

Printed Name and Title: Drew Docter
Organization Name: Behavioral Health Medicaid Research Analyst
Mailing Address: 500 Summer Street NE, Salem, OR 97301
Physical Address: 500 Summer Street NE, Salem, OR 97301
Telephone: (971) 393-3863
Email: drew.d.docter@oha.oregon.gov

REVIEWED BY OHA INFORMATION SECURITY AND PRIVACY OFFICE:

Printed Name and Title: Shannon Corr, Information Exchange Coordinator

Approved by the BOC on: 2/22/24

via Board Order No.: 24-57

EXHIBIT A

Third Party Information System Access Request (MSC 0785)

Upon execution, the finalized 785 will be inserted here.

Third Party Information System Access Request

An DHS or OHA program completes this form to request access for a **third-party entity*** (*organization or individual*) to data within an DHS or OHA information system or network.

**Please note that each entity only needs one form.*

 Hover over **blue** text for more information.

Request type (<i>required</i>): New request (ISPO will add agreement number)	Agreement number: 182234
---	-----------------------------

Section 1. Third party information

This section defines the third party needing access to DHS/OHA network and information system(s). A third party is any individual or entity that is not part of the DHS/OHA workforce. Workforce means employees, volunteers, trainees and other individuals whose DHS or OHA work is under that agency's direct control. This applies to paid and unpaid workforce members.

Third-party agreement administrator contact information

This individual signs the contracts for the third party. (This is NOT a DHS/OHA employee.)

Organization/entity name: Yamhill County Health & Human Services	
Contact name (<i>first, last</i>):	Lindsey Manfrin
Position/title:	HHS Director
Work street address:	627 NE Evans Street
City, State, ZIP:	McMinnville, OR 97128
Phone:	503-474-4917
Email:	manfrinl@co.yamhill.or.us
Website address (<i>optional</i>):	

Additional contact for third party

*This individual will be the contact for setting up or terminating users for the third party. (This is **not** a DHS/OHA employee.)*

Same contact information as above.

Section 2. Governing contract details

A DHS/OHA employee fills out this section. If a [governing contract](#) applies, please complete all applicable fields, below.

Does a governing contract establish a need for access? Yes No

Background checks

Please ensure all applicable required background checks are completed. DHS and OHA systems containing or accessing regulated data may require additional background check requirements beyond the pre-employment background checks. Regulated data sets requiring additional background checks include but are not limited to:

- Criminal Justice Information (CJI) in the Criminal Justice Information Services (CJIS) policy, 5.12.1 Personnel Security Policy and Procedures
- Federal tax information (FTI) as documented in Internal Revenue Service (IRS) Publication 1075, 5.1.1 Background Investigation Minimum Requirements.

Direct questions related to the background check process to BCU.Info@state.or.us or 503-378-5470 or 1-888-272-5545.

Section 3. Access description

Reason for access

Describe in detail the [business need](#) for access:

All Community Certified Behavioral Health Clinics (CCBHCs) in Oregon need access to internal Behavioral Health Analytics (BHA) Power BI reports housed within the BHA Power BI Workspace. Federal CCBHC Certification Criteria outlines the following need for access: "States participating in the Section 223 Demonstration program are expected to share the results from the State-Collected measures with their Section 223 Demonstration program CCBHCs in a timely fashion". This language is found on page 43 of the federal criteria document: <https://www.samhsa.gov/sites/default/files/ccbhc-criteria-2023.pdf>

The data will be sourced from both the CCBHC-based electronic health records (EHRs) as well as from the Oregon Medicaid Management Information System (MMIS), the Measures and Outcomes Tracking System (MOTS) and the Mental Health Statistics Improvement Program (MHSIP). Though the reports will not display any client-level data, the reports cannot be shared publicly as they will display federally-mandated quality performance metrics specific to each CCBHC. The CCBHCs have not approved of this information being released publicly, nor have they approved of sharing their performance metric results amongst other CCBHCs. The BHA team needs to share these individual reports exclusively with the aforementioned third party for purposes of quality improvement and clinical monitoring. Once the CCBHC viewer opens the link, they will need to login using their assigned OHA email account, password and multi-factor authentication.

