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

Revision History:

January 5, 2010

Original Version

March 15, 2010

(Overview)
Deletion: ~~CPHP is collaborating with the DHS Information Security Office (ISO) and Office of Information Systems (OIS), CDC, and Local Health Authorities to develop a services level agreement. These security policies and procedures will be part of that larger agreement.~~

(Footnote 1)
Revision: A minor ~~infraction,~~ **inadvertent violation of local or CPHP security policies such as~~, like~~** forgetting to lock a file drawer **that policy requires be locked when not in use ~~containing sensitive information (even if inside a secure area)~~**, constitutes a breach of security protocol as compared with a breach of confidentiality.

(Section 5.A.)
Addition Subsection Header: **Public Health Users**
Correction: **C**~~c~~itrix
Correction: of program
Addition Subsections 3–5:

3. **Exporting data from Orpheus for analysis, or short- or long-term storage**
   a. **Exporting data from Orpheus and short- or long-term storage shall be explicitly approved by the Orpheus ORP or LPHA 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, and supervises and renews case record access for local users.**
   d. **State ORP or designee authorizes, delimits, and 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 her public health responsibilities.**
f. **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 her public health responsibilities.**
g. **Local users are limited by the Orpheus software to accessing case records within disease groups to which they have been granted access where case residence at diagnosis is within the jurisdiction in which they work except for certain diseases and circumstances listed below.**
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, she 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.)**
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 the collaborating jurisdiction/s 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 does not reveal the occurrence of the disease nor details of the case via the person record when the user does not have privileges to access that disease group or 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 ORP from both LPHA's. However, access to cases of specific diseases by users of the cooperating LPHA's 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.

(Section 5.C.)
Deletion Subsection 2: ~~Authorized staff providing access to, use of, or copies of the requested data shall consult with the LPHA ORP or their designee prior to release of summary or aggregate data involving the residents of a single LPHA or the Orpheus ORP in the event of proposed release of summary or aggregate data involving the residents of more than one LPHA if uncertain that the proposed release is compliant with program policy (Appendix 2).~~
Renumbered Subsection "3" to Subsection "2"
Added Subsection 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 (Appendix 2).**
Added Subsection 4: Authorized staff should consult with the LPHA or Orpheus ORP if they are uncertain that the proposed release is compliant with program policy.

(Section 6.A.)
Revise Subsection 2.c: **If feasible, ~~K~~k**eys

(Section 6.B.)
Revise Subsection 1.d: When an authorized user leaves their position the Orpheus ORP (CPHP staff) or LPHA ORP (LPHA staff) **or designee** shall be informed by the supervisor of the departing staff member and will request that the DHS Service Desk suspend access (log-in ability) to the workstations and remote servers immediately.

Revise Subsection 2: Storage or viewing of record-level ~~data~~ surveillance data on laptop computers or other portable devices, or external storage devices.

Revise Subsection 2.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 ~~that are~~ **with** simultaneous connections to the internet or local wide-area networks ~~that~~ **unless those connections** ~~in the opinion of the DHS Information Security Office are not properly secured.~~ comply completely with local or state information policies and procedures on security of record-level data.

Revise Subsection 4.a.: Each workstation from which Orpheus data are accessed shall revert to screen-saver mode no more than **10~~5~~** minutes after last activity, and require a password to resume activity.

July 15, 2010

(Section 5.A.)
Addition: **The State ORP or designee shall not revoke Orpheus access of an authorized LPHA user without the request of the LPHA ORP or designee or prior notification of the LPHA ORP.**

(Section 6.B.)
Revise Subsection 3.d. When an authorized user leaves their position the Orpheus ORP (CPHP staff) or LPHA ORP (LPHA staff) or designee shall be informed by the **LPHA ORP or designee (e.g.,** supervisor of the departing staff member**)** and will request that the DHS Service Desk suspend access (log-in ability) to the workstations and remote servers immediately.

