Oregon Public HealthEpidemiology User System (Orpheus) and Orpheus Linked Databases
Security Policies and Procedures

Oregon Health Authority
Public Health Division
Center for Public Health Practice

New language is highlighted in red.

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 (public health data) is confidential and not subject to public disclosure, and can only be disclosed in certain circumstances (ORS 433.008; available at: https://www.oregonlegislature.gov/bills_laws/ors/ors433.html). Public health data must be handled properly to prevent inappropriate disclosure and maintain confidentiality. These policies and procedures seek to ensure the security and confidentiality of public health data contained in the Oregon Public Health Epidemiology User System (Orpheus) operated and owned by the State of Oregon, Oregon Health Authority (OHA), and the databases linked to Orpheus.

These policies and procedures 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 Orpheus computer application and its data are on secure State of Oregon servers in Salem. Orpheus is a comprehensive case reporting database developed by the OHA, Oregon Public Health Division (OPHD), Center for Public Health Practice (CPHP). All surveillance data contained within Orpheus are owned by OHA.

Orpheus is intended for use by state, local and tribal public health officials to investigate, analyze, and report on disease outbreaks in Oregon and cases of reportable diseases among Oregon residents for the overarching purpose of reducing morbidity and mortality.

Orpheus is also linked to "Opera," "Outbreaks," "Case Log," "Napoli," "Shotgun" and "Shiver"—other disease surveillance databases that house confidential, personally identifiable information (PII) related to communicable disease control. These policies and procedures also pertain to authorized users (AUs) who access these linked databases.

Policies

1) WRITTEN POLICIES AND PROCEDURES

A. 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.

B. At least one up-to-date copy of this document shall be kept by the Orpheus overall responsible party (ORP) and each approved entity (AE), e.g, local public health authoritities (LPHA), Oregon Enterprise Technology Services (ETS), Tribal jurisdictions, etc.

2) STATE OVERALL RESPONSIBLE PARTY

A. The state ORP for the security of Orpheus data is the CPHP Administrator, 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 AUs to one of several roles, or 'privilege sets,' within Orpheus (All Records, County Data Entry, County Read-Only Analyst, Data Entry, Full Access, Read Only, State Data Entry, State Power, State Power STD. See Section 5.A.1.) that constrain the AU's ability to enter and edit data and revise, make design changes to Orpheus, and revise the roles or privileges of other AUs.
   3. Conduct an annual review of security practices in consultation with OHA Information Security and Privacy Office (ISPO) 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 AUs and roles and retain the current copy the of signed confidentiality statement for each AU.
   5. Annually review these policies and procedures with all active AUs and answer any questions those AUs might have about these policies and procedures.
   6. Deactivate AUs or AE ORPs who fail to read, sign, and return to CPHP their agreements to the following within two months of receipt of AU-specific annual security audits:
      a. Orpheus Security Policies and Procedures (this document).
      b. AU-specific Security Audit produced by CPHP, which includes:
         i. AU's secure data export location(s);
         ii. AU's county and disease-group settings;
         iii. AU'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. AU-specific Orpheus Confidentiality Statement (AU Oath).

7. In collaboration with ISPO, 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.
    a. Provide and maintain a list of all personnel at ETS or other co-located sites), with the ability to access Orpheus data, and the date of their most recent security or privacy training.
    b. Review at least annually with OIS, all users with privileged access (PA) to relevant servers.
8. Ensure that all state AUs assume responsibility for:
    a. fully implementing OHA's data security policies and procedures, including but 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 CPHP 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.
    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.

9. Ensure the completion of periodic random audits of AU logs, investigation of any irregular use patterns, and maintenance of 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 OHA, i.e., using "#secure#" in the subject line.
11. Ensure that 2-factor authentication tokens are distributed to validated AUs.

B. Each approved entity (AE) shall appoint an ORP for the security of Orpheus data within its agency. The AE ORP or their designee shall:
    1. Authorize access for each AE-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 AUs and roles in their jurisdiction and retain a current copy of the signed confidentiality statement for each AU.
    4. Certify AE adherence to the security policies and procedures in this document upon request of the state ORP.
    5. Annually review these policies and procedures with all active AE AUs within the

AE's jurisdiction and answer any questions those AUs might have about these policies and procedures.

