Oregon Provider Directory Policies and Procedures

Contents

Section 1: Who Must Comply with the Oregon Provider Directory (OPD) Policies and Procedures

These Policies and Procedures represent an important safeguard for protecting information from various internal and external risks, including unauthorized access. They are a part of the agreement between OHA and each participating entity and Authorized User. Each participating entity, Authorized User, and Extract Recipient must review and enter into an agreement to comply with these Policies and Procedures prior to being granted access to the System or Provider Data.

1. All participating entities that have signed an organizational participation agreement ("Participation Agreement") and wish to participate in the Oregon Provider Directory must comply with these Policies and Procedures. Participating Entity's failure to comply with these Policies and Procedures constitutes a breach of the Participation Agreement and may result in termination of the Participation Agreement, denial of access to the System, or other sanctions as may be designated in the Participation Agreement and in these Policies and Procedures.

2. All Authorized Web Portal Users of a participating entity, Oregon Health Authority, and the Department of Human Services that have signed an Authorized User Agreement must comply with the provisions of these

Policies and Procedures as applicable to Authorized Web Portal Users. An Authorized Web Portal User's failure to comply with applicable provisions of these Policies and Procedures constitutes a breach of the Authorized User Agreement and may result in termination of the Participation Agreement, denial of access to the System by the Authorized Web Portal User, or other sanctions as may be designated in the Authorized User Agreement and in these Policies and Procedures.

3. All Authorized System to System Interface Users of a participating entity, Oregon Health Authority, and the Department of Human Services that access the System must comply with the provisions of these Policies and Procedures applicable to Authorized System to System Interface Users. An Authorized System to System Interface User's failure to comply with applicable provisions of these Policies and Procedures constitutes a breach of the Participation Agreement and may result in termination of the Participation Agreement, denial of access to the System or Provider Data by the Authorized System to System User, or other sanctions designated in these Policies and Procedures.

4. All Extract Recipients that have received OHA authorization and have signed a data use agreement ("Extract Agreement") with OHA to use Provider Data for purposes set forth in the Extract Agreement must comply with these Policies and Procedures. An Extract Recipient's failure to comply with these Policies and Procedures applicable to Extract Recipients constitutes a breach of the Extract Agreement and may result in termination of the Extract Agreement or other sanctions as may be designated in the Extract Agreement and in these Policies and Procedures.

Section 2: Definitions

1. **"Agreement"** means a Participant Agreement, Authorized Web Portal User Agreement, or Extract Agreement.
2. **"Authorized Provider Data Extract Recipient" or "Extract Recipient"** means those persons or entities that do not have access to the Oregon Provider Directory System but receive OHA-approved limited data extracts that meet criteria for permitted uses of the data.
3. **"Authorized System to System Interface Users"** means those persons who have been authorized by Participating Entity to access the Oregon Provider Directory System via a System to System Interface.

4. "**Authorized Users**" means Authorized System to System Interface Users and Authorized Web Portal Users that may include, but are not limited to, healthcare providers and employees, staff, contractors, or agents of Participating Entity.

5. **"Authorized Web Portal Users"** means those persons who have been authorized by Participating Entity to access the Provider Directory System.

6. **"Breach"** means the acquisition, access, use, or disclosure of Provider Data in a manner not permitted by the Agreement which compromises the security or privacy of Provider Data.

7. **"Data Contributor" or "Data Source"** means a participating entity that contributes data to the Oregon Provider Directory.

Section 3: Authentication

1. **Purpose.** Authentication is the process of verifying that a Participating Entity, and its designated Organization Administrator who is seeking to access information via the System, is the organization or individual.

2. **Process.** OHA's vendor OneHealthPort, is responsible for authorizing and authenticating a Participating Entity and its designated administrator(s) ("Administrator") who will be responsible for granting and managing access to Authorized Users within its Organization. The process of authorizing and authenticating will include verifying the identity of Participating Entity, its Organization Administrator(s) and the administrator's affiliation with Participating Entity based on the information provided to OneHealthPort.