(Overview)
Addition: **All surveillance data contained within Orpheus are owned jointly by the LPHA of the county where the case is diagnosed and CPHP.**

(Title page; Overview)
Replace: ~~Oregon Department of Human Services~~ with **Oregon Health Authority**

(Overview; Section 2.A, Subsection 3; Sections 3.C and E; Section 4.B, Subsection 1; Section 5.A. (twice); Subsection 5.b., Subsection 1.f.; Section 6.B, Subsections 1.d. and 2.c.)
Replace: ~~DHS~~ with **OHA**

(Section 5.A.)
Addition of Subsection 6:
Changes to data
Changes to Orpheus data are automatically captured in two logs: the Case Log and the Audit Log. All authorized Orpheus users have access to both logs. All 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 cases" status when a suspect case has been "ruled-out;" *Deceased* (i.e., a case is designated as died), *Disease*, 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 Epidemiologist after considering opinions expressed.

Addition of Subsection 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 diagnosis will work with the State Epidemiologist 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 State retains the final authority to determine case Status (confirmed, probable, suspect, or non-case)."

September 3, 2010

(Section 6)
Addition: Added the fields indicating **"*Hospitalized,*""** and **"*Associated with an Outbreak*""** to the list of fields, that when modified, will trigger a notification to the appropriated LHD.

October 26, 2010

(Section 6 B 4 a)
Data change: **no more than 15 minutes** from 10 minutes.

4. Other practices related to computer workstations, laptops and other electronic storage media used to store, view or analyze record-level data.
a. Each workstation from which Orpheus data are accessed shall revert to screen-saver mode no more than ~~10~~ **15 minutes** after last activity, and require a password to resume activity.

(Section 6 C)

Addition: Paper and other hard copies of data **originating from Orpheus**

(Section 6 C 2)

Addition: **"if feasible"**

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.

December 12, 2010

(Section B)

Addition: Added the following: (#6): Exercise their right to implement local security policies that are more stringent than these statewide Orpheus security policies and procedures.

(Section 3 F) Staff Responsibilities and Requirements

Addition: **performed by authorized OHA staff**
All authorized users will be subject to periodic random audits of Orpheus logs **performed by authorized OHA staff.**

(Section 4 A 1) Breaches of Confidentiality

Revised: Anyone who becomes aware of a breach of security protocol without breach of confidentiality shall report this to ~~CPHP or LPHA ORP or their designee~~ **LPHA ORP or designee, or to the STATE ORP**;

(Section 4 B 1) Breaches of Confidentiality
Revised: All must be reported ~~immediately~~ **within one working day** to **the** STATE ORP, ~~the~~ **who will be responsible for reporting to** OHA ISO and to CDC.

(Section 4 B 2) Breaches of Confidentiality
Addition: Employee(s) responsible for any breach may face disciplinary action, up to and including termination of employment **as determined by the employer.**

(Section 5 A 2 c) Data Access and Use
Addition: Added the following disease groups:
x. Pertussis
xi. CIN (cervical intraepithelial neoplasia)

(Section 5 B 1 k) Data Access and Use
Revision: 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 level data (~~Appendix 2~~ **available from CPHP upon request**) and reviewed by the LPHA ORP for publications involving residents of a single LPHA or the Orpheus ORP or their designee for publications involving more than one LPHA prior to publication.

(Section 5 C 2) Data Access and Use
Revision: Release of aggregate data shall be compliant with all aggregate data release guidelines (~~Appendix 2~~ **available from CPHP upon request**).

(Section 5 C 3) Data Access and Use
Revision: 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 (~~Appendix 2~~ **available from CPHP upon request**).

(Section 5 A 7) Data Access and Use
Adition: **time of** diagnosis**:** 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 State Epidemiologist 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 State retains the final authority to determine case Status (confirmed, probable, suspect, or non-case)."

(Section 6 B 1 d) Data Security
Revision: ~~When an authorized user leaves their position the Orpheus ORP (CPHP staff) or LPHA ORP (LPHA staff) or designee shall be informed by the LPHA ORP or designee (e.g., supervisor of the departing staff member) and will request that the OHA Service Desk suspend access (log-in ability) to the workstations and remote servers immediately.~~
The LPHA ORP or designee must notify the STATE ORP within 14 days after an

authorized user leaves their position. The STATE ORP will be responsible for contacting the OHA Service Desk to immediately suspend Orpheus access for that user.