6. Annually provide a list to the State ORP of AE IT personnel who have privileged access to Orpheus data and their most recent date of AE security and privacy training.
7. Request that the state ORP or designee de-activate AUs or ORPs who fail to sign and return to CPHP the following agreements within two months of receipt of a AU-specific annual security audit:
    a. AU acknowledgement of familiarity with Orpheus Security Policies and Procedures (this document);
    b. AU-specific Security Audit produced by CPHP, which includes;
        i. AU's secure data export location(s);
        ii. AU's county and disease-group privileges; and
        iii. AU's jurisdiction-specific security and confidentiality policies.
    c. AU-specific Orpheus Confidentiality Statement (AU Oath).
8. As the need arises, exercise their right to implement security policies that apply to AUs under its jurisdiction that are more stringent than these statewide Orpheus security policies and procedures.
9. Ensure that all AUs under the AE's jurisdiction 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 AUs 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 AE computer systems with viruses and other malware; and
    c. limiting use of personal computers and storage devices to activities directly related to AE work in a manner consistent with all AE work and with common sense; and
    d. limiting removal of data from secure facilities to circumstances that have been explicitly approved by an AE supervisor, AE ORP or a AE ORP designee and are otherwise consistent with this policy and with AE policy.
    e. protecting mobile devices and storage from loss and theft; and
    f. obtaining authorization prior to removal from secure AE facilities.
10. Ensure that any PII sent from Orpheus in an e-mail is sent in encrypted form, using the encryption standard of the AE.
11. Ensure that AUs within the AE's jurisdiction meet at least annually with the ORP (or designee) to review each AU's Orpheus Security Audit Report, including but not limited to, review of the current Orpheus Security Policies and Procedures document, Assurance of Confidentiality (AU Oath), current AU access privileges, Orpheus data export location(s), and agency-specific security policies.
12. The AE ORP or designee must notify the Orpheus Tech Team (Orpheus.ODPE-Tech@state.or.us) within seven days after an AU leaves their position.

3) AU RESPONSIBILITIES AND REQUIREMENTS

A. Each AU with access to record-level Orpheus data shall be knowledgeable about and

abide by the information security policies and procedures in this document.

1. Each AU 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.
2. Each AU 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.)
3. Each AU is individually responsibile 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.
4. Staff e.g., system administrators, who are not involved in public health data collection, case investigation or related activities, must also review these policies and procedures and other policies related to reporting suspected security breaches to the ORP in accordance with the OHA Privacy and Information Security Incident Response Policy (https://www.dhs.state.or.us/policy/admin/security/090_005.pdf.
5. All AUs will be subject to periodic random audits of Orpheus logs performed by other authorized OHA staff. Irregular use patterns will be investigated. AUs 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 AE ORP or designee, or to the state ORP, or to ISPO.
2. State ORP shall ensure that all reports are logged and investigated and shall 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. State 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 unlawful or improper disclosure of confidential data can occur inadvertently, through employee miscalculation, or intentionally, as in acts of sabotage.

1. All breaches that fall into one of the categories in B. above must be reported

within one working day to the state ORP, who will be responsible for reporting to 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 a suspected intentional breach, the state 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 AUs

Record-level access without special approval shall be restricted to AUs authorized by the state ORP or an AE ORP. Once the state ORP or an AE ORP has identified an individual that requires access to Orpheus, the individual must be provided with these policies and procedures and the individual must read these policies and procedures, sign the confidentiality oath, and return 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). The ORP must first submit an MSC 0786 via the Oregon's online system to obtain a "P-number" for their user, after which the ORP must submit the user Oath (Appendix 1) to the Orpheus Project Manager, which must include the P-number for their user. An AU's access to Orpheus is restricted by the "privilege set" that the state ORP or AE ORP has authorized for an AU based on the individual's role within their organization. "Privilege sets" and individual AU settings available in the FileMaker® software. The state ORP or AE ORP, or designees assign each AU to one or more roles based on whether the AU is a AE AU or a state AU, their level of authority within their organization, and their public health responsibilities. The state ORP or designee shall not revoke Orpheus access of an AE AU without prior notification to the AE ORP or designee. An AU's program area and jurisdiction rights are assigned by one of the Orpheus Team members at OPHD based on the programs and jurisdictions approved by the State or AE ORP, as appropriate. The state ORP or an AE ORP is automatically notified of any changes to its AU's access priviliges.

