Oregon Public Health Epi User System (Orpheus)
Security Policies and Procedures

Oregon Health Authority
Center for Public Health Practice

Overview

Information obtained by the Oregon Health Authority (OHA) or a local public health administrator in the course of an investigation of a reportable disease or disease outbreak is confidential (ORS 433.008 §1.a; available at: https://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors433.html. Public health surveillance data must be handled properly to prevent inappropriate disclosure and maintain confidentiality. This document prescribes policies and procedures by which public health employees in Oregon safeguard the confidentiality of public health data collected by public health professionals and maintained by Local Public Health Authorities, the Center for Public Health Practice and the Oregon Department of Administrative Services/Oregon Health Authority Enterprise Technology Services (ETS). It contains security and confidentiality standards, expectations, practices, and corrective procedures.

These policies align wherever possible with requirements, recommendations, and practices contained in the Centers for Disease Control and Prevention's (CDC) *Data Security and Confidentiality Guidelines* (Atlanta, GA; 2011. Available at http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf.

The Oregon Public Health Epidemiology User System (Orpheus) application and data are stored on secure State of Oregon servers in Salem, Oregon and are accessed remotely via secure Citrix® portal. Orpheus is a comprehensive case reporting database developed by the Center for Public Health Practice (CPHP), Public Health Division, Oregon Health Authority (OHA). All surveillance data contained within Orpheus are owned jointly by the Local Public Health Authority (LPHA) of the county of residence of a case and CPHP.

Orpheus, designed for public health use, is a public health surveillance application intended for state and local public health officials to investigate, analyze, and report on cases of reportable diseases among Oregon residents for the overarching purpose of reducing morbidity and mortality.

Orpheus is also linked to "Outbreaks," "Case Log," "Napoli," "Shotgun" and "Shiver"—other disease surveillance databases that house confidential, personally identifiable information (PII) related to communicable disease control. This policy also pertains to users who access these databases.

Policies

1) WRITTEN POLICIES AND PROCEDURES

A. Operating policies and procedures for securing Orpheus data are specified in this document.

B. A master copy of this document shall be kept up-to-date and stored on OHA's website: http://public.health.oregon.gov/DiseasesConditions/CommunicableDisease/ReportingCommunicableDisease/Documents/Orpheus/OrpheusSecurity/SurvPoliciesPro_Orpheus.pdf.

C. At least one up-to-date copy of this document shall be kept by the Orpheus ORP and each LPHA ORP.

2) OVERALL RESPONSIBLE PARTY

A. The Overall Responsible Party (ORP) for the security of Orpheus data is the Center for Public Health Practice Administrator, (Collette Young, PhD) in the Oregon Public Health Division. The state ORP or designee shall:
   1. Authorize access for each state-level staff person or affiliate newly requesting access to record-level Orpheus data.
   2. Authorize the assignment of all Orpheus users to one of three roles, or 'privilege sets,' within Orpheus (Full Access User, State Data Entry User, Power User (i.e., Higher-level user), Outbreak Only User, Script Learner, All Records, All Records & Scripts, or County Data Entry User. See Section 5.A.1.) that constrain the user's ability to enter and edit data and revise, make design changes to Orpheus, and revise the roles or privileges of other authorized users.
   3. Conduct an annual review of security practices in consultation with OHA Information Security Office (ISO) to include:
      a. Review of evolving technology to ensure that data remain secure and that policies are consistent with the technology in use; and
      b. A written report of the annual review of security practices to accompany certification of compliance with CDC Program Requirements.
   4. Keep a current list of authorized CPHP users and roles and retain the current copy the of signed confidentiality statement for each authorized user.
   5. Annually review these policies and procedures with all active CPHP Orpheus users and answer any questions those employees might have about these policies and procedures.
   6. Deactivate users or ORPs who fail to read, sign, and return to CPHP their agreements to the following within two months of receipt of user-specific annual security audits:
      a. Orpheus Security Policies and Procedures (this document).
      b. User-specific Security Audit produced by CPHP, which includes:
         i. user's secure data export location(s);
         ii. user's county and disease-group settings;
         iii. user's OHA-specific security and confidentiality policies, i.e., the

090 and 100 series found at http://www.oregon.gov/oha/OIS/ispo/Pages/policies.aspx.

c. User-specific Orpheus Confidentiality Statement (User Oath).

7. Ensure that State of Oregon information technology staff and others who might have incidental access or exposure to Orpheus data, including any persons with access to servers, workstations, or backup devices adhere in substance to this policy.
8. Ensure that all state Orpheus users assume responsibility for:
    a. fully implementing OHA's data security policies and procedures;
    b. safeguarding the security of any OHA device in their possession on which personally identifiable information (PII) from Orpheus is stored;
    c. reporting suspected security breaches.

