Oregon Public Health Epidemiology User System (Orpheus) and Orpheus Linked Databases – Security Policies and Procedures

Version 6 – October 10, 2025

Table of Contents

Overview

This document describes the security policies and procedures for accessing and using the Oregon Public Health Epidemiology User System (Orpheus) and its associated databases. These policies align, where applicable, with the Centers for Disease Control and Prevention's (CDC's) *Data Security and Confidentiality Guidelines* (2011).[1]

Orpheus is Oregon's statewide database for managing reportable disease information. It was developed by the Oregon Health Authority (OHA), Oregon Public Health Division (OPHD), Center for Public Health Practice (CPHP), and serves as a comprehensive case reporting system for public health surveillance and response. The application and its data are hosted on secure State of Oregon servers located in Salem. All surveillance data in Orpheus are owned by OHA. Orpheus is intended for use by authorized public health officials to investigate, analyze, and report on reportable diseases and outbreaks in Oregon.

Orpheus operates in a secure environment that adheres to rigorous information security standards. These include access controls, encryption at rest, secure backups with recovery strategies, and regular audits. This infrastructure supports compliance with state and federal regulations and reduces the risk of data breaches or unauthorized access.

Orpheus and its linked databases contain confidential, personally identifiable information (PII) collected during public health investigations. Authorized users access Orpheus through a secure Citrix gateway using multifactor authentication (e.g., YubiKey or Microsoft Authenticator). This information is protected under Oregon Revised Statute (ORS) 433.008[2] and may only be disclosed under specific legal circumstances. Improper disclosure is prohibited. All data use must comply with ORS 433.008. Users and their organizations are responsible for securing any data exported from Orpheus.

This document defines the responsibilities of all users in protecting the confidentiality, integrity, and security of data within Orpheus. It outlines the legal requirements, operational standards, and procedures that must be followed by public health professionals from Tribal, local, and state health authorities. All users must review and

[1] https://www.cdc.gov/program-collaboration-service-integration/php/index.html
[2] https://www.oregonlegislature.gov/bills_laws/ors/ors433.html

comply with these policies before accessing Orpheus. The Overall Responsible Party (ORP) for each organization is accountable for ensuring compliance.

Policies

1) Written Policies and Procedures

1. The Oregon Health Authority (OHA) will maintain an up-to-date copy of this document on its website: http://healthoregon.org/orpheus
2. Each Overall Responsible Party (ORP), their designees, and each Approved Entity (AE)—such as Local Public Health Authorities (LPHAs), Oregon Enterprise Technology Services (ETS), and Tribal jurisdictions—must also maintain at least one current copy of this document.

2) Overall Responsible Party (ORP) and Designees

A. Oregon Health Authority (OHA) ORP

The Overall Responsible Party (ORP) at the Oregon Health Authority (OHA) is responsible for overseeing the security of Orpheus data accessed by its Authorized Users (AUs). This role is held by the Administrator of the Center for Public Health Practice (CPHP) within the Oregon Public Health Division, or their designee.

The OHA ORP or designee must:

1. **Authorize** access to record-level Orpheus data for OHA staff or affiliates, based on work-related need.
2. **Assign** each OHA AU to defined privileges within Orpheus which determine their ability to view, enter, or edit data; approve design changes; or manage other users' access.
3. **Conduct** an annual review of security practices, in consultation with Oregon's Information Security and Privacy Office (ISPO), including:
    a. Reviewing current technologies to ensure that data security and policy alignment.
    b. Preparing a written report to accompany certification of compliance with CDC Program Requirements.

4. **Ensure** that all current OHA AUs sign an annual confidentiality assurance statement confirming their understanding of and compliance with Orpheus confidentiality policies. These attestations are maintained electronically in the Orpheus Oath tool.
5. **Submit** deactivation requests via the Orpheus Oath tool for OHA AUs who no longer require access.
6. **Review** these policies and procedures annually with all active OHA AUs and respond to any questions.
7. **Conduct** an annual security audit with each OHA AU and attest that the following have been completed:
    a. The AU's Orpheus activity has been reviewed.
    b. The AU has read and is familiar with this document.
    c. The AU has reviewed OHA-specific security and confidentiality policies (e.g., the 090 and 100 series).[3]
    d. The AU's secure data export location(s) have been verified.
    e. The AU has deleted exported files that are no longer in use.
    f. The AU's access privileges have been confirmed.
8. **Deactivate** OHA AUs and AE ORPs who do not complete the required annual security audit and documentation within two months of receipt.
9. **Ensure** that any State of Oregon IT personnel with incidental access to Orpheus data (e.g., server or backup access) comply with the substance of these policies by:
    a. Maintaining a current list of personnel at Oregon Enterprise Technology Services (ETS) or other co-located sites who have access to Orpheus data, including the date of their most recent security or privacy training.

[3] http://www.oregon.gov/oha/OIS/ispo/Pages/policies.aspx

b. Reviewing, at least annually, the list of users with privileged access to relevant servers in coordination with Oregon's Office of Information Services (OIS).

10. **Ensure** that all OHA AUs follow OHA data security policies,[4] including:
    a. Protecting passwords, keys, and access codes.
    b. Avoiding malware and viruses.
    c. Using state-issued devices only for official work.
    d. Minimizing the export of personally identifiable information (PII) and securely deleting it when no longer needed.
    e. Protecting mobile devices and storage media from loss and theft.
    f. Safeguarding the security of any OHA device that stores PII from Orpheus.
    g. Reporting suspected security breaches using the OHA Privacy and Compliance Incident Report Form.[5]
11. **Oversee** periodic random audits of AU activity logs, investigate irregular use, and maintain records of audit outcomes.
12. **Ensure** that any PII sent via email is encrypted using OHA's standard (i.e., "#secure#" in the subject line). PII must never appear in the subject line.[6] When referring to a specific case, users should refer to the Orpheus Case or Person ID.