April 13, 2011

(Section 6)
Added "County/counties of jurisdiction" to Overall Responsible Party signature block

July 7, 2011

(Section 5 A 2 c) Data Access and Use
Addition: Added the following disease group:
xii. Syphilis

May 29, 2012

(Section 5 A 2 c) Data Access and Use
Addition: Added the following disease group:
xiii. LTBI

July 17, 2012

Changed "Office of Disease Prevention and Epidemiology (ODPE) to Center for Public Health Practice (CPHP)

December 27, 2012

Addition: First sentence to the Overview
Information obtained by the Oregon Health Authority 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); http://www.leg.state.or.us/ors/433.html).

December 24, 2013

Formatting: Moved the Revision Section from beginning of the document to the end of the document.

Addition: Created a Definition section.

(Overview)
Addition: Added web link to (ORS 433.008(1)(a); http://www.leg.state.or.us/ors/433.html
Change (from public health "professionals" to public health "officials")

Overview

Information obtained by the Oregon Health Authority 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); http://www.leg.state.or.us/ors/433.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 security and 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 Enterprise Technology Services (ETS)It contains security and confidentiality standards, expectations, practices, and corrective procedures.

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

(Policies|Written Policies and Procedures)
Changed web link: B.

B. A master copy of this document shall be kept up-to-date and stored on Oregon's OHA's website: http://public.health.oregon.gov/DISEASESCONDITIONS/COMMUNICABLEDISEASE/LOCALHEALTHDEPARTMENTS/Pages/Orpheus.aspx~~Health Alert Network (HAN).~~

C Removed the word, hard. No need to require a hard copy; electronic copy suffices.

C. At least one up-to-date ~~hard~~ copy and each LPHA ORP.

(Policies|Overall Responsible Party|2A)
Change:

2) OVERALL RESPONSIBLE PARTY]

A. The Overall Responsible Party (ORP) for the security of Orpheus data is the Center for Public Health Practice Administrator, ~~Oregon State Epidemiologist~~ (~~Katrina Hedberg, MD, MPH~~Tom Eversole, DVM, MS) in Oregon Public Health Division. The ORP or designee shall:

(Addition 5 (a-c), 7, 8 d -11)

5. Annually ~~R~~review these policies and procedures with all active CPHP ~~employees authorized to access record level~~ Orpheus users ~~data~~ and answer any questions those employees might have about these policies and procedures. Users will be de-activated if ORPs or their designees fail to verify (read, signed, and return to CPHP) the following within two months after receipt of user-specific annual security audits and following forms:
    a. Orpheus Security Policies and Procedures (this document).
    b. User-specific Security Audit produced by CPHP
        i. Users' secure data export location(s)
        ii. Users' county and disease-group settings
        iii. Users' OHA-specific security and confidentiality policies
    c. User-specific Orpheus Confidentiality Statement (User Oath)

7. Ensure that state Orpheus users take responsibility for 1) implementing OHA's data security policy and procedures, 2) for protecting the security of any device in their possession on which personally identifiable information (PII) from Orpheus is stored, and 3) for reporting suspected security breaches. These responsibilities include but are not limited to:
    a. Protecting keys, passwords, and codes that would facilitate unauthorized access to PII
    b. Taking appropriate action to avoid infecting computer systems with viruses and other malware
    c. Appropriate use of personal computers and storage devices
    d. Appropriate removal of data from secure facilities

8. ~~Assure~~ Ensure the completion of periodic random audits of user logs and investigation of any irregular use patterns, and maintain records of the outcomes of these audits. Ensure that all Orpheus users:
    ~~1)~~a. ~~f~~Fully implement OHA's data security policy and procedures;
    ~~, 2~~b.~~)~~ ~~p~~Protect the security of any device in their possession on which personally identifiable information (PII) from Orpheus is stored;
    ~~, and 3)~~ c. R~~r~~eport suspected security breaches;
    ~~7.~~ ~~4~~d. ~~S~~Safeguard~~ing~~ keys, passwords, and codes that would facilitate unauthorized access to PII;
    e. Take~~ing~~ appropriate action to avoid infecting computer systems with viruses and other malware;
    f. ~~P~~Protect~~ing~~ mobile devices and storage media from loss and theft;e
    ~~. Appropriate use of personal computers and storage devices~~
    ~~8.~~ g. Obtain authorization prior to ~~Appropriate~~ removal of data from secure facilities.
    9. Ensure that any PII sent from Orpheus in an e-mail is sent using the encryption standard of the department, e.g., using "#secure#" in the subject line.
    10. Ensure that 2-factor authentication tokens are distributed to validated Orpheus users.
    11. State ORP will send proof of annual review to independent OHA reviewer, e.g., the Performance Management Program.