    Steps users can take to fufill these responsibilities include but are not limited to:
    i. protecting keys, passwords, and codes that would facilitate unauthorized access to PII; and
    ii. exercising reasonable judgement in the use of technology to avoid infecting OHA computer systems with viruses and other malware; and
    iii. limiting use of personal computers and storage devices to activities directly related to CPHP work in a manner consistent with all OHA and CDPH work and with common sense; and
    iv. limiting removal of data from secure facilities to circumstances that have been explicitly approved by a supervisor, ORP, or a designee and are otherwise consistent with this policy and with OHA policy.
    v. protecting mobile devices and storage media from loss and theft; and
    vi. obtaining authorization prior to removal of data from secure facilities.
9. Ensure the completion of periodic random audits of user logs, investigation of any irregular use patterns, and maintenance records of the outcomes of these audits.
10. Ensure that any PII sent from Orpheus in an e-mail is sent using the encryption standard of the department, i.e., using "#secure#" in the subject line.
11. Ensure that 2-factor authentication tokens are distributed to validated Orpheus users.
12. Send proof of annual review to independent OHA reviewer, e.g., the Performance Management Program.

B. Each Local Public Health Authority (LPHA) shall appoint an ORP for the security of Orpheus data within its agency. The LPHA ORP or their designee shall:
    1. Authorize access for each LPHA-level staff person or affiliate newly requesting access within their jurisdiction to record-level Orpheus data.
    2. Ensure that their agency complies with the requirements of this document, including all future updates.
    3. Keep a current list of authorized Orpheus users and roles in their jurisdiction and retain a current copy of the signed confidentiality statement for each authorized user.
    4. Certify LPHA adherence to the security policies and procedures in this document upon request of CPHP ORP.
    5. Annually review these policies and procedures with all active LPHA Orpheus users and answer any questions those employees might have about these policies

and procedures.

6. Direct the state ORP or designee to de-activate users or ORPs who fail to read, sign, and return to CPHP their agreements to the following within two months of receipt of user-specific annual security audits:
    a. Orpheus Security Policies and Procedures (this document);
    b. User-specific Security Audit produced by CPHP, which includes;
        i. User's secure data export location(s);
        ii. User's county and disease-group privileges; and
        iii. User's jurisdiction-specific security and confidentiality policies.
    c. User-specific Orpheus Confidentiality Statement (User Oath).
7. Exercise their right to implement local security policies that are more stringent than these statewide Orpheus security policies and procedures.
8. Ensuring that all Orpheus users take responsibility for
    a. fully implementing local data security policy and procedures;
    b. safeguarding the security of any device in their possession on which personally identifiable information (PII) from Orpheus is stored;
    c. reporting suspected security breaches.

    Steps users can take to fufill these responsibilities include but are not limited to:
    a. protecting keys, passwords, and codes that could facilitate unauthorized access to PII; and
    b. exercising reasonable judgement in the use of technology to avoid infecting LPHA computer systems with viruses and other malware; and
    c. limiting use of personal computers and storage devices to activities directly related to LPHA work in a manner consistent with all LPHA work and with common sense; and
    d. limiting removal of data from secure facilities to circumstances that have been explicitly approved by an LPHA supervisor, LPHA ORP or a LPHA ORP designee and are otherwise consistent with this policy and with LPHA policy.
    e. protecting mobile devices and storage from loss and theft; and
    f. obtaining authorization prior to removal from secure LPHA facilities.
9. Ensure that any PII sent from Orpheus in an e-mail is sent securely using the encryption standard of the LPHA.
10. Ensure that Orpheus Users (within their purview) meet at least annually with the ORP (or designee) to review their Orpheus Security Audit Report, including but not limited to, the current Orpheus Security Policies and Procedures document, their Assurance of Confidentiality (User Oath), their current user access privileges, their Orpheus data export location(s), and agency-specific security policies.
11. The LPHA ORP or designee must notify the Orpheus Tech Team (Orpheus.ODPE-Tech@state.or.us) within 14 days after an authorized user leaves their position.

3) STAFF RESPONSIBILITIES AND REQUIREMENTS

A. Each state and local public health professional authorized to access record-level Orpheus data shall be knowledgeable about and abide by the information security policies and procedures in this document.