---

[4] ODHSOHA Administrative, Technical and Physical Safeguards section 16 states that:
ODHS and OHA staff shall not connect non-agency owned or approved devices such as USB drives or printers to any ODHS and OHA network, with the limited exception of appropriate use of the guest network.
DAS 50.050.01 Working Remotely Policy 7(b): The agency provides basic technology equipment and related devices necessary for the employee to perform their assigned job duties at the alternate workplace. The equipment and devices are for agency business only and must comply with the agency's desktop security and maintenance policies and practices. Employees will not conduct state business on the following personal equipment: phones, computers, laptops or other information-storing devices. (A) Exceptions to section (b) are subject to the approval of the State Chief Operating Officer

[5] https://app.radarfirst.com/incidents/new/?token=99f17b20-f1bb-41c1-b27e-2d6e96150943#/guest-form/form
(Note: this link is not accessible to non-OHA/ODHS staff.)

[6] https://sharedsystems.dhsoha.state.or.us/DHSForms/Served/me090-015.pdf

B. Approved Entity (AE) ORP

An Approved Entity (AE)—such as a Local Public Health Authority (LPHA), Oregon Enterprise Technology Services (ETS), or a Tribal jurisdiction—must have an Access Agreement on file with Oregon's Information Security and Privacy Office (ISPO). This agreement is initiated by OHA and executed by ISPO. Agreements are valid for two years and may be renewed as needed.

Each AE must designate an Overall Responsible Party (ORP) to oversee the security of Orpheus data accessed by its Authorized Users (AUs). The AE ORP or their designee must:

1. **Authorize** access to record-level Orpheus data for AE staff, based on work-related need.
2. **Assign** each AE AU to defined privileges within Orpheus which determine their ability to view, enter, or edit data.
3. **Ensure** that AE AUs comply with the requirements of this document, including any future updates.
4. **Ensure** that each AU signs an annual confidentiality assurance statement and completes annual security training. These attestations are maintained electronically in the Orpheus Oath tool.
5. **Submit** deactivation requests via the Orpheus Oath tool for AE AUs who no longer require access.
6. **Review** these policies and procedures annually with all active AE AUs and respond to any questions.
7. **Certify** the AE's adherence to these security policies and procedures upon request by the OHA ORP.
8. **Conduct** an annual security audit with each AE AU and attest that the following have been completed:
    a. The AU's Orpheus activity has been reviewed.
    b. The AU has read and is familiar with the Orpheus Security Policies and Procedures (this document).
    c. The AU has read and is familiar with AE-specific security and confidentiality policies.

d. The AU's secure data export location(s) have been verified.

e. The AU has deleted exported files that are no longer in use.

f. The AU's access privileges have been confirmed.

9. **Deactivate** AE AUs or who do not complete the required annual security audit and documentation within two months of receipt.
10. **Implement** more stringent local security policies, if needed, for AUs under the AE's jurisdiction.
11. **Ensure** that all AE AUs follow local data security policies, including:
    a. Protecting passwords, keys, and access codes.
    b. Avoiding malware and viruses.
    c. Using AE-issued devices only for official work.
    d. Minimizing the export of personally identifiable information (PII) and securely deleting it when no longer needed.
    e. Protecting mobile devices and storage media from loss and theft.
    f. Safeguarding the security of any device that stores PII from Orpheus.
    g. Reporting suspected security breaches immediately to the Orpheus Tech Team.
12. **Monitor** AE AU activity logs as needed, investigate irregular use patterns, and maintain records of any findings or corrective actions.
13. **Ensure** that any PII sent from Orpheus via email is encrypted using the AE's standard. PII must never appear in the subject line. When referencing a specific case, users should refer to the Orpheus Case or Person ID.

3) Authorized User (AU) Responsibilities and Requirements

Each Authorized User (AU) with access to record-level Orpheus data must be familiar with and comply with the security policies and procedures outlined in this document. The AU must:

1. **Review** these policies and electronically sign a confidentiality assurance statement before being granted access to Orpheus, and annually thereafter. Access will be denied to individuals who do not complete the required review and attestation.

2. **Challenge** any unauthorized access attempts and **report** suspected security breaches to their Overall Responsible Party (ORP) or designee, in accordance with the OHA Information Security Incident Reporting Process[7] and the OHA Report and Response to Privacy Incidents[8] policies.
3. **Protect** assigned workstations, laptops, and other devices used to access Orpheus data from theft or unauthorized disclosure. This includes:
    a. Safeguarding passwords, keys, and authentication devices.
    b. Preventing exposure to malware or viruses.
    c. Avoiding physical damage, including those caused by environmental factors.
4. **Comply** with all relevant security policies, even if not directly involved in public health data collection or case investigation. This includes system administrators and other staff with access to Orpheus data or infrastructure.
5. **Participate** in an annual security audit conducted by the ORP or designee that includes:
    a. Review of the AU's Orpheus activity. Irregular use patterns will be investigated. AUs found responsible for breaches of security protocol or confidentiality may:
        i. Have their access reduced or revoked.
        ii. Be subject to disciplinary action, up to and including termination.
    b. Confirmation that the Orpheus Security Policies and Procedures (this document) has been read.
    c. Confirmation that AE- or OHA-specific security and confidentiality policies have been read.
    d. Verification of the AU's secure data export location(s).
    e. Deletion of exported files that are no longer in use.
    f. Confirmation of the AU's access privileges needs.

[7] https://sharedsystems.dhsoha.state.or.us/DHSForms/Served/me090-005-01.pdf
[8] https://sharedsystems.dhsoha.state.or.us/DHSForms/Served/ME100-014.pdf

4) Security Breaches

Security breaches may involve either a violation of security protocols or the unauthorized disclosure of confidential data. All breaches must be reported and addressed in accordance with applicable policies.

A. Breaches of Security Protocol Without Breaches of Confidentiality

1. Anyone who becomes aware of a breach of security protocol that does not involve a breach of confidentiality must report it to their ORP or designee, the OHA ORP, or the Information Security and Privacy Office (ISPO).
2. The OHA ORP must ensure that all such reports are logged and investigated. OHA must maintain a breach log that includes:
    a. Date of the breach.
    b. Date the breach was reported.
    c. Description of the breach.
    d. Severity level.
    e. Investigators involved.
    f. Conclusions and any corrective actions taken.
3. The OHA ORP or their designee must review the breach log at least twice annually to identify recurring patterns or individual incidents that may require corrective action.