5. Annually ~~R~~review these policies and procedures with all active LPHA ~~employees authorized to access record-level~~ Orpheus users ~~data~~ and answer any questions those employees might have about these policies and procedures. Users will be de-activated if ORPs or their designees fail to verify (read, signed, and return to CPHP) the following within two months after receipt of user-specific annual security audits and following forms:
    a. Orpheus Security Policies and Procedures (this document)
    b. User-specific Security Audit produced by CPHP
        i. Users' secure data export location(s)
        ii. Users' county and disease-group privileges
        iii. Users' jurisdiction-specific security and confidentiality policies
    c. User-specific Orpheus Confidentiality Statement (User Oath)

~~5.d~~

of these audits.

8. Ensure that all Orpheus users
    ~~1)~~a. ~~f~~Fully implement OHA's data security policy and procedures;
    ~~, 2b.)~~ ~~p~~Protect the security of any device in their possession on which personally identifiable information (PII) from Orpheus is stored;
    ~~, and 3)~~ c. ~~R~~report suspected security breaches;
    ~~7.~~ ~~4~~d. ~~S~~Safeguard~~ing~~ keys, passwords, and codes that would facilitate unauthorized access to PII;
    e. Take~~ing~~ appropriate action to avoid infecting computer systems with viruses and other malware;
    f. ~~P~~Protect~~ing~~ mobile devices and storage media from loss and theft;~~e~~
    ~~Appropriate use of personal computers and storage devices~~
    ~~8.~~ g. Obtain authorization prior to ~~Appropriate~~ removal of data from secure facilities.
9. Ensure that any PII sent from Orpheus in an e-mail is sent using the encryption standard of the department, e.g., using "#secure#" in the subject line.
10. Ensure that 2-factor authentication tokens are distributed to validated Orpheus users.
11. State ORP will send proof of annual review to independent OHA reviewer, e.g., the Performance Management Program.

~~5.~~d.

6. Exercise their right to implement local security policies that are more stringent than these statewide Orpheus security policies and procedures.
    a. Ensure that all Orpheus users take responsibility for 1) implementing their local data security policy and procedures, 2) for protecting the security of any device in their possession on which personally identifiable information (PII) from Orpheus is stored, and 3) for reporting suspected security breaches. These responsibilities include but are not limited to;
    b. Protecting keys, passwords, and codes that would facilitate unauthorized access to PII
    c. Taking appropriate action to avoid infecting computer systems with viruses and other malware
    d. Appropriate use of personal computers and storage devices
    e. Appropriate removal of data from secure facilities
7. Ensure that any PII sent from Orpheus in an e-mail is sent using the encryption standard of the LPHA, e.g., using "#secure#" in the subject line.
~~6.~~ Ensure that Orpheus Users (under their purview) meet at least annually with their 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.

Staff Responsibilities And Requirements
(Addition 3c e, f)
Addition:

C. Each person authorized to access record-level Orpheus data assumes individual responsibility for challenging any unauthorized individual who is observed attempting to access Orpheus data; and to report immediately any suspected security breaches[1] to the ORP or designee, according to the OHA Privacy and Information Security Incident Response Policy (http://www.dhs.state.or.us/policy/admin/security/090_005_01.htm).

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 associated with 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 damaging causes, such as extreme heat or cold.

E. Confidentiality training of non-surveillance staff must also include review of these policies and reporting of suspected security breaches to the ORP and in accordance with the OHA Privacy and Information Security Incident Response Policy (http://www.dhs.state.or.us/policy/admin/security/090_005.htm).