Section 4: Access

1. **Purpose.** Access controls govern when and how Authorized Users or a Participating Entity may access the System. These access policies are designed to minimize unauthorized access and ensure that Provider Data are used for authorized purposes. In addition, access to the System and Provider Data is available only to Participating Entities and Extract Recipients that are considered part of the "Medicaid enterprise" (see below). OHA will determine whether the organization is part of the Medicaid enterprise prior to

approving access. In the future with approval by Centers for Medicaid and Medicare Services, OHA may allow access to entities that do not qualify as part of the Medicaid enterprise ("Non-Medicaid entities").

This Section 4 describes the entities that are part of the Medicaid enterprise, and the minimum controls that Participating Entity shall implement to ensure that: (1) only Authorized Users access Provider Data via the System or a System to System Interface; and (2) they do so only in accordance with the requirements (specified herein) that limit their access to specified information.

2. **Medicaid Enterprise.** The following entities are considered part of the Medicaid enterprise:

- Oregon Health Authority (OHA) and Department of Human Services (DHS)
- Entities currently enrolled or contracted with OHA to provide Medicaid services. This includes but is not limited to Coordinated Care Organizations (CCOs) and their affiliated entities, individual practitioners, facilities, and hospitals
- Entities that participate in statewide health information exchange and submit health information exchange endpoints for its providers as a Data Contributor
- Entities that have been pre-approved by OHA to supply Provider Data as a Data Contributor to improve Provider Data quality

Entities that are selected by OHA to participate in soft launch. Soft launch is a period when the OPD is initially deployed to a targeted audience. During soft launch, users assess the value of the OPD and its readiness to be deployed to additional users across the state.

b. Authorized Users. Participating Entity is responsible for facilitating its Authorized Users' access to the System through a Web Portal or System to System Interface, and will identify individuals within its organization that need access to carry out their professional responsibilities. This may include, but are not limited to, health care providers, employees, staff, contractors, or agents of an organization.

c. System Access Specifications. The Program will provide two methods to access Provider Data in the System:

- **A Web Portal** that may be used to search and access reports for Provider Data accessed within the System.

- **System to System Interfaces** including Application Programming Interfaces (APIs) that may be used by a Participating Entity to access Provider Data within their own software applications or their instance of a commercial product by establishing a connection to the System.

d. **Access via Web Portal User.** Participating Entity will identify an Administrator (or delegate) who will take the steps necessary to obtain a user name and password for each Authorized Web Portal User and will require that Authorized Web Portal Users agree to terms in the Authorized Web Portal User agreement. Authorized Web Portal Users must be informed of the Administrator as the point of contact for all questions, training, and to whom reports of any potential unauthorized access must be made. This contact information must be readily available to all Authorized Users within the organization. OneHealthPort's policies that describe responsibilities of an Administrator can be found on their website: http://www.onehealthport.com/sso/register-your-organization and http://www.onehealthport.com/sso/frequently-asked-questions.

e. **Access via System to System Interface User.** Participating Entity will identify an Administrator who will be responsible for establishing, supporting, managing, and maintaining the interface with the System, granting access to its Authorized System to System Interface Users. Authorized System to System Interface Users must be informed of the Administrator as the point of contact for all questions, training, and to whom reports of any potential unauthorized access must be made. This contact information must be readily available to all Authorized Users within the organization.

f. **Access Records.** A Participating Entity shall maintain all records of access and training as part of contract compliance documentation for six years. Records include, but are not limited to names of Authorized Users, dates when access was granted, dates when training was completed, details if a user has violated the User Agreement, dates if access is terminated and reason for termination, and dates if access is reinstated.

g. **Access Limited to Minimum Necessary Information.** Participating Entity shall ensure that reasonable efforts are made to limit the information accessed via the System to the minimum amount

necessary to accomplish the intended purpose for which the information is accessed. An Authorized User shall limit access to the System to the minimum amount necessary to accomplish the intended purpose for which the information is accessed.

h. Training. The access controls set forth above will only be effective if Authorized Users understand their responsibilities to comply with these Policies and Procedures.