B. Breaches of Confidentiality

Breaches of confidentiality involve the unlawful or improper disclosure of confidential data. These may occur inadvertently (e.g., through employee error) or intentionally (e.g., sabotage or malicious activity).

1. All breaches of confidentiality, regardless of cause, must be reported within one working day to the OHA ORP. The OHA ORP is responsible for notifying ISPO and other entities as appropriate (e.g., CDC).
2. Employees responsible for a breach may be subject to disciplinary action, up to and including termination of employment, as determined by their employer.

3. In the event of a suspected intentional breach, the OHA ORP must consult with appropriate legal counsel to determine whether reporting to law enforcement is warranted.

5) Data Access and Use

Access to record-level data in Orpheus is restricted to Authorized Users (AUs) who have been approved by an Overall Responsible Party (ORP). Once an ORP identifies an individual who requires access, the following steps must be completed:

1. The ORP must provide the individual with this policy document.
2. The ORP must submit a user request via the Orpheus Oath tool.
3. The individual must review the policies and digitally sign the confidentiality assurance statement (i.e., the Oath).

An AU's access is governed by the privileges assigned by the ORP, based on the AU's role and responsibilities. AUs must log in to Orpheus at least once every 90 days to maintain an active account. If an account is deactivated due to inactivity, the ORP will be notified and must either request reactivation or confirm deactivation.

A. System Access

Each AU is assigned to a group that allows network access to Orpheus:

1. **Citrix – Orpheus**: Standard non-state user
2. **Citrix – Orpheus State**: Standard state user

B. Privileges

1. All AUs have default statewide access to all conditions except:
    a. HIV
    b. HIV/Sexually Transmitted Infection (STI) Statewide Services (HSSS)
    c. RESP-NET (COVID-19, influenza, RSV hospitalizations)
    d. Active Bacterial Core surveillance (ABCs includes invasive infections by groups A and B streptococci and *Streptococcus pneumoniae*)
    e. Cervical Intraepithelial Neoplasia (CIN)

2. Access to RESP-NET, ABCs, or CIN are special state-funded surveillance activities and approval is handled on a case-by-case basis.
3. By default, AUs with access to HIV data may view cases only within their jurisdiction. Temporary access to HIV cases outside their jurisdiction may be granted during an active session, is logged, and is revoked at the end of the session.
4. HSSS is a subset of HIV and STI cases that require additional approval from a designated OHA HIV ORP designee. AE ORPs may request access through the Orpheus Oath tool.
5. AUs may configure their settings to limit what is visible upon login (e.g., disease groups, jurisdictions, or date ranges). Any other change to an AU's profile must be initiated by an ORP through the Orpheus Oath tool.

C. Exporting Data

1. Each AU must annually identify, via the Oath tool, an ORP-approved location for storing any exported data containing personally identifiable information (PII).
2. ORPs should only approve storage locations that are:
    a. On restricted-access public health department networks behind firewalls.
    b. On password-protected local drives or encrypted media.
3. AUs unsure of appropriate storage locations must consult their supervisor.
4. AUs must obtain prior approval from their ORP or designee before storing or transferring data to any location not already approved.

D. Data Storage, Access, and Transfer

All data storage, access, and transfer must comply with the policies outlined in Section 6.B.

E. Cross-Jurisdictional Sharing

1. Orpheus uses both person- and case-centric functionality. Each individual is represented by a single "person record," which may be linked to multiple "case records."
2. AE ORPs authorize and manage case record access for AE AUs.

3. OHA ORPs authorize and manage case-record access for OHA AUs.
4. AUs have access to case records for all diseases and jurisdictions, except for HIV and special state projects (described above).
5. AE AUs are expected to work primarily within their assigned jurisdiction but may view or update cases from other jurisdictions when appropriate.

F. Changes to Data and Logging

Selected changes to Orpheus records and user actions are automatically logged. Users may view logged data for any case by selecting the “Log” tab from the left-hand panel of the case entry screen. Data collected in the log are used to generate the annual security audit reports.

The log includes:

1. Account Name and User ID of the AU.
2. Date and time of the change.
3. Details of the user action, script, or data change (including user login and logout, record views, field edits, data exports, etc.).

Viewing a case record is also logged, even if no changes are made. In addition to logging, AUs are notified via a “To Do” note when key fields are changed in case records for which they have primary responsibility. These fields include:

1. Case Status (including deletions or “no case” designations)
2. Deceased status
3. Disease
4. Hospitalization status
5. Outbreak association
6. County (includes contacts’ counties)

G. Resolution of Disputes

If a disagreement arises regarding case data, the parties involved must first attempt to resolve it informally. If unresolved:

1. The AE ORP (or designee, such as a Health Officer) for the county of residence at diagnosis will work with the OHA ORP to reach a resolution.
2. The AE's position will be given substantial weight; however, the OHA ORP retains final authority to determine case status (confirmed, probable, suspect, or non-case) to ensure consistency across jurisdictions.

H. Authorized Uses and Disclosures

AUs may use Orpheus data only in accordance with ORS 433.008 and these policies.

1. If an individual or their authorized representative requests a copy of their own record, an AU must submit the request via the "Public Records Request" button in the Orpheus Case Record. A specific review of the requested records will take place to ensure only information specific to the individual is included, and that information relating to other individuals or their connections is redacted.[9] The OHA ORP is responsible for reviewing and responding to the request, including attaching a copy of the response to the request. A signed OHA release, authenticated by either a notary public or the individual's attorney, is required.
2. If an AE receives a public records request (PRR) for Orpheus data under the state's Public Records Act (PRA, ORS 192),[10] it must be forwarded to the OHA ORP immediately. If the AE holds responsive records outside of Orpheus, it

[9] Only pertinent information regarding the subject person may be disclosed: the individual person's medical records, questionnaires completed by the individual person, interviews with the individual person, information contained in a larger document that is specific to the individual person. All other information, including the chart (which any information regarding others involved) should be redacted: case numbers, outbreak numbers, anything that identifies that there are other ill persons, anything that indicates that the person is associated with an outbreak.