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 loses or suffer reduced access (e.g., constraining their privilege set) to confidential data and may face disciplinary action up to and including termination.

5 DATA ACCESS AND USE
Correction:

OHA remote access form to the Orpheus Team at OPHD (Orpheus.~~CPHP~~ODPE-Tech@state.or.us or 971-673-1100). Within a week they will receive a Citrix ID

A2c (Privilege sets-Disease Groups)
Addition: Pertussis, CJD, ABC, Lead, MDRO

A3 (Exporting)
Addition:

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. ~~Exporting data from Orpheus and short- or long-term storage shall be explicitly approved by the Orpheus ORP or LPHA ORP or designee.~~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 encrypted when not in use.
   c. Users who are unsure of appropriate storage locations should consult with their supervisor.
   ~~a.~~d. If a user wishes to store or transfer data via a location not already approved, he/she shall obtain prior approval from ORP.

6 Changes to Data
Subtraction):

6. Changes to data
   Changes to Orpheus data are automatically captured in ~~two logs: the Case Log and the Audit Log~~the Orpheus Log file; all ~~authorized~~ Orpheus users have access to ~~both~~ view the Orpheus Log file (*More* Tab|*Log*) ~~logs~~. ~~All R~~record

Comment: We are using only one audit log instead of 2 logs; we've discontinued use of FMDataGuard due to performance issues with FMDataGuard and FileMaker 12's ability to do progressive back-ups

Subtraction: ~~All~~ 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.
Comment: Not all record modifications are captured. We stopped using FMDataGuard in Spring of 2012 due to performance issues; Orpheus Log file was separated from the Orpheus Data file to increase performance and reliability. (Personal communication: Matt Navarre, MSN Media, Inc. (mattn@msnmedia.com) December 24, 2013.

B: Record-level access: Addition

B. Record-level access – all others. The following are subject to ORS 433.008 (http://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors433.html).
1. For public health or human subjects research purposes.

B. Electronic data storage, access and transfer
1. The Orpheus application
Orpheus is ~~being built using~~a FileMaker Pro® application; it is a relational database ~~under development by~~~~developed~~sponsored by CPHP. Orpheus houses public health case report data for all cases of reportable communicable disease in Oregon.

C: Aggregate-level access: Addition

C. Aggregate-level access – everyone
1. Any person may obtain summary or aggregate de-identified data upon request, as may be allowed under ORS 433.008 (http://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors433.html).
2. Release of aggregate data shall be compliant with all aggregate data release

Data Security (6 b 1 a)
Correction:

the same or another reportable disease.
b. Authorized users external to ~~the state data center~~ ETS shall use two-factor authentication. Data ~~should be~~ encrypted~~ion of data~~ when not in use, and ~~encryption of~~during transmissions between workstations. ~~and remotely stored and accessed data.~~

Data Security (6 b 2 c & f & 3d)
Addition:

secure areas shall be locked in a secure cabinet when not in use.
c. DHS Office of Information Technology staff shall use ISO-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 ISO-approved vendor, assuring that all data are inaccessible or destroyed in the process. Record-level data shall be deleted from laptops computers,

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 ~~with simultaneous connections to the internet or local wide-area networks unless those connections comply completely 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

restrict access to record-level data to authorized users.

d. Indefinite storage of confidential surveillance data if necessary for public purposes.

   i. Storage, e.g., of exported data, must be approved by the State or LPHA ORP.

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

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 _____

~~County (counties) of j~~Jurisdiction _____
Date _____

April 23, 2014

5 DATA ACCESS AND USE
Correction:

organization, and their public health responsibilities. The State ORP or designee shall not revoke Orpheus access of an authorized LPHA user without the request ~~of the LPHA ORP or designee~~ or prior notification of the LPHA ORP or designee. ~~The assignment of p~~Program area and jurisdiction rights to a user will be ~~performed~~ assigned by one of the Orpheus Team members at ~~the~~ OPHD based on the programs and jurisdictions approved by the State or LPHA ORP, as appropriate.

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.

~~e.~~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.

~~f.~~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.