1. Roles (privilege sets):
   a. **Citrix – Orpheus**: Standard non-state user (access restricted by jurisdiction and disease group).
   b. **Citrix – Orpheus State**: Standard state user (access restricted by disease group)
   c. **Citrix – Orpheus All Data**: Enhanced state user (no restriction by disease group)
   d. **Citrix – Orpheus Super User:** Tech Team state user (enhanced system functionality)
   e. **Citrix – Opera**: Standard non-state user (access restricted by jurisdiction and disease group)
   f. **Citrix – Opera State**: Standard state user (access restricted by disease group)
   g. **Citrix – Opera Super User:** Tech Team state user (enhanced system functionality)
   h. **Citrix – DUDE**, an application launcher that automatically provides access to the appropriate outbreaks databases, such as Outbreaks, and Opera Outbreaks.

2. AU Settings
   a. The User Administrator Setting allows modification of security settings for

other AUs including setting the counties of case or person residence and diseases for which AUs can see cases or person data.

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. Emerging (e.g., vaping associated lung injury)
    vi. Enteric diseases;
    vii. Env Exp (Environmental Exposures, e.g., cadmium);
    viii. HAI (Healthcare Associated Infections, e.g., *C. difficile*)
    ix. Hepatitis;
    x. HIV;
    xi. Lead;
    xii. LTBI (Latent TB Infection);
    xiii. MDRO (Multi-Drug Resistance Organisms);
    xiv. Miscellaneous communicable diseases;
    xv. Opera (e.g., COVID-19 (spun off into new database on 7/9/2020)
    xvi. Pertussis;
    xvii. STD (Gonorrhea & Chlamydia);
    xviii. Syphilis;
    xix. TB (Tuberculosis);
    xx. Vaccine Preventable diseases; and
    xxi. Vector-borne diseases.
d. A separate AU setting allows an AU to view HIV cases. This setting can be set by any AU Administrator. To view HIV cases, the AU 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 AU shall annually identify an ORP-approved location(s) for storing all PII-containing data exported from Orpheus. All AUs shall identify a secure export location(s) on their Oath.
    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. AUs who are unsure of appropriate storage locations should consult with their supervisor.
    d. If an AU 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 AE ORP or designee authorizes, delimits, supervises, and renews case record access for local AUs.
d. State ORP or designee authorizes, delimits, supervises, and renews case-record access for all state AUs.
e. Non-State AUs may be granted case-record access to one or more disease groups by the local AE ORP or designee. The AE ORP shall limit case-record access to those disease groups necessary for the AU to complete their public health responsibilities.
f. Non-State AUs 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 AUs 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 AU to complete their public health responsibilities.
h. State AUs 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 AUs. (An example of such a disease might be Hepatitis C.) Or, the state ORP may authorize Orpheus programmers to systematically grant a local AU 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 AU 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 AU 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 AU. The local AU 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 AU 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, an AU 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 AUs 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 AUs 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 AUs without privileges to access that disease group, or if the person resided in another jurisdiction at the time of diagnosis.

l. Any AE may request to share all of its cases with any other AE upon written request to the Orpheus state ORP from both AEs (Appendix 3, Cross-jurisdictional agreement). However, access to cases of specific diseases by AUs of the cooperating AEs still requires that the individual AU has been granted access to the specific disease group.

m. When an LPHA AU has a legitimate public-health need to view a case in another jurisdiction (e.g., contact tracing), the AU may request transfer of the case from that jurisdiction. Subsequently, the case will be visible to both AUs.

6. Changes to data.

   Changes to key Orpheus data are automatically captured in the Orpheus Log file; all Orpheus AUs have access to view the Orpheus Log file (*More* Tab|*Log*) . Record modifications are logged with the name and AU number of the AU who makes the modification, the time and date of the modification, and the specific change made. Whenever a record is viewed by an AU who does not make a modification to the record, this event is also recorded in the log. In addition, Orpheus AUs 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 AU 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 AE 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 disagreement 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 AE 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 AE representative opinion shall be given substantial weight; however, to ensure consistency of case definitions across Oregon counties, the state ORP retains the final authority to determine case Status (confirmed, probable, suspect, or non-case).

8. Authorized uses and disclosures
AUs may only use data in Orpheus and its linked databases in accordance with ORS 433.008, other applicable laws and these Policies and Procedures.