- OHA will provide training materials to Participating Entity on the technical aspects on how to use the System and the System to System Interface. Participating Entity shall ensure that its Authorized Users review the training materials provided before they begin to use the System.
- Participating Entity shall ensure that each of its Authorized Users review and execute an Authorized User Agreement, including review these Policies and Procedures, before they begin to use the System.
- OHA will provide an implementation guide to Participating Entity that describes the technical details for how to connect to the System to access Provider Data using a System to System interface.

i. Termination of Access and Other Sanctions. Participating Entity shall ensure that an Authorized User's access to the System and Provider Data is terminated in the following situations:

- Immediately or as promptly as reasonably practicable but in any event within one business day of termination of a Participating Entity's Agreement with OHA;
- Immediately following an Authorized User's failure to comply with the Authorized User Agreement; or
- Immediately or as promptly as reasonably practicable but in any event within one business day of notification of termination of an Authorized User's employment or affiliation with Participating Entity.
- Participating Entity shall notify OHA immediately upon termination of an Authorized User's access to the System due to an Adverse Security Event.

Section 5: Audit

1. **Purpose.** Audits are useful oversight tools for recording and examining access to information through the System (e.g., who accessed what data and when) and are necessary for verifying compliance with access controls like those specified in Section 4, and are developed to prevent/limit inappropriate access to information. This Section 5 sets forth minimum requirements that Participating Entity shall follow for audits regarding access to Provider Data via the System.

2. **Compliance Audits.** OHA (or a third party engaged by OHA) may audit Participating Entity on a periodic basis. The purpose of the audits will be to confirm compliance with and proper use of the System and Provider Data in accordance with the Agreement, including the Policies and Procedures.

3. **Conduct of Audits.** Audits will take place during normal business hours and at mutually agreeable times and shall be limited to such records, personnel and other resources of Participating Entity as are necessary to determine proper use of the System and Provider Data, compliance with the Agreement, or the Oregon Provider Directory Policies and Procedures, or to comply with applicable state or federal requirements. Each Party will bear its own costs relating to audits relating to this Agreement. OHA will conduct audit activities in a manner designed to reasonably minimize interference with Participating Entity's day-to-day operations.

Section 6: Adverse Security Events

1. **Purpose.** This Section 6 sets forth minimum standards OHA, Participating Entity, Authorized Users, and Extract Recipients shall follow in the event of any actual or suspected Breach, unauthorized use of the System or Provider Data, or other mis-use of the System or Provider Data ("Adverse Security Event"). These standards are designed to promote accountability, assure providers and all parties' about the Program's commitment to privacy and security, and mitigate any harm.

2. **Responsibilities of a Participating Entity or Extract Recipient.** In the event that a Participating Entity or Extract Recipient becomes aware of an Adverse Security Event, a Participating Entity or Extract Recipient shall:

a. **Notify OHA.** Notification must be made in the most expedient time possible and without unreasonable delay. Notification will be given by personal delivery, prepaid certified or registered U.S. mail, reputable commercial overnight courier service with tracking capabilities, by facsimile, or by email if receipt of email is confirmed within 48 hours to OHA:

Office of Health information technology
500 Summer Street NE, E-52
Salem, OR 97301
ATTN: Oregon Provider Directory Program
Facsimile: 503-378-6705
Oregon.Provider-Directory@dhsoha.state.or.us

b. **Investigate the Adverse Security Event.** In the most expedient time possible and without unreasonable delay, investigate the scope and magnitude of the Adverse Security Event, and identify the root cause of the Adverse Security Event.

c. **Mitigate.** To the extent practicable, mitigate any harmful effect of the Adverse Security Event that is known to Participating Entity or Extract Recipient.

3. **Responsibilities of OHA**. In the event OHA becomes aware of an Adverse Security Event, OHA will:

a. **Notify Participating Entity or Extract Recipient**. Notify any Participating Entity or Extract Recipient whose data is affected by the Adverse Security Event.

b. **Investigate the Adverse Security Event.** In the most expedient time possible and without unreasonable delay, investigate (or require the applicable Participating Entity or Extract Recipient to investigate) the scope and magnitude of the Adverse Security Event, and identify the root cause of the Adverse Security Event.

c. **Mitigate.** Mitigate (or require the applicable Participating Entity to mitigate) to the extent practicable, any harmful effect of an Adverse Security Event that is known to OHA, Participating Entity, or an Extract Recipient. OHA's mitigation efforts shall correspond with and be dependent upon their internal risk analyses.

d. **Notify**. Notify (or require the applicable Participating Entity or Extract Recipient to notify) the provider and any applicable regulatory agencies as required by and in accordance with applicable federal, state, and local laws and regulations.