~~g. Local users are limited by the Orpheus software to accessing case records within disease groups to which they have been granted access where case residence at diagnosis is within the jurisdiction in which they work except for certain diseases and circumstances listed below.~~

h. State users are permitted by the Orpheus software to access case records for

June 2, 2015

Overview

Information obtained by the Oregon Health Authority 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); https://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors433.html) ~~http://www.leg.state.or.us/ors/433.html~~). Public health surveillance data must be handled

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 Oregon's reportable diseases for the overarching purpose of reducing morbidity and mortality.

Orpheus is also linked to "Outbreaks," "Case Log," "Napoli," "Shotgun" and "Shiver" – disease surveillance databases that house confidential, outbreak-specific information – this policy also pertains to users who access these databases.

Policies

1) WRITTEN POLICIES AND PROCEDURES

A. Operating policies and procedures for Orpheus 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
~~http://public.health.oregon.gov/DISEASESCONDITIONS/COMMUNICABLEDISEASE/LOCALHEALTHDEPARTMENTS/Pages/Orpheus.aspx.~~

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

Overall Responsible Party

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 for ~~Orpheus CPHP ORP~~ in 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.
~~5.~~6. Deactivate ~~U~~users. ~~will be de-activated if~~for ORPs ~~or their designees~~who fail to read, sign, and return to CPHP their agreements to the following within two months ~~after~~ 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~~²~~ secure data export location(s)

        ii. User's~~²~~ county and disease-group settings
        iii. User's~~²~~ OHA-specific security and confidentiality policies, i.e., the 090 and 100 series found at http://www.dhs.state.or.us/policy/
    c. User-specific Orpheus Confidentiality Statement (User Oath);

~~6.~~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 state Orpheus users ~~take~~ assume responsibility for:

   1. ~~1)~~ implementing OHA's data security policy and procedures,
   2. ~~2) for~~ protecting the security of any device in their possession on which personally identifiable information (PII) from Orpheus is stored, ~~and 3)~~
   3. ~~for~~ reporting suspected security breaches.

~~7.~~ These responsibilities include but are not limited to:

   a. Protecting keys, passwords, and codes that would facilitate unauthorized access to PII; and
   b. Taking appropriate action to avoid infecting computer systems with viruses and other malware; and
   c. ~~Appropriate~~ 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
   d. ~~Appropriate~~ 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.

~~8.~~10. Ensure that all state Orpheus users:

   a. Fully implement OHA's data security polic~~y~~ies and procedures;
   b. ~~Protect~~ Safeguard the security of any OHA device in their possession on which personally identifiable information (PII) from Orpheus is stored;
   c. Report suspected security breaches;
   d. Safeguard keys, passwords, and codes that would facilitate unauthorized access to PII;
   e. ~~Take appropriate action to~~Exercise reasonable judgement in use of technology avoid infecting OHA computer systems with viruses and other malware;
   f. Protect mobile devices and storage media from loss and theft; and
   g. Obtain authorization prior to removal of data from secure facilities.

~~9~~11. ~~.~~Ensure that any PII sent from Orpheus in an e-mail is sent using the encryption standard of the department, ~~e.g~~i.e., ~~,~~ using "#secure#" in the subject line.

12. ~~10.~~Ensure that 2-factor authentication tokens are distributed to validated Orpheus users.

11. State ORP will 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 agencies comply 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.

and procedures.

5.6. ~~Users will be de~~De-activate~~d~~ users or ~~if~~ ORPs ~~or their designees~~who fail to read, sign, and return to CPHP their agreements to the following within two months ~~after~~ 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~~s' secure data export location(s)
      ii. User's' county and disease-group privileges
      iii. User's' jurisdiction-specific security and confidentiality policies
   c. User-specific Orpheus Confidentiality Statement (User Oath)

6.7. Exercise their right to implement local security policies that are more stringent than these statewide Orpheus security policies and procedures. Local security policy may include:

a. Ensuring that all Orpheus users take responsibility for

i. 1) implementing their local data security policy and procedures, 2

ii.) for protecting the security of any device in their possession on which personally identifiable information (PII) from Orpheus is stored, and 3) for

a. iii. reporting suspected security breaches. These responsibilities include but are not limited to:

b. Protecting keys, passwords, and codes that could facilitate unauthorized access to PII

c. Taking appropriate action to avoid infecting computer systems with viruses or malware

d. Appropriate use of personal computers and storage devices

e. Appropriate removal of data from secure facilities

7.8. Ensure that any PII sent from Orpheus in an e-mail is sent securely using the encryption standard of the LPHA, e.g., using "#secure#" in the subject line.