[10] https://www.oregonlegislature.gov/bills_laws/ors/ors192.html

may respond directly but must inform the requestor that OHA is custodian of Orpheus data and will only respond upon receipt of the PRR.

3. Subpoenas or court orders for Orpheus data must be forwarded to the OHA ORP immediately.
4. Public health data may not be transferred from Orpheus to LPHA medical records. However, ORS 433.008 allows release of information (e.g., laboratory results) to health care providers if necessary for evaluation or treatment of a reportable disease. Such releases must be approved by the AE ORP and documented in Orpheus.
5. Statistical reports that do not identify individuals or sources of information may be published in accordance with ORS 433.008 and the *Oregon Public Health Division's Guidelines for Reporting Small Numbers to Protect Confidentiality*.[11] AUs should consult their ORP if unsure whether a release is permitted.

6) Data Security

All Authorized Users (AUs) must follow the data security requirements outlined in this section to protect the confidentiality, integrity, and availability of Orpheus data.

A. Physical Barriers

1. AUs must take reasonable precautions to ensure that Orpheus data are not visible or accessible to unauthorized individuals. This includes:
    a. Using screen privacy filters.
    b. Closing data files when others are present.
    c. Working in private or secure locations.
    d. Avoiding access to Orpheus in public settings.
2. Remote work areas must be approved by the ORP or their designee.
3. All areas used to access Orpheus data must remain secure at all times.

[11] A summary of this information is provided in Appendix A. The full version to those who have access to the OHA network or upon request.

4. For Oregon Department of Administrative Services (DAS)-managed facilities:
    a. Keys, codes or other entry control devices must be issued only to authorized personnel.
5. For AE-managed facilities:
    a. Keys, codes, or other entry-control devices must be issued only to those personnel authorized by the AE.
6. Keys, codes, or other entry-control devices should be changed at least annually and whenever an AU leaves employment.
7. The ORP or designee must maintain a current list of individuals authorized to access secure Orpheus work areas unaccompanied.
8. Unaccompanied access may be granted only to public health employees and building security staff.
9. Unauthorized individuals may only enter secure Orpheus work areas when escorted by authorized surveillance or IT personnel, or covered by a written and approved security policy.

B. Electronic Data Storage, Access, and Transfer

1. Storage of Record-Level Surveillance Data
    a. Laptop computers, removable hard drives, or external storage devices must be locked in a secure cabinet when not in use.
    b. These devices should only be used in secure, limited-access areas unless explicitly authorized by the ORP or designee.
    c. Devices must be wiped using approved software before being repurposed or disposed of.
    d. Record-level data must be deleted from portable devices after use and sanitized in accordance with ISPO and DAS policies.[12]

[12] https://www.oregon.gov/das/Surplus/Pages/Electronics-E-Waste.aspx. Specifically, the Media Protection and Disposal Policy (https://sharedsystems.dhsoha.state.or.us/DHSForms/Served/me090-011.pdf) and the Media Disposal Policy (https://sharedsystems.dhsoha.state.or.us/DHSForms/Served/me090-011-01.pdf)

e. Devices used outside of secure areas must use FIPS 197-compliant encryption. Decryption keys must not be stored on or with the device.

f. Data stored on portable devices must be limited to the minimum necessary for assigned tasks.

2. Electronic Transfer of Confidential Data

   a. Transfers not required for surveillance or case investigation must be pre-approved by the ORP or designee.

   b. Transfers from Orpheus using desktop computers at the Portland State Office Building occur over secure, high-speed lines behind an OHA/DHS firewall.

   c. FileMaker Pro® encrypts data transfers at the 128-bit level.

   d. AU privileges and password controls restrict access to record-level data.

   e. Whenever feasible, transfers should only occur in a secure surveillance area.

3. Long-Term Storage of Confidential Data

   a. Exported data must be stored only in ORP-approved locations (e.g., H:\Orpheus exports\).

   b. Servers or workstations storing confidential data must be physically and electronically secured.

   c. Data should be encrypted when not in use and during transfer.

C. Paper and Other Hard Copies

1. Any paper or hard copy containing PII must be locked in a secure drawer, container, or a file cabinet when not in use.
2. Confidential paper records must be shredded—preferably using a cross-cut shredder—when it is no longer needed.[13]

[13] All other physical media must be rendered unreadable, undecipherable, and otherwise cannot be reconstructed by using a minimum of cross-cut shredding.

3. When transporting paper records outside secure areas (e.g., for outbreak investigations), AUs must:
    a. Include only the minimum necessary identifying information.
    b. Use a cover sheet indicating the contents are confidential.
    c. De-identify or code documents when feasible.
    d. Obtain prior approval from the ORP or designee if transport extends overnight or beyond one workday.
    e. Return or shred documents immediately after use.

Definitions

Aggregated Data

Summarized data that do not include identifiers such as names, phone numbers, and home addresses. Aggregated data are presented as frequencies (e.g., number of cases of Salmonellosis) or rates (e.g., rate of Chlamydia cases per 100,000 people) rather than as individual-level records.

Approved Entity (AE)

An organization—such as a Local Public Health Authority (LPHA), Tribal jurisdiction, or other authorized body—approved by the State Overall Responsible Party (ORP) to access Orpheus and its linked databases.

Authorized User (AU)

An individual who has been approved by an ORP to access Orpheus and its linked databases.

Breach

Any unauthorized use, access, or disclosure of data, regardless of whether the data include personally identifying information (PII). A breach may result from human error, system failure, or malicious activity. All breaches must be reported, documented, and investigated

Case

As defined in Oregon Administrative Rule 333-017-0000, a "case" refers to a person who has been diagnosed with a specific reportable disease, infection, or condition by a healthcare provider, or who meets the defining criteria outlined in the Oregon Health Authority's Investigative Guidelines.

Overall Responsible Party (ORP)

An individual designated by an AE or OHA who is responsible for assuring that all AUs under their jurisdiction are compliant with Orpheus Policies and Procedures.