B. Each person authorized by the ORP to access record-level information shall review these policies and sign a confidentiality oath (Appendix 1) before being granted access, and annually thereafter. Access to Orpheus will be denied to persons who fail to complete the initial or annual review and sign the confidentiality oath.
C. Each person authorized to access record-level Orpheus data assumes individual responsibility for challenging anyone who attempts unauthorized access to Orpheus data; and for reporting immediately any suspected security breaches to the ORP or designee, according to the OHA Privacy and Information Security Incident Response Policy (090 and 100 series found at http://www.oregon.gov/oha/OIS/ispo/Pages/policies.aspx.)
D. Each person authorized to access Orpheus data assumes individual responsibility for protecting from theft or unauthorized disclosure their own workstation, laptop, and other devices used to view or access Orpheus data. This responsibility includes protecting keys, passwords, codes, or tokens that would allow access to confidential information or data. Staff must take care to protect their workstations, laptops and other devices from computer viruses and other damage, such as that caused by extreme heat or cold.
E. Confidentiality training of non-surveillance staff, e.g., system administrators, must also include review of these policies and reporting suspected security breaches to the ORP in accordance with the OHA Privacy and Information Security Incident Response Policy (http://www.oregon.gov/oha/Admin/infosec/pages/incdnt_resp.aspx).
F. All authorized users will be subject to periodic random audits of Orpheus logs performed by authorized OHA staff. Irregular use patterns will be investigated. Users found responsible for breaches of security protocol or confidentiality may lose or suffer reduced access (e.g., constraining their privilege set) to confidential data and may face disciplinary action up to and including termination.

4) SECURITY BREACHES

A. Breaches of security protocol without breaches of confidentiality.
   1. Anyone who becomes aware of a breach of security protocol without breach of confidentiality shall report this to their LPHA ORP or designee, or to the CPHP ORP.
   2. ORP shall ensure that all reports are logged and investigated and oversee the maintenance of a breach log that includes date of breach, date breach was reported, description of breach, severity, person(s) investigating, conclusions, and disposition or corrective action prescribed.
   3. ORP or their designee will review the breach of security protocol log at least twice annually to look for recurring patterns and individual incidents that may require corrective action.

B. Breaches of confidentiality that result in improper disclosure of confidential data can occur inadvertently, through employee miscalculation, or intentionally, as in acts of sabotage.
   1. All must be reported within one working day to the CPHP ORP, who will be responsible for reporting to the OHA Information Security and Privacy Office

(ISPO) and to CDC.
2. Employee(s) responsible for any breach may face disciplinary action, up to and including termination of employment as determined by the employer.
3. In event of an intentional breach, the ORP should consult with appropriate legal counsel to determine whether reporting to law enforcement agencies is warranted.

5) DATA ACCESS AND USE

A. Public Health Users

Record-level access without special approval shall be restricted to public health users authorized by CPHP or LPHA ORP. Once an individual has read these policies and procedures and signed the confidentiality oath, the user returns the signed oath and the OHA remote access form to the Orpheus Team (Orpheus.ODPE-Tech@state.or.us or fax to 971-673-1100). Within a week the user will receive a Citrix ID number assigned by the Orpheus Tech Team, and obtain access to the Orpheus application from the Orpheus Team at OPHD. Orpheus has been designed such that users are restricted to specific actions that they can perform and records that they can view or edit. This is accomplished employing the tools of "privilege sets" and individual user settings available in the FileMaker® software. The LPHA, or state ORP, or designee authorizes the assignment of each user to one of several roles based on whether the user is a LPHA or state user, their level of authority within their organization, and their public health responsibilities. The State ORP or designee shall not revoke Orpheus access of an authorized LPHA user without prior notification of the LPHA ORP or designee. Program area and jurisdiction rights to a user will be assigned by one of the Orpheus Team members at OPHD based on the programs and jurisdictions approved by the State or LPHA ORP, as appropriate. ORPs are automatically notified of any changes to their users' access priviliges.

1. Roles (privilege sets):
   a. The Full Access role allows the user to view all records, manage privilege sets (including creating new accounts), edit data tables, create new fields, etc. Twenty-four users—mostly Orpheus Tech Team members and other administrators have full access; all are state-level users or MSN Media contractors.
   b. The State Data Entry role allows state users to enter and edit data, run individual-level reports on information other than cases and people such as laboratory results; most State users have this role.
   c. The County Data Entry role allows county users to enter and edit data about cases, providers and facilities, and run pre-formatted reports. All County users have this role.
   d. The Power User role allows higher level use and editing of graphics, release notes, tool tips, global fields, plugins, etc. Currently, no State users belong to this role.
   e. The Outbreak Only role is for managing the Outbreak database only. Only one State user has this role.
   f. The Script Learner role is for learning script writing; only one user has this privilege set.
   g. The All Records role is mainly for State STD workers to efficiently manage

case records within Orpheus—Only two State STD workers have this role.
h. Two State workers have the All Records+Scripts role..