8.9. Ensure that Orpheus Users (under within their purview) meet at least annually with their 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.

Staff Responsibilities and Requirements (re-numbered)

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.dhs.state.or.us/policy/)

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 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).

~~A.~~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.

Data Access and Use

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, ~~they~~ the user returns the signed oath

and the OHA remote access form to the Orpheus Team at OPHD (Orpheus.ODPE-Tech@state.or.us or 971-673-1100). Within a week ~~they~~ the user will receive a Citrix ID number assigned by the OHA Service D~~d~~esk, 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 ~~they are~~ 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 ~~the request or~~ 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.

Security Breaches (minor edit)

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 ~~at~~ 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~~s~~ 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 Office (ISO) 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.

Data Access and Use

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, ~~they~~ the user returns the signed oath

and the OHA remote access form to the Orpheus Team at OPHD (Orpheus.ODPE-Tech@state.or.us or 971-673-1100). Within a week ~~they~~ the user will receive a Citrix ID number assigned by the OHA Service Ddesk, 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 ~~they are~~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 ~~the request or~~ 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.

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. ~~Very few~~About 26 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. About seven 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 2 users – both State users – have this privilege set.
   g. The All Records role is mainly for State STD workers to efficiently manage case records within Orpheus – Only three State STD workers have this role.
   h. The All Records + Scripts role is only for one State Lead Surveillance worker.
   ~~e.~~ i

~~e.~~i.

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 ~~only a few~~,about 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 ~~the~~ records that can be viewed by disease group. Currently available disease groups include:

Alphabetized disease groups

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. Hepatitis;
vii. HIV;
viii. Lead
ix. LTBI (Latent TB Infection)
x. MDRO (Multi-Drug Resistance Organisms)
xi. Miscellaneous communicable diseases;
xii. Pertussis;
xiii. STD (Gonorrhea & Chlamydia)
xiv. Syphilis;
xv. TB (Tuberculosis);

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 ~~via~~ in a location not already approved, he/she must obtain prior approval from ORP or designee.
4. Data storage, access and transfer of data shall be consistent with all related

Cross-jurisdictional sharing

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, ~~and~~ supervises, ~~,~~ and renews

Record Level Access

B. Record-level access – all others. The following are ~~subject to~~consistent with ORS 433.008 (http://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors433.html).
   1. For public health or human subjects research purposes.

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 Orpheus ORP or the PRT—or the LPHA ORP in the case of requests for data involving residents of a single LPHA—or the investigator must be approved by the Institutional Review Board for Oregon Public Health Division.
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 he/she understands the penalties for unauthorized disclosure, assures that the data will be stored in a secured area, and agrees to ~~sanitize or destroy any~~adhere to any commitments to sanitize hard drives or other storage devices ~~computer 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

B. Electronic data storage, access and transfer

1. The Orpheus application

Orpheus is a FileMaker Pro® application; it is a relational database ~~sponsored~~ developed and maintained by CPHP. Orpheus houses public health data for all cases of reportable communicable disease in Oregon; it also houses ~~blood lead~~ data related to reportable blood lead levels, as well as reportable animal bite data.

the process. Record-level data shall be deleted from laptops 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 ISO.

d. Data stored on laptop computers, removable hard drives or external storage

Electronic data storage, access and transfer

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 at OPHD (Orpheus.ODPE-Tech@state.or.us or 971-673-1100). Within a week the user will receive a Citrix ID number assigned by the ~~OHA Service Desk~~Orpheus Tech Team, and obtain access to

by authorized users using desktop computers located within the Portland State Office Building occurs over private, high-speed transmission lines behind a 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~~ 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. Storage ~~must occur~~ on computer servers or workstations is approved by ORP that are not conveniently portable.
    iii. Computer servers or workstations storing confidential data must be

physically and electronically protected in a manner completely consistent with these policies.

iv. If feasible, ~~D~~data ~~must~~ should be be encrypted using FIPS-197-compliant encryption when not in use and during transfer.