Personally identifiable information (PII)

Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other data. Examples include name, date of birth, Social Security Number, home address, and personal email. The definition of PHII is broad and context dependent.[14]

Protected Health Information (PHI)

Individually identifiable health information–oral, written, or electronic-- created or received by a healthcare provider, health plan, public health authority, or other covered entity. PHI relates to an individual's physical or mental health, healthcare services, or payment for healthcare. PHI does not include education or employment records.[15]

Record-level data

Data that pertain to individual record (e.g., person, case, laboratory, or contact records in Orpheus) and are not aggregated. These data are most likely to contain PII.

Surveillance data

Health-related information collected by public health authorities for the purpose of monitoring, investigating, and controlling diseases and conditions of public health importance.

[14] https://www.gsa.gov/directives-library/gsa-rules-of-behavior-for-handling-personally-identifiable-information-pii-2

[15] Oregon Administrative Rule 943-014-0000(32) (https://oregon.public.law/rules/oar_943-014-0000)

Addendum – Disaster Recovery and Business Continuity

Nightly Backups

Orpheus FileMaker® servers follow a structured local backup schedule. Backups are written to disk on the server and retained according to the following schedule:[16]

- **Weekly backups**: 4 copies retained
- **Monthly backups** (every 30 days): 5 copies retained
- **Quarterly backups** (every 120 days): 3 copies retained
- **Annual backups** (every 365 days): 20 copies retained

In addition, Data Center Services (DCS) provides robust backup and disaster support. Within the State Data Center, DCS uses Commvault for local backups and system restoration, enabling rapid recovery and minimizing downtime.

To enhance redundancy, encrypted backups of the Orpheus database suite are securely transmitted and stored offsite in Bend, Oregon. This offsite storage ensures that data can be recovered even in the event of a major disaster affecting the primary site.

Recovery Point Objective (RPO)

The maximum acceptable amount of data loss is 60 minutes. In the event of a disruption, up to one hour of data may need to be re-entered, re-processed, or re-collected.

Recovery Time Objective (RTO)

The maximum allowable time between an unexpected failure or disaster and the resumption of normal operations is three (3) business days.

[16] Details provided by Stephen Lofamia, Sr. DBA & Team Lead, Technology Platform via email on July 31, 2025.

Technical Support and Response Time

The Orpheus Technical Team (Orpheus.ODPE-Tech@odhsoha.oregon.gov) is available Monday through Friday, 08:00 to 17:00 (Pacific Time). This team is responsible for:

1. Managing access requests.
2. Communicating outages, downtime, and uptime.
3. Reporting and investigating bugs.
4. Documenting feature requests.

Outages and Maintenance

1. Orpheus is taken offline every other Wednesday from 17:30 to 18:30 (Pacific Time) for scheduled interface replacements.
2. System changes are documented in the Release Notes following each update.
3. Larger outages or infrastructure maintenance are scheduled outside of business hours and communicated in advance whenever possible.

Revision History

Version 1 – January 5, 2010

- Initial release of the Orpheus Security Policies and Procedures.

Version 1.1 – March 15, 2010

- Removed language about collaboration with DHS, CDC, and local health authorities.
- Clarified what counts as a breach of security protocol.
- Added rules for exporting and storing data, sharing data across jurisdictions, and accessing case and person records.
- Introduced guidelines for releasing aggregate data.
- Increased screen lock timeout from 5 to 10 minutes.

Version 1.2 – July 15, 2010

- Added rule that the State ORP cannot revoke a local user's access without LPHA request or notice.
- Clarified that surveillance data is jointly owned by the LPHA and CPHP.
- Replaced "DHS" with "OHA" throughout the document.
- Introduced Case Log and Audit Log to track data changes.
- Added a process for resolving disagreements about case data.

Version 1.3 – September 3, 2010

- Added "Hospitalized" and "Associated with an Outbreak" as fields that trigger notifications when updated.

Version 1.4 – October 26, 2010

- Increased screen lock timeout from 10 to 15 minutes.
- Required shredding of paper records using a cross-cut shredder, if feasible.

Version 2 – December 12, 2010

- Allowed LPHAs to adopt stricter local security policies.
- Required breach reporting within one working day.
- Added disciplinary consequences for staff responsible for breaches.
- Added Pertussis and CIN to the list of disease groups.
- Clarified the review process for publications involving confidential data.
- Required LPHA ORPs to notify the State ORP within 14 days when a user leaves.

Version 2.1 – April 13, 2011

- Added “County/counties of jurisdiction” to the ORP signature block.

Version 2.2 – July 7, 2011

- Added Syphilis to the list of disease groups.

Version 2.3 – May 29, 2012

- Added LTBI (Latent Tuberculosis Infection) to the list of disease groups.

Version 2.4 – July 17, 2012

- Replaced all references to “ODPE” with “CPHP.”

Version 2.5 – December 27, 2012

- Added a confidentiality statement to the Overview referencing ORS 433.008(1)(a).

Version 3 – December 24, 2013

- Moved the Revision History to the end of the document.
- Created a Definitions section.
- Removed the requirement to keep hard copies; electronic copies are now acceptable.
- Added disease groups: CJD, ABC, Lead, and MDRO.
- Discontinued use of FMDataGuard; clarified that not all record changes are logged.
- Added guidance for handling paper records.

- Clarified expectations for annual security audits and secure data export locations.

Version 3.1 – April 23, 2014

- Made minor corrections and clarifications to the Data Access and Use section.

Version 3.2 – June 2, 2015

- Reorganized and renumbered sections for clarity.
- Clarified policies on cross-jurisdictional data sharing and data storage.

Version 3.3 – June 23, 2015

- Made minor grammar and language updates.

Version 3.4 – August 15, 2015

- Continued grammar and language updates.
- Clarified ORP responsibilities and updated section numbering.
- Added Environmental Exposures (Env Exp) as a disease group.
- Added language about case status and access to cases outside a user's jurisdiction in specific situations.
- Clarified that aggregate data is accessible to all authorized users.

Version 4 – December 7, 2017

- Clarified the roles and responsibilities of ORPs.
- Updated the dispute resolution process and data access rules.
- Made minor text edits throughout the document.
- Updated the ORP signature page.