2. User Settings
   a. The User Administrator Setting allows modification of security settings for other users including setting the counties of case or person residence and diseases for which users can see cases or person data. Presently, 21 users are designated as User Administrators, and all of these are state-level users.
   b. The County User setting restricts records that can be viewed and edited to records for persons or cases who are residents of a specific county or counties;
   c. Disease Group settings limit records that can be viewed by disease group. Currently available disease groups include:
      i. ABC (Active Bacterial Core surveillance);
      ii. Animal disease reports;
      iii. CIN (cervical intraepithelial neoplasia);
      iv. CJD (Creutzfeldt-Jakob Disease) and Other Prion Diseases;
      v. Enteric diseases;
      vi. Env Exp (Environmental Exposures, e.g., cadmium);
      vii. Hepatitis;
      viii. HIV;
      ix. Lead;
      x. LTBI (Latent TB Infection);
      xi. MDRO (Multi-Drug Resistance Organisms);
      xii. Miscellaneous communicable diseases;
      xiii. Pertussis;
      xiv. STD (Gonorrhea & Chlamydia);
      xv. Syphilis;
      xvi. TB (Tuberculosis);
      xvii. Vaccine Preventable diseases; and
      xviii. Vector-borne diseases.
   d. A separate user setting allows a user to view HIV cases. This setting can be set by any User Administrator. To view HIV cases, the user must be granted the HIV disease group setting in addition to the separate HIV User setting.

3. Exporting data from Orpheus for analysis, or short- or long-term storage.
   a. Every user shall annually identify ORP-approved location(s) for storing all PII-containing data exported from Orpheus.
   b. Locations that ORPs should consider approving include those that are found on restricted access public health agency networks behind agency firewalls, or password-protected local hard drives or other media on which data are automatically encrypted when not in use.
   c. Users who are unsure of appropriate storage locations should consult with their supervisor.
   d. If a user wishes to store or transfer data in a location not already approved, they must obtain prior approval from ORP or designee.
4. Data storage, access and transfer of data shall be consistent with all related policies herein. (6.A.– C.)
5. Cross-jurisdictional sharing

a. Orpheus is designed with both person- and case-centric functionality. Most permanent attributes of a unique individual are recorded within a single "person record" in Orpheus. Ideally, Orpheus contains only one person record for each unique individual recorded. Records for a particular instance of a case of a reportable disease ("case records") contain attributes specific to that instance of a specific disease for a unique person. All case records relate to one and only one person record. Each person record may have zero, one, or multiple related case records of reportable disease.
b. Access to Orpheus case records will be considered according to two attributes of each record: disease group, and county of residence.
c. The LPHA ORP or designee authorizes, delimits, supervises, and renews case record access for local users.
d. State ORP or designee authorizes, delimits, supervises, and renews case-record access for all state users.
e. Local users may be granted case-record access to one or more disease groups by the local ORP or designee. The local ORP shall limit case-record access to those disease groups necessary for the user to complete their public health responsibilities.
f. Local users are further restricted by the Orpheus software to accessing case records for which case residence at diagnosis is within the jurisdiction in which they work except for certain diseases and circumstances listed below.
g. State users may be granted case-record access to one or more disease groups by the state ORP or designee. The state ORP shall limit case-record access to those disease groups necessary for the user to complete their public health responsibilities.
h. State users are permitted by the Orpheus software to access case records for all jurisdictions within disease groups to which they have been granted access.
i. When the State ORP determines that the public health benefit of case-record access for a specific disease group across jurisdictions exceeds the risk of loss of confidentiality, the State ORP may allow access to case records for that disease across jurisdiction by all state and local users. (An example of such a disease might be Hepatitis C.) Or, the State ORP may authorize Orpheus programmers to systematically grant a local user who creates a new case report for a disease to view all existing cases for that person within the same disease group regardless of residence at onset. (An example of such a disease might be syphilis, where determination that a new case has occurred often requires review of laboratory and historical information related to previous cases. In that example, if a local user is in receipt of information such as a laboratory test result that suggests a new case but does not offer sufficient information to define a confirmed or probable case, the user might create a new case and categorize it as "under-investigation," or "suspect." Then, any other previous cases of syphilis recorded by local health authorities in other counties would become visible to the local user. The local user then could revise the category of the case from "Under investigation" or "Suspect" to "No case" or to "Presumptive" or "Confirmed" based on the additional information, and all syphilis cases for that person would remain visible to the local user even if the permanent status of the local case is changed to "No case."