Given that these reports cannot be shared publicly or shared with other CCBHCs, CCBHCs will access their individual reports as "viewers" only through a secure link that is provided by the BHA Power BI Workspace administrator, Jonnaliz Corbett (jonnaliz.r.corbett@oha.oregon.gov). Once the CCBHC viewer opens the link, they will need to login using an assigned OHA email account. For this reason, third party viewers need network login credentials, including an OHA email account, password and multi-factor authentication (MFA).

Requested access start date: _____

Method of access

Check all methods the third party will use to access DHS/OHA information systems.

- DHS/OHA on-site Will only use DHS/OHA supplied PC, laptop or workstation: Yes No
- Remote access via **VPN** Will only use DHS/OHA supplied PC, laptop or workstation: Yes No
- Remote access via **Citrix**
- Access to folder on **Secure File Transfer Protocol (SFTP) server**
- Other (*explain below*): Will only use DHS/OHA supplied PC, laptop or workstation: Yes No

CCBHCs will access individual reports as "viewers" only through a secure link that is provided by the BHA Power BI Workspace administrator, Jonnaliz Corbett (jonnaliz.r.corbett@oha.oregon.gov). Once the CCBHC viewer opens the link, they will need to login using their assigned OHA email account, password and MFA through the Microsoft Authenticator application. Further, a link can only be opened by a CCBHC user who has been granted access to view that specific report by the BHA Power BI Workspace administrator. CCBHC report viewers do not need a Power BI Pro account in order to view the reports as they will be able to access the report through Power BI Service, which is the free cloud-based software.

Access and information flow will occur from:

DHS/OHA to third party (i.e., third party has access to DHS/OHA's information assets and systems)

Scope of access

List all system names the third party needs to access. (*This form authorizes access for the third-party organization as a whole. A partner number [P#] and a network login are needed to access the following information systems. The system-specific individual user access request forms must be used to request access for individual third-party employees using the system.*)

- Email:** DHS/OHA email account authorized. This authorizes the third party to get DHS/OHA email accounts after receiving a completed individual user access request form for each individual.
- Network:** Network login authorized. This authorizes the third party to get DHS/OHA network login IDs after receiving a completed individual user access request form for each individual.

System 1
Name of system: Power BI
Type of access requested: View only (please describe):
Description of access: Designated CCBHC users will be granted access as a "viewer" of individual reports housed in the OHA_HA_BH_CCBHC Power BI Workspace. Report viewers can interact with the report along with exporting visuals and summary tables displayed, though they cannot access the underlying datasets. The data in the underlying datasets originates from CCBHC EHRs as well as from MMIS, MOTS and MHSIP. This workspace was created as an added layer of security to prevent CCBHCs from potentially gaining access to other reports produced by the Behavioral Health Analytics team. Though all CCBHC Power BI reports will be housed in the OHA_HA_BH_CCBHC workspace, the BHA Power BI Workspace administrator will be able to control access on a report-by-report basis. For reports created solely for a specific CCBHC, only viewers associated with that CCBHC will be granted access the report.
Expiration date of access: 02.26.2026
Information type Will information being shared or accessed be identifiable (i.e., names, DOB, address, etc.)? <input type="radio"/> Yes <input checked="" type="radio"/> No

Information owner review (<i>internal use only</i>)	
Name of reviewer: Lisa Wyman	Review date: 12.14.23
Access determination:	
Role or group assigned (<i>if applicable</i>):	
Access is: Choose one	
Reason for determination:	

System 2	
Name of system: Oregon Medicaid Management Information System - MMIS	
Type of access requested: View only (please describe):	Data will be visualized in Power BI
Description of access: Designated CCBHC viewers will be able to view summarized metric results originating from MMIS data. The most granular level of reporting will be at the subpopulation level (race, age, dual-eligibility status, etc.) and client-level data will not be accessible.	
Expiration date of access: 02.26.2026	
Information type	
Will information being shared or accessed be identifiable (<i>i.e., names, DOB, address, etc.</i>)?	
<input type="radio"/> Yes <input checked="" type="radio"/> No	
Information owner review (<i>internal use only</i>)	
Name of reviewer: Christopher W. Coon	Review date: 11/9/2023
Access determination:	
Role or group assigned (<i>if applicable</i>):	
Access is: Granted as requested	
Reason for determination:	