Version 4.1 – December 4, 2018

- Replaced "user" with "authorized user."
- Replaced "LPHA" with "Authorized Entity (AE)" throughout.
- Made minor text edits for clarity.
- Clarified user roles and privilege sets.

- Simplified language about transferring cases between jurisdictions.
- Clarified authorized uses and disclosures, including public records requests.

Version 5 – July 4, 2020

- Removed all references to Citrix based on ISPO recommendations.
- Added new disease groups: Emerging, HAI (Healthcare-Associated Infections), and Opera (COVID-19).

Version 5.1 – August 10, 2021

- Added Opera-specific Citrix access groups in addition to Orpheus groups.

Version 5.2 – July 21, 2022

- Added Orthopox to the list of disease groups.
- Updated the Disaster Recovery Addendum.

Version 6 – September 24, 2025

- Reformatted the document using the OHA publication template.
- Added footnotes and hyperlinks to legal references, policies, and tools.
- Created a new Revision History section.
- Added Appendix A – Reporting Small Numbers.
- Rewrote sections using plain language to improve accessibility.
- Replaced “CPHP ORP” and “state ORP” with “OHA ORP.”
- Clarified the roles of OHA ORPs, AE ORPs, and Authorized Users (AUs).
- Updated references from two-factor to multi-factor authentication (e.g., YubiKey, Microsoft Authenticator).
- Replaced manual access and deactivation processes with the Orpheus Oath tool.
- Removed names of linked databases (e.g., Shotgun, Shiver, Napoli, Opera).
- Removed detailed workstation security procedures (now covered in annual training).

- Updated data export and storage policies to emphasize minimizing exported data and secure deletion.
- Most disease groups are now accessible statewide, except: HIV, HSSS, RESP-NET, ABCs, and CIN.
- Removed references to deprecated Citrix access groups.
- Simplified cross-jurisdictional sharing expectations.
- Clarified guidance on device encryption and data export locations.
- Simplified the definition of “breach” and removed illustrative examples.
- Removed the requirement to access data only at secure facilities; replaced with guidance on minimizing exported data.
- Updated Disaster Recovery and Business Continuity expectations.

Appendix A – Reporting Small Numbers

This appendix provides guidance to help Orpheus users minimize the risk of disclosing personally identifying information (PII) when reporting data. These recommendations are based on the Oregon Public Health Division's *Guidelines for Reporting Small Numbers to Protect Confidentiality* (Version 2).[1]

Background

All Orpheus users have a responsibility to protect private information about individuals from disclosure when reporting data. Even when data are aggregated and do not include direct identifiers (e.g., name, date of birth, address), there is still a risk of re-identification--especially when the underlying population is small. The risk increases when data are stratified by detailed demographic characteristics such as race, ethnicity, or geography.

When data are used internally by authorized Orpheus users and reported only within their jurisdiction, discretion may be used to report small-numbers data without applying suppression or aggregation. However, caution is advised, as small numbers also produce unstable rates.

General Guidance

- These recommendations are the **minimum standard** necessary to protect confidentiality.
- A **denominator of fewer than 50** is the threshold for identifying sensitive cells.
- Represent small cell counts between 1 and 5 as **"1-5"**
- Do **not report events with 100% rates**.
- **Aggregate first**, then suppress sensitive cells if needed.
- Apply **complementary cell suppression** to prevent back-calculation.

[1] Available at https://www.oregon.gov/cd-informatics

Denominator Evaluation

The size of the denominator is a key factor in determining disclosure risk. If a data point applies to 100% of the underlying population, it may allow identification of individuals. The Oregon Public Health Division recommends a **minimum denominator of 50**.[2]

Aggregation Strategies

Aggregation reduces disclosure risk but may also reduce data utility. To reduce disclosure risk, aggregate data by:

- **Time**: Group by week, month, quarter, year, or multi-year periods.
- **Geography**: Combine small geographic units (e.g., Census Blocks into Census Tracts, or ZIP codes into county).
- **Age**: Use broad age groups (e.g., 10-year intervals).
- **Category**: Collapse detailed race, ethnicity, or other stratified groups into broader or more general categories.

Cell Suppression

When aggregation is not sufficient, suppression sensitive cells. A sensitive cell is one that, if reported, could pose a significant risk of re-identification. Use a symbol (e.g., "*") or a binned value (e.g., "1-5") to indicate suppression. Always use a footnote explaining why the data were withheld. Suppression may be based on:

- Small **cell counts**
- Small **denominators**
- **100% rates**

[2] These recommendations fall under the "Expert Determination" method section found https://www.hhs.gov/hipaa/for-professionals/special-topics/de-identification/index.html

Complementary Cell Suppression

To prevent back-calculation of suppressed values, additional cells—called **complementary cells**—must also be suppressed. This prevents users from inferring suppressed values by subtracting known values form totals. Choose complementary cells that are less analytically important (e.g., "Unknown") to minimize data loss.

Examples of When to Apply Suppression

- **MMWR weeks** that span multiple months or years
- **Overlapping multi-year averages** (e.g., 2020–2022 and 2021–2023)
- **Non-hierarchical geographies** (e.g., ZIP code and county)
- **Highly stratified demographic groups** (e.g., REALD) with small populations

Examples of Reporting with Small Numbers

1. **Tables**: In the example below, the threshold cell (population fewer than 50) is filled blue. The associated count and crude rate are sensitive cells, filled orange.