j. When two or more local jurisdictions need to collaborate on a case investigation or treatment, a user from the county of residence at diagnosis of the case with access to the disease group in which the case falls can grant access to that case record to all users from collaborating jurisdictions who already have access to the same disease group within their own jurisdiction. (An example of a circumstance where this might become necessary would be when a tuberculosis case-patient moves to another county before completion of therapy, also known as a "transfer.")
k. All state and local users authorized to access case records are permitted by the Orpheus software to access all person records (as distinguished from case records) contained in Orpheus regardless of location of residence. This is necessary to avoid creation of duplicate person records when a person record has already been created in Orpheus for an individual upon the occurrence of a reported disease when that person was a resident of another local jurisdiction. Orpheus reveals neither the occurrence of the disease nor details of the case via the person record to users without privileges to access that disease group, or if the person resided in another jurisdiction at the time of diagnosis.
l. Any LPHA may elect to share all of its cases with any other LPHA upon written request to the Orpheus State ORP from both LPHAs (Appendix 2, Cross-jurisdictional agreement). However, access to cases of specific diseases by users of the cooperating LPHAs still requires that the individual user have been granted access to the specific disease group.
m. Sometimes a local user will be in receipt of a report of a case or suspect case of a reportable disease and discover that the person with the suspected case has already been recorded in Orpheus. Sometimes, the case to which this report refers will not be visible if the case was initially investigated in another jurisdiction. Before entering a new case for the person, local public health staff should contact the Public Health Division to determine whether the case has already been entered by another LPHA. If the case has already been entered, state or local staff should contact the investigating LPHA and ask that the case be made visible ("transferred") to the new LPHA. Subsequently, the case will be visible to both LPHA's.

6. Changes to data.

   Changes to key Orpheus data are automatically captured in the Orpheus Log file; all Orpheus users have access to view the Orpheus Log file (*More* Tab|*Log*) . Record modifications are logged with the name and user number of the user who makes the modification, the time and date of the modification, and the specific change made. Whenever a record is viewed by a user who does not make a modification to the record, this event is also recorded in the log. In addition, Orpheus users are automatically notified within Orpheus when the following fields are changed to cases for which they have been assigned primary state or local responsibility: *Case Status* (includes deletion of cases or assignment of "no case" status when a suspect case has been "ruled out;" *Deceased* (i.e., a case person is designated as having died), *Disease*, *Hospitalized, Associated with an Outbreak*, and *County* (includes County of contacts of cases). Any authorized user may suggest additions or revisions to the list of "notifiable" changes. Any non-controversial revisions or additions

to the list shall be made by OHA. Decisions on disputed or controversial revisions or additions to the list shall be made by the State ORP after considering opinions expressed.

7. Resolution of Disputes about person and case attributes and other Orpheus field values.

   If LPHA and CPHP disagree on data entered on specific cases, especially as new information comes to light during the course of an investigation, the parties to the dispute will meet informally and attempt to come to agreement on the data of record to be retained within Orpheus. If an agreement is not reached by the parties to the dispute, the LPHA ORP or designee (such as the Health Officer) for the county where the case-patient resides at time of diagnosis will work with the OHA ORP or designee to come to a resolution, with the understanding that the LPHA representative opinion shall be given substantial weight; however, to ensure consistency of case definitions across Oregon counties, the OHA ORP retains the final authority to determine case Status (confirmed, probable, suspect, or non-case).

B. Record-level access—all others. The following are consistent with ORS 433.008 (http://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors433.html).

1. For public health or human subjects research purposes.
   a. Requests by others for access to, use of or copies of record-level data for public health or human research purposes must be in writing and based on a public health need, the expected benefit of which exceeds the risk of inappropriate disclosure of confidential information as determined by the respective ORP or their designee.
   b. Requests for record-level data containing information about episodes of diseases or related events stored within Orpheus involving residents of a single LPHA may be approved by Orpheus ORP or by the LPHA ORP without review by the Orpheus ORP.
   c. Requests for record-level data containing information about episodes of diseases or related events stored within Orpheus involving residents of more than one LPHA shall be approved by the Orpheus ORP.
   d. Requests for data access or release of names or other identifying information must specifically address the need for personal identifiers.
   e. Projects must not reasonably affect the public perception of confidentiality of the surveillance system.
   f. If after review, the Orpheus ORP or LPHA ORP or designee is uncertain about whether all conditions for data access or release have been met, she may consult with other individuals or groups with relevant expertise. These might include legal counselors, institutional review boards, ethicists and public health directors. Within CPHP, a committee of public health managers, the Project Review Team (PRT), meets regularly to consider such topics. The OHA ISPO is another resource for this purpose. These resources shall also be available to a LPHA ORP seeking consultation on proposed data release.
   g. Data access or release for purposes defined as human subjects research by the investigator, the Orpheus ORP, the PRT,—or the LPHA ORP in the case of requests for data involving residents of a single LPHA—must be approved by

the Oregon Public Health Division's Institutional Review Board.