4. **Sanctions**. OHA may impose sanctions to Participating Entity and its Authorized Users or on Extract Recipients in the event of an Adverse Security Event, and may impose or may require a Participating Entity to impose sanctions on its Authorized Users. Such sanctions may include but are not limited to temporarily restricting or terminating an Authorized User's access to the System or Provider Data; requiring Authorized Users to undergo additional training in the use of the System; requiring the destruction of all Provider Data provided to Participating Entity or Extract Recipient and confirming such destruction; or terminating a Participating Entity's participation in the Oregon Provider Directory Program.

Section 7: Data Contribution

1. **Purpose.** This Section 7 sets forth minimum standards OHA and Participating Entity shall follow to ensure data of the highest quality is maintained in the Oregon Provider Directory. Data displayed in the Oregon Provider Directory are gathered from multiple Data Contributors. These data are cleaned, matched, and compiled. The highest quality data elements, as determined by the Program, are then displayed in a Master Record. Data Contributors are responsible for ensuring the data elements they contribute are accurate.

2. **Data Contributor Source Records.** Data Contributors provide data to the Oregon Provider Directory ("Source Records") in two ways. Source Records remain the intellectual property of the Data Contributor.

   a. **Data Contribution by Data Entry.** A Data Contributor may enter data using the System's web portal. Any Authorized User may contribute Source Records by data entry.

   b. **Data Contribution by File Upload or Interface.** A Data Contributor may submit data on a scheduled basis for a set of providers by establishing file uploads in the web portal or by system to system interfaces.

      - **Data Source Onboarding.** Prior to submitting data to the System, the Program will work with the Data Contributor to

review all data submission specifications in the onboarding process which includes the review of data transport options, data that will be included in the submission, the frequency of transmission, and testing. The System will send a confirmation notification for data transmission acceptance/failure.

- **Data Transport**. Transport mechanisms to submit the data are listed in the data source onboarding form. Refer to the website for the most current version of the document. <website here>

- **Data Fields.** Data that can be submitted to the Oregon Provider Directory are listed in a data loading specification document. Refer to the program website for the most current version of this document. <website here>

- **Restricted Data.** In the future, Data Contributors may be able to request to restrict viewing of source data or subset of source data ("Restricted Data") to certain users or classes of users.

- **Frequency of Transmission.** Data Contributors select the frequency for their data submissions (e.g., weekly, monthly, or quarterly) and agree to submit on an ongoing basis according to the agreed upon frequency until termination of the Agreement.

3. **Master Records.** Source Records are cleaned, deduplicated, formatted, parsed, selected, matched, and merged to create a single master record ("Master Record") according to a set of business rules. Because Source Records from Data Contributors may conflict, trust preferences in the business rules determine which source record to include in the Master Record. Business rules are reviewed on an ongoing basis by the Program and updated when necessary. Master Records are OHA work product and the intellectual property of OHA.

4. **Data Discrepancy Flagging.** Authorized Users may report data discrepancies in either a Source Record or a Master Record to the Program. Authorized Web Portal Users may report or flag Provider Data discrepancies within the System. Authorized System to System Interface Users may report Provider Data discrepancies by contacting the help desk at help@Oregon-PD.org. The Program will research and verify the discrepancies. If the Provider Data is found to be inaccurate, the Program will change the Master Record by adding a program level source record with the correct data, notify the Authorized User who reported the discrepancy, and if provided by a file upload or interface, notify the Data Contributor who provided the data.