1. Individual's request for their Orpheus data.
   a. If an individual, or an individual's authorized representative requests a copy of their own record in Orpheus, for example, a disease outbreak form or a lab result, the request will be processed through Orpheus via a "Public Records Request" button located within the Orpheus Case Record. An AU with access to the Orpheus record can initiate and attach a copy of the request. The state ORP will be responsible for responding to the request and for attaching a copy the response to the same public record request. A signed OHA release, authenticated either by a notary public or by the case'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), that request must be provided by the AE to the state ORP immediately. If the AE has its own records, outside of Orpheus that are responsive to the PRR, the AE should respond in accordance with the PRA, as appropriate but should inform the requestor that OHA is the entity to which the PRR must be made in order to request Orpheus data.

3. If an AE receives a subpoena or court order for Orpheus data the subpoena or court order must be provided by the AE to the state ORP immediately.

4. OHA or a Local Public Health Authority may publish statistical compilations and reports relating to reportable disease investigations if the compilations and reports do not identify individual cases or sources of information in accordance with ORS 433.008. Release of any report or information must be consistent with the Oregon Public Health Division's *Guidelines for Reporting Small Numbers to Protect Confidentiality* https://dhsoha.sharepoint.com/teams/Hub-OHA-PH/SitePages/Science-Research.aspx?web=1 . An AU should consult with the AE ORP or the state ORP if they are uncertain whether a release is compliant with state law and this policy and procedures.

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 AUs 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 AU 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 state or AE ORP or their designees.

2. A limited-access, physically secure surveillance area shall be available to AUs. This area must always be kept secure.
    a. Keys, codes or other entry control devices shall be provided only to those persons authorized by DAS.
    b. The state or AE ORP or designees 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 state ORP in the case of state-level surveillance areas or the AE ORP in the case of surveillance areas overseen at the AE 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 bites. 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 AUs are encrypted. (See below.)

        a. All AUs 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. AUs external to Enterprise Technology Services (ETS) network 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 state ORP or AE 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 to re-image computers, ensuring that all data are wiped clean. Computers sent to surplus shall be physically destroyed by an 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 in accordance with ISO and DAS policies (http://www.oregon.gov/das/Surplus/Pages/E-waste.aspx)
   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 state ORP, AE 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 state ORP for DHS personnel or affiliates or the AE ORP for AE 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 AUs 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. AU privileges and password controls built in to Orpheus restrict access to record-level data to AUs.

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 AUs from outside of Portland State Office Building and AUs 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, when possible. AU privileges and password controls built into Orpheus restrict access to record-level data to AUs.
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 AE 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 AUs 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 AU 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, container, 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 AE ORP.

For Overall Responsible Parties and their Designees Only.
Please sign and return this page (e-mail or fax) to OHA
(Stephen.G.Ladd-Wilson@state.or.us; fax 971-673-1100).
Orpheus users will indicate that they have read this Policy on their Oaths.

Jurisdiction_____

Overall Responsible Party Printed Name_____
Overall Responsible Party Signature_____
Date_____

ORP Designee Printed Name_____
ORP Designee Signature_____
Date_____

ORP Designee Printed Name _____
ORP Designee Signature_____
Date_____

ORP Designee Printed Name _____
ORP Designee Signature_____
Date_____

ORP Designee Printed Name _____
ORP Designee Signature_____
Date_____

Definitions

Authorized Entity (AE): An Authorized Entity is an entity, e.g., local public health authority, tribal jurisdiction, etc., allowed by the State overall responsible party (ORP) to access Orpheus and its linked databases, provided they have an ORP for the entity, and that their users are authorized users (AUs).

Authorized User (AU): An individual approved by the state ORP or an AE ORP to access Orpheus and its linked databases to the extent permitted by the authorized access level.

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.

Overall Responsible Party (ORP): An overall responsible party (ORP) is an individual of an authorized entity (AE) who is responsible for assuring that Orpheus users within their purview are compliant with Orpheus Policies and Procedures.

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).

Record level data: Data elements from an individual record (e.g., Orpheus Case Record, Orpheus Person Record, Orpheus Laboratory Record, Orpheus, Contact Record), i.e., not aggregated with those in other records."

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.

Addendum – 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/Opera suite of databases 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*). Additionally, the Orpheus/Opera FileMaker Pro® Servers have the following back up schedule in place:

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

Recovery Point Objective (RPO) – 60 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.