h. Requests for data access or release must include signed confidentiality statements that address rules of access and final disposition of the data.
i. Each investigator must sign a statement indicating that they understand the penalties for unauthorized disclosure, assures that the data will be stored in a secured area, and agrees to adhere to any commitments to sanitize hard drives or other storage devices that contained the data set when the project is completed.
j. Confidential information may not be re-disclosed to a third party not authorized to view the information by ORP approval.
k. Any publication or re-disclosure of summary data based on released confidential information must be consistent with the Oregon Public Health Division policy on release of aggregate or summary data (available from CPHP upon request) and reviewed by the LPHA ORP for publications involving residents of a single LPHA or the Orpheus State ORP or their designee for publications involving more than one LPHA prior to publication.
l. All data storage and transfer methods shall be entirely consistent with these policies and procedures.

2. Other purposes (e.g., litigation).
   For purposes other than public health or research, access to, use of, or copies of record-level Orpheus data shall be granted only to the extent required by law.

C. Aggregate-level access—everyone.
1. Any person may obtain summary or aggregate de-identified data upon request, as allowed under ORS 433.008 (http://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors433.html).
2. Release of aggregate data shall be compliant with the Oregon Public Health Division's *Guidelines for Reporting Small Numbers to Protect Confidentiality* https://inside.dhsoha.state.or.us/oha/public-health/science-a-research.html.
3. Authorized staff may provide aggregate data to anyone upon request without prior approval of ORP, provided the data release complies with all aggregate data release guidelines, available from CPHP upon request.
4. Authorized staff should consult with the LPHA or Orpheus State ORP if they are uncertain whether the requested release is compliant with program policy.

6) DATA SECURITY

A. Physical barriers
1. Unless otherwise necessary for surveillance, case investigation or other public health responsibilities, access to and use of record-level data shall be restricted to authorized users within limited-access, physically secure surveillance areas. If access to or use of record-level data should become necessary outside of locked and physically secure surveillance areas, the user shall take all necessary precautions to ensure that data are not visible or accessible to others not authorized to access these data. Such precautions might include using screen privacy filters, closing data files when they might be visible to others, viewing data only in physically isolated or private areas, and refraining from accessing

data in public settings. Regular or recurring access to data outside of limited-access, physically secure areas shall be approved by the ORP or their designee.

2. A limited-access, physically secure surveillance area shall be available and maintained by Orpheus users. This area must always be kept secure.
    a. Keys, codes or other entry control devices shall be provided only to those persons authorized by ORP.
    b. The ORP or designee shall maintain a current list of all persons authorized to enter the surveillance area unaccompanied.
    c. If feasible, keys, codes or other entry-control devices should be changed at least annually and upon cessation of employment of authorized staff.
    d. Unaccompanied access may be granted only to public health employees and building security staff.
    e. Access to any limited-access, physically secure surveillance area by unauthorized individuals may be granted only when authorized surveillance or IT personnel are available for escort or under conditions where the data are protected by security measures specified in a specific written policy that has been approved by the Orpheus ORP in the case of state-level surveillance areas or the LPHA ORP in the case of surveillance areas overseen at the LPHA level.
    f. Entry for cleaning by custodial staff should ideally occur during daytime when at least one authorized staff member is present; otherwise, all confidential materials must be stored in a locked location when cleaning staff are present.