5. **Data Stewardship.** The Program will provide data stewardship services over Provider Data quality. Such services consist of automated and manual activities.

   a. **Automated Data Stewardship** includes data management tasks to clean, deduplicate, format, parse, select, match, and merge data.

   b. **Manual Data Stewardship** includes performing data management tasks that could not be automated and the following:

      - Conducting randomized sampling of Provider Data
      - Resolving data discrepancy flags submitted by Authorized users
      - Reaching out to Data Contributors when necessary to resolve data file errors or missing file submissions, or other data improvement efforts
      - Reaching out to providers or their designated contacts directly to resolve data validation errors

Section 8: Data Use Policies

1. **Purpose.** This Section 8 outlines permitted, prohibited, and limited uses for the Provider Data. Data Contributors that provide data to the Oregon Provider Directory do so with the expectation it will only be used in the manner specified in these Policies and Procedures. Participating Entity, Authorized Users, and Extract Recipients are authorized to access Provider Data only for purposes allowed under these Policies and Procedures.

2. **Permitted Uses.** OHA provides Provider Data for the purposes of participating entities' managing internal provider directories and networks, finding contact information such as Direct secure messaging email addresses or phone numbers for providers to enable health information exchange, and utilizing practice and program information to support the calculation of metrics and outcomes.

3. **Prohibited Uses.** Participating Entity shall not use Provider Data for any purpose not listed in this section or otherwise authorized in advance (e.g., via an Extract Agreement), and shall not make available, transfer, or sell Oregon Provider Directory data or files to a third party, without the express consent of the parties concerned. This includes but is not limited to:

   a. pop-up ads

b. soliciting business

c. surveys not pre-authorized in writing by the Program

d. spamming messages

e. direct marketing, database marketing, or telemarketing activities

Violation of this section may result in immediate suspension under Section IV.3, or termination under Section IX.2. of the Agreement.

4. **Limited Uses**. At its discretion, OHA may provide limited data sets to Extract Recipients who have received authorization from OHA to receive extracts for authorized research purposes.

a. Extract Recipients do not have access to the System and may only use the data for purposes outlined in an agreement with OHA and for no other purposes.

b. Extract Recipients are required to submit an application to OHA that includes: information the purpose for the request, how data will be used, if it has been approved by the organization's institutional review board, and the timeline for the project. Refer to the Oregon Provider Directory website at https://www.oregon.gov/oha/HPA/OHIT/Pages/PD-Overview.aspx for more information on data requests.

c. Data requests are approved by a data review committee established by OHA.

d. Data elements requested by Extract Recipients may include any element that is included as a viewable field by Authorized Users in the Oregon Provider Directory.

e. Extract Recipients are required to sign an agreement which outlines the agreement for the limited use of the data, and the privacy and security requirements for that use.

5. **OHA Uses.** OHA and DHS may use Provider Data to evaluate and inform statewide health policy and programs. This includes but is not limited to: reporting on program participation and impacts of programs around the state, publishing reports on health care outcomes and utilization, conducting environmental scans, overseeing public health surveillance and practice, managing OHA and DHS provider directories, finding

providers and their practice information, and supporting evaluation, forecasting, and audit functions of OHA and DHS programs.

Section 9: Notice and Process for Updating the Policies and Procedures

1. **General**. OHA will make available the current versions of the Policies and Procedures on its website at https://www.oregon.gov/oha/HPA/OHIT/Pages/PD-Overview.aspx. Interested parties may sign up to receive notices and provide feedback when there are proposed changes to the Policies and Procedures by subscribing to updates here: https://public.govdelivery.com/accounts/ORDHS/subscriber/new?topic_id=ORDHS_635. General questions may be directed to the Oregon Provider Directory Program at Oregon.Provider-Directory@dhsoha.state.or.us.

2. **Notice of Changes.** OHA may implement any new Policies and Procedures, or amend, or repeal and replace any existing Policies and Procedures, at any time by providing participating entities and Extract Recipients Users with notice of the change via email at least 30 calendar days prior to the effective date of the change, unless in OHA's sole discretion a shorter time frame is required.

    a. Participating entities and Extract Recipients shall inform their respective Authorized Users of updates to the Policies and Procedures. Authorized Users shall to review updates to the Policies and Procedures following notice of the update(s).

    b. Within 15 calendar days of receiving notice of the change, a participating entity, Extract Recipient, or Authorized User may request that OHA delay implementation of the change based on unforeseen complications or other good cause. OHA will respond to a request to delay implementation within seven calendar days of receiving the request. Continued use of the System or Provider Data after the effective date of a change of the Policies and Procedures constitutes acceptance of such Policies and Procedures.