Before Cell Suppression				
Subset	**Rate per 1,000**	**95% CI**	**Count**	**Pop**
Age 0-17	65	(40 to 100)	20	306
Age 18-34	128	(13 to 240)	6	47
Age 35-64	58	(21 to 126)	6	103
Age 65+	19	(15 to 24)	77	3,992

Partial Cell Suppression				
Subset	**Rate per 1,000**	**95% CI**	**Count**	**Pop**
Age 0-17	65	(40 to 100)	20	306
Age 18-34	*	(13 to 240)	*	47
Age 35-64	58	(21 to 126)	6	103
Age 65+	19	(15 to 24)	77	3,992

* Data not reported to protect confidentiality

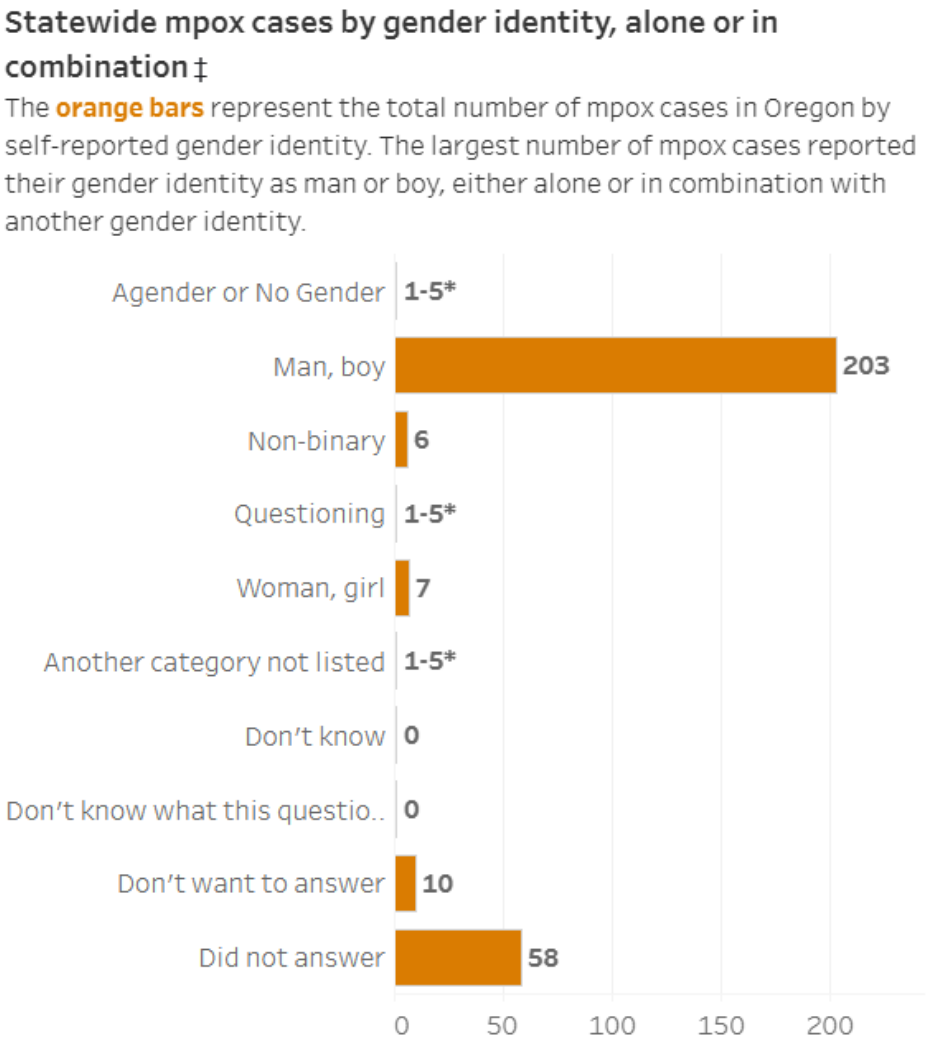
Full Cell Suppression				
Subset	**Rate per 1,000**	**95% CI**	**Count**	**Pop**
Age 0-17	65	(40 to 100)	20	306
Age 18-34	*	*	*	*
Age 35-64	58	(21 to 126)	6	103
Age 65+	19	(15 to 24)	77	3,992

* Data not reported to protect confidentiality

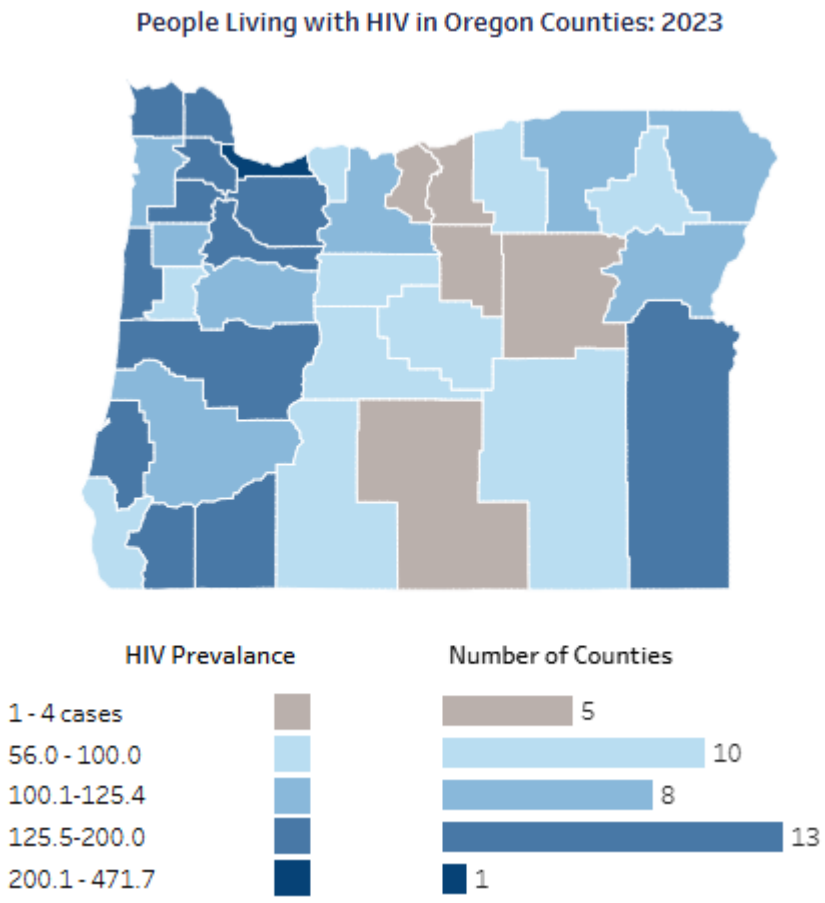
Complementary Suppression				
Subset	**Rate per 1,000**	**95% CI**	**Count**	**Pop**
Age 0-17	65	(40 to 100)	20	306
Age 18-34	*	*	*	47
Age 35-64	58	(21 to 126)	6	103
Age 65+	19	(15 to 24)	77	3,992
Unknown			*	
All Ages	**25**	**(21 to 27)**	**113**	**4,448**

* Data not reported to protect confidentiality

2. **Charts**: In the chart below, case counts of five or less are suppressed and published as "1-5". Case counts of greater than five are published as the number. Demographic categories with no cases are published as zero.