B. Electronic data storage, access and transfer

1. The Orpheus application

    Orpheus is a FileMaker Pro® application; it is a relational database developed and maintained by CPHP. Orpheus houses public health data for all cases of reportable communicable disease in Oregon; it also houses data related to reportable blood lead levels, as well as reportable animal bite data. Orpheus contains a table with a record for each person connected with a communicable disease case investigation, including people who have been named as epidemiologic contacts to persons with a case of a reportable disease. These "person records" contain personal and demographic attributes of the person, including names and aliases, date of birth, sex, address, and contact information. Case details such as the identity of a reportable disease, treatment, laboratory results, exposures related to a particular disease and names and disposition of contacts are stored in related tables. All data transmitted between Orpheus and remote users are encrypted. (See below.)

    a. All authorized public health users shall have password-protected access to all person records within Orpheus for purposes of linking a new laboratory report or follow-up detail to a previously reported case of any communicable disease or for linking a new disease report to someone who has previously had a case of the same or another reportable disease.
    b. Authorized users external to Enterprise Technical Services (ETS) shall use two-factor authentication. All data are encrypted during transmission via secure socket layer (SSL).
    c. Access to Orpheus record-level data shall be password-protected and

restricted to those persons authorized to access or use specific program area data.

2. Storage or viewing of record-level surveillance data on laptop computers or other portable devices, or external storage devices.
   a. Unless explicitly authorized in advance by the Orpheus ORP or LPHA ORP or their designee, these devices should only be used within designated, limited-access, physically secure areas.
   b. Laptop computers, removable hard drives or external storage devices containing confidential data outside of designated limited access, physically secure areas shall be locked in a secure cabinet when not in use.
   c. DHS Office of Information Technology staff shall use ISPO-approved software, e.g., Acronis™, to re-image computers, ensuring that all data are wiped clean. Computers sent to surplus shall be physically destroyed by an ISPO-approved vendor, e.g, assuring that all data are inaccessible or destroyed in the process. Record-level data shall be deleted from laptop computers, removable hard drives, and other external storage devices after use, and storage media sanitized (i.e., made unreadable) using software, e.g., Acronis™, approved by Oregon OHA ISPO.
   d. Data stored on laptop computers, removable hard drives or external storage devices outside of designated limited-access, physically secure areas must be encrypted using real-time FIPS-197-compliant encryption. Decryption keys must not be stored on or with the laptop or other portable device.
   e. External storage devices and removable hard drives containing encrypted data must be stored separately from the computer when not in use.
   f. Unless explicitly authorized by the Orpheus ORP, LPHA ORP or their designee for completion of surveillance, case investigation and other public health responsibilities, record-level data shall not be stored on computer workstations unless the workstation is up-to-date with current patching, anti-virus and any other designated security software and also complies with local or state information policies and procedures on security of record-level data.
   g. Data stored on portable devices such as laptop computers, removable hard drives and external storage devices must include only the minimum amount of information necessary to accomplish assigned tasks as determined by the Orpheus ORP for DHS personnel or affiliates or the LPHA ORP for LPHA personnel or affiliates or their designees.

3. Electronic transfer and storage of confidential data for laboratory reporting and other public health-related transfer of record-level data.
   a. Electronic data transfers not ordinarily necessary for completion of surveillance, case investigation and other public health responsibilities must be approved in advance by an ORP or their designee.
   b. Transfer of record-level public health surveillance data to and from Orpheus by authorized users using desktop computers located within the Portland State Office Building occurs over private, high-speed transmission lines behind a OHA/DHS firewall. The FileMaker Pro® application automatically encrypts these data for transfer at the 128-bit level. User privileges and password controls built in to Orpheus restrict access to record-level data to authorized

users. Whenever feasible, transfer of record-level data should be limited to a limited-access, physically secure surveillance area.

c. Record-level public health surveillance data transfer to and from Orpheus by authorized public health users from outside of Portland State Office Building and users inside the building who lack the FileMaker Pro® application installed on their desktop computer occurs via an encrypted Citrix® connection with two-factor authentication using a password and a random number from a security token. User privileges and password controls built into Orpheus restrict access to record-level data to authorized users.
d. Indefinite storage of confidential surveillance data if necessary for public purposes.
    i. Storage of exported data, e.g., to H:\Orpheus exports\ must be approved by the State or LPHA ORP.
    ii. Computer servers or workstations storing confidential data must be physically and electronically protected in a manner completely consistent with these policies.
    iii. If feasible, data should be be encrypted using FIPS-197-compliant encryption when not in use and during transfer.

4. Other practices related to computer workstations, laptops and other electronic storage media used to store, view or analyze record-level data.
    a. Each device from which Orpheus data are accessed shall revert to screen-saver mode no more than 15 minutes after last activity, and require a password to resume activity.
    b. When leaving an area where case data are being stored, viewed or analyzed authorized users shall lock access to their computers regardless of how quickly they intend to return (using <Ctrl><Alt><Del>).
    c. Access to computer workstations, laptop computers or other portable storage devices used to transfer or store confidential surveillance data or information shall be controlled by unique user identification and passwords.
    d. When a staff member leaves the program, the program administrator will request that the Service Desk suspend access (log-in ability) to all workstations.