System 3	
Name of system: Mental Health Statistics Improvement Program - MHSIP	
Type of access requested: View only (please describe):	Data will be visualized in Power BI
Description of access: Designated CCBHC viewers will be able to view summarized metric results originating from MHSIP data. The most granular level of reporting will be at the subpopulation level (race, age, dual-eligibility status, etc.) and client-level data will not be accessible.	
Expiration date of access: 02.26.2026	
Information type	
Will information being shared or accessed be identifiable (<i>i.e., names, DOB, address, etc.</i>)?	
<input type="radio"/> Yes <input checked="" type="radio"/> No	
Information owner review (<i>internal use only</i>)	
Name of reviewer: Rebekah Gould	Review date: 11/13/2023
Access determination:	
Role or group assigned (<i>if applicable</i>):	

Access is: Choose one
Reason for determination:

System 4

Name of system: Measures and Outcomes Tracking System - MOTS/Resilience Outcomes Analysis

Type of access requested: View only (please describe): Data will be visualized in Power BI

Description of access:
 Designated CCBHC viewers will be able to view summarized metric results originating from MOTS/ROADS data. The most granular level of reporting will be at the subpopulation level (race, age, dual-eligibility status, etc.) and client-level data will not be accessible.

Expiration date of access: 02.26.2026

Information type

Will information being shared or accessed be identifiable (i.e., names, DOB, address, etc.)?

Yes No

Information owner review (internal use only)

Name of reviewer: Gina Mason	Review date: 10/24/2023
------------------------------	-------------------------

Access determination:

Role or group assigned (if applicable):

Access is: Granted as requested

Reason for determination:

Check all methods the third party will use to access DHS/OHA information systems.

Section 4. Program sponsor

The **program sponsor** is the DHS or OHA manager who sponsors the requested access. That person must monitor and ensure the third party complies with the terms and conditions of the access agreement. (Note that the program sponsor is usually the contract administrator of the governing contract authorizing the access.)

Verification of need to know:

As program sponsor, I certify that sections 1 through 3 of this form note the minimum necessary access.
 Date: 09/28/2023

Name (first, last):	Lisa Wyman
Position/title:	Behavioral Health Analytics Manager/Health Policy and Program Manager 3
Office:	Health Policy & Analytics
Program:	Behavioral Health Analytics
District name:	N/A
Work street address:	500 Summer Street NE
City, State, ZIP:	Salem, OR 97301
Phone (include ext.):	971-372-1981
Email:	lisa.wyman@oha.oregon.gov

Section 5. Program requestor

The **program requestor** is the DHS or OHA staff person who works with the third party on a day-to-day basis. That person requests the access agreement for the third party. The requestor can be the same person as the program sponsor or contract administrator. However, a program can list separate requestors/contract administrators. This will ensure all relevant parties receive contract communication and expiration notices.

Check this box and skip this section if the program requestor is also the program sponsor.

Name (<i>first, last</i>):	Drew Docter
Position/title:	Research Analyst 4
Office:	Health Policy & Analytics
Program:	Behavioral Health Analytics
District name:	N/A
Work street address:	500 Summer Street NE
City, State, ZIP:	Salem, OR 97301
Phone (<i>include ext.</i>):	971-393-3863
Email:	Drew.D.Docter@oha.oregon.gov

Submission

Click the submit button below to submit electronically, or email this completed form to the Information Exchange (InfoEx) Program within the Information Security and Privacy Office at DHSOHA.InfoEx@dhsoha.state.or.us. You can also email this address if you need more help.

Policy reference: <https://apps.state.or.us/Forms/Served/de090-003.pdf>

Submit by email

DHS/OHA Information Security and Privacy Office use only

Date received: 12.14.23	Date completed: 02.26.24
Date approved by all information owners: 12.14.23	Date executed: 02.26.24
Notes: 785 and signed AA (2024) on file.	
Completed by: Shannon Corr	

B.O. 24-57
Exhibit A