3. **Maps**: Use caution when presenting data in interactive GIS platforms. Users should not be able to zoom in to the address level. If the size of the underlying population is unknown, it should be assumed to be fewer than 50.



Summary Recommendations

1. Use these recommendations as the **minimum standard** necessary to protect confidentiality.

   Programs that collect or manage data may choose to apply more stringent standards for data release. Conversely, exceptions may be made when there is compelling public health interest.

2. A **denominator of fewer than 50** is the threshold for identifying sensitive cells.

   The size of the underlying population is the primary factor determining the risk of disclosure. If the denominator is smaller than 50, consider the cell count sensitive.

3. Represent small cell counts between 1 and 5 as "**1-5**."

   Small cell counts between one and five are also considered sensitive for REALD & SOGI data due to the specificity of the categories.

4. Do **not report events with 100% rates**.

   Although rates of 100% are rare, they represent a high risk of breaching confidentiality. Note that 0% rates may or may not pose the same risk, depending on whether the inverse represents a confidential characteristic.

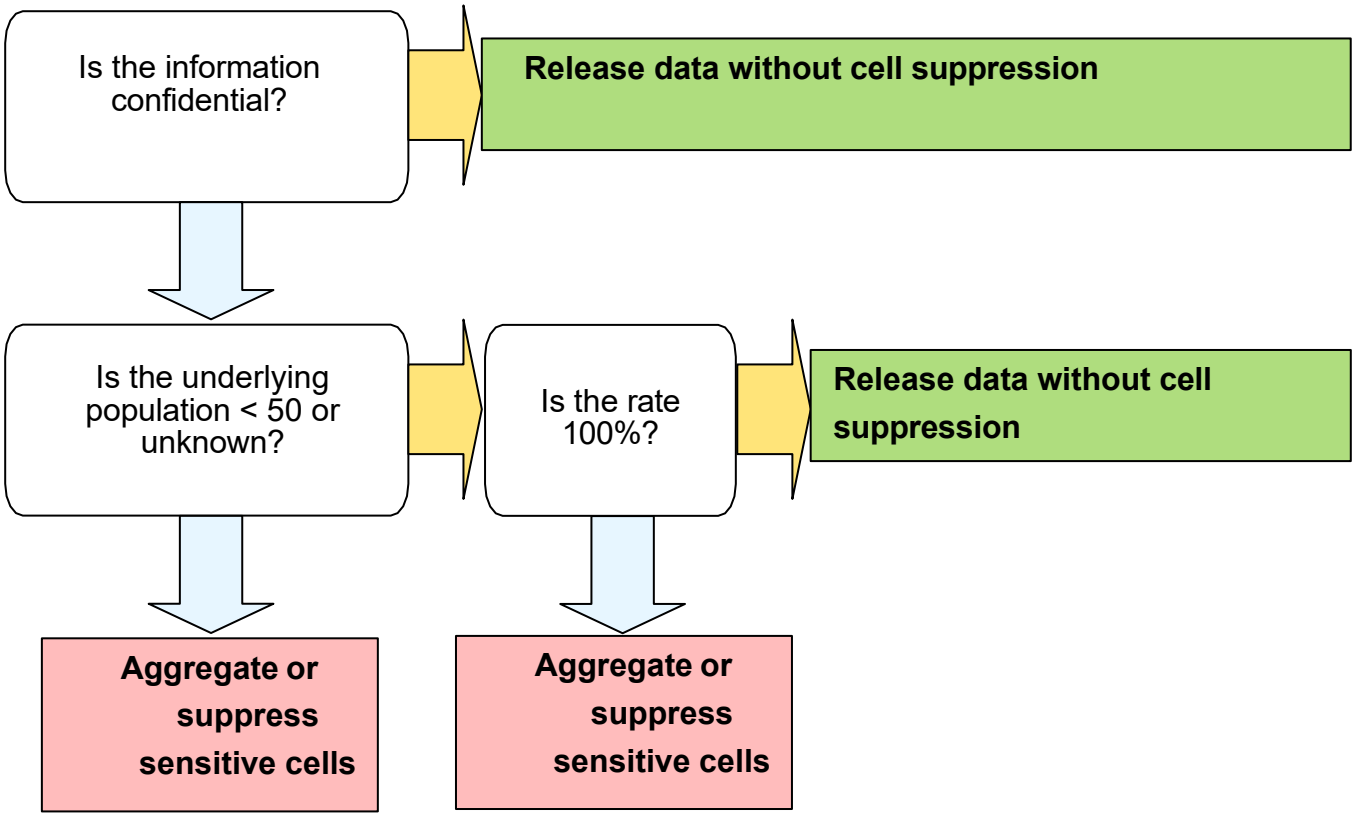
5. **Aggregate first**, then suppress sensitive cells if needed.

   If the size of the cells is still too small or the denominator is still below the threshold, withhold it from published tables.

6. Apply **complementary cell suppression** to prevent back-calculation.

   Be aware that data users may attempt to link published data with other sources to back-calculate suppressed values.

Data Release Decision Tree



You can obtain this document in other languages, large print, braille or a format you prefer free of charge. Contact the Orpheus Tech Team at orpheus.odpe-tech@odhsoha.oregon.gov or 971-673-1111. We accept all relay calls.

Public Health Division
Center for Public Health Practice
800 NE Oregon St., Suite 772
Portland, OR 97232
Orpheus.ODPE-Tech@odhsoha.oregon.gov
http://healthoregon.org/orpheus