June 2, 2015

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 at OPHD (Orpheus.ODPE-Tech@state.or.us or 971-673-1100). Within a week the user will receive a Citrix ID number assigned by the ~~OHA Service Desk~~Orpheus Tech Team, and obtain access to

June 23, 2015

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 ~~an act of God~~a natural disaster, a person, or an application/system and may be malicious in nature or purely unintended. An example of a

August 15, 2015

Overview (page 1)

maintain confidentiality. This document prescribes policies and procedures by which public health employees in Oregon safeguard the ~~security and~~ confidentiality of public health data collected by public health professionals and maintained by Local Public Health Authorities, Center for Public Health Practice and the Oregon Department of Administrative Services Enterprise Technology Services (ETS). It contains security and confidentiality standards,

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.

Orpheus is also linked to "Outbreaks," "Case Log," "Napoli," "Shotgun" and "Shiver" – disease surveillance databases that house confidential, ~~outbreak-specific information~~personally identifiable information related to communicable disease control – this policy also pertains to users who access these databases.

Policies, 1) Written Policies and Procedures (page 2)

Policies

1) WRITTEN POLICIES AND PROCEDURES

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

Policies, 2) Overall Responsible Party (page 2)

2) OVERALL RESPONSIBLE PARTY

A. The Overall Responsible Party (ORP) for the security of Orpheus data is the Center for Public Health Practice Administrator, (~~Tom Eversole, DVM, MS~~Collette Young, PhD) in the Oregon Public Health Division. The state ORP or designee shall:

Policies, 2) Overall Responsible Party (page 3)

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.

~~These responsibilities include but are not limited to~~Steps users can take to fufill these responsibilities include but are not limited to:

8. Ensure that all state Orpheus users assume responsibility for:
    a. fully implementing OHA's data security policies~~y~~ and procedures,
    b. ~~protecting~~ 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.

These responsibilities include but are not limited to:

a. Protecting keys, passwords, and codes that would facilitate unauthorized access to PII; and
~~Taking appropriate action to avoid infecting computer systems with viruses and other malware~~Exercising reasonable judgement in the use of technology to avoid infecting OHA computer systems with viruses and other malware; and
b. 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
c. 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.
e. protecting mobile devices and storage media from loss and theft; and
~~d.~~ f. obtaining authorization prior to removal of data from secure facilities.

merge 8 &10 correct subsequent numbering

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 all state Orpheus users:~~
~~a. Fully implement OHA's data security policies and procedures;~~
~~b. Safeguard the security of any OHA device in their possession on which personally identifiable information (PII) from Orpheus is stored;~~
~~c. Report suspected security breaches;~~
~~d. Safeguard keys, passwords, and codes that would facilitate unauthorized access to PII;~~
~~e. Exercise reasonable judgement in use of technology avoid infecting OHA computer systems with viruses and other malware;~~
~~f. Protect mobile devices and storage media from loss and theft; and~~
~~g. Obtain authorization prior to removal of data from secure facilities.~~

~~11.~~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.

~~12.~~11. Ensure that 2-factor authentication tokens are distributed to validated Orpheus users.

~~13.~~12. State ORP will send proof of annual review to independent OHA reviewer, e.g., the Performance Management Program.

12. ~~State ORP will s~~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~~ies~~ comply~~ies~~ with the requirements of this document, including all future updates;
        6. Direct the state ORP or designee to ~~D~~de-activate users or ORPs who fail to read,

7. Exercise their right to implement local security policies that are more stringent than these statewide Orpheus security policies and procedures. ~~Local security policy may include:~~

Policies, 2) Overall Responsible Party (page 4)

7. Exercise their right to implement local security policies that are more stringent than these statewide Orpheus security policies and procedures.
    a. Ensuring that all Orpheus users take responsibility for
        i. fully implementing local data security policy and procedures,
        ii. ~~protecting~~ safeguarding the security of any device in their possession on which personally identifiable information (PII) from Orpheus is stored,