C. Paper and other hard copies of data originating from Orpheus

1. Any piece of paper or other hard copy containing names of cases or potential cases should be locked in a drawer, an overhead bin, or a file cabinet within a limited-access, physically secure surveillance area each night.
2. Any piece of paper or other hard copy containing confidential information must be shredded using a shredder with a cross-cutting feature if feasible after it is no longer needed.
3. Paper or other hard copies of identifying information that are removed or faxed from a limited-access, physically secure surveillance area must contain the minimum amount of identifying information necessary to complete the task. A cover letter stating that the data are confidential must be used.
4. When identifying information must be transported outside of a limited-access,

physically secure surveillance area for legitimate public health purposes such as case or outbreak investigations, paper and other hard copies must contain only the minimum amount of identifying information necessary for completing a given task and stored within the secure surveillance area or shredded upon task completion. Where feasible, any information that could be used to associate a person with a reportable disease should be coded or disguised. When a need to transport paper or hard copies of identifying information outside of a limited-access, physically secure surveillance area arises and is anticipated to last overnight or for more than a single workday, advance approval shall be obtained from the Orpheus or LPHA ORP.

Overall Responsible Party's Printed Name_____
Overall Responsible Party Signature _____
Date_____

ORP Designee Printed Name_____
ORP Designee Signature_____
Date_____

ORP Designee Printed Name _____
ORP Designee Signature _____
Date_____

Jurisdiction _____
Date_____

Definitions

Breach: A breach is an infraction or violation of a standard, obligation, or law. A breach in data security would include any unauthorized use of data, even data without names. A breach, in its broadest sense, may be caused by a natural disaster, a person, or an application/system and may be malicious in nature or purely unintended. An example of a malicious breach of confidentiality would be if staff intentionally, but without authorization, released patient names to the public. An example of an unintended breach of confidentiality would be if completed HIV/AIDS case reports were inadvertently mailed to and read by an unauthorized individual. A breach does not necessarily mean that sensitive information was released to the public or that any one person was harmed. A minor, inadvertent violation of local or ODPE security policies such as forgetting to lock a file drawer that policy requires be locked when not in use, constitutes a breach of security protocol as compared with a breach of confidentiality. Other examples of possible breaches of security protocol: 1) A hacker gains access to an internal machine via the Internet or a dial-up connection. 2) A trusted programmer introduces a program into the production environment that does not behave within expected limits. 3) A technician creates a backdoor into the operation of a system, even for positive and beneficial reasons, that alters the information protection provided. 4) After having been entered into a computerized file, confidential forms are left for removal in the standard paper waste process in an openly accessible location. Breach of confidentiality: A security infraction that results in the release of private information with or without harm to one or more individuals.

Case: Based on Oregon Administrative Rule 333-017-0000, "Case" means a person who has been diagnosed by a health care provider as having a particular disease, infection, or condition, or whose illness meets defining criteria published in the Authority's Investigative Guidelines.

Personally identifiable information (PII): The term “PII” refers to information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available—in any medium and from any source—that, when combined with other available information, could be used to identify an individual (http://www.gsa.gov/portal/content/104256).

Surveillance data: Case reports and other personal and health-related information collected by public health authorities in connection with investigation, control and monitoring of diseases and conditions of public health importance.

User: a person with a valid Orpheus account.

Appendix – Disaster Recovery

Nightly Backups - Enterprise Technology Services (ETS) uses commvault® software for nightly back-up (and restore, if necessary) processes; Secure, encrypted copies of Orpheus are stored off site by Montana's State Information Technology Services Office (http://itsd.mt.gov/default.mcpx, *personal communication, Brian Swick, ETS, July, 2013*). Furthermore, Orpheus leverages native FileMaker Pro® progressive backup processes throughout the day (every 30 minutes) to minimize loss of data. Additionally, the Orpheus FileMaker Pro® Server has the following back up schedule in place:

- Weekly - 5 copies retained. Starts 6/6/2015
- Monthly (30-day) - 6 copies retained. Starts 6/3/2015
- Quarterly (120-day) - 4 copies retained. Starts 6/3/2015
- Annual (365-day) - 20 copies retained. Starts 12/31/2015

Recovery Point Objective (RPO) – 30 minutes. Orpheus leverages FileMaker Server 12 technology and automatically conducts a progressive backup every 30 minutes.

Recovery Time Objective (RTO) - Our current recovery time objective, which is the maximum time allowed between unexpected failure or disaster and the resumption of normal operations, is 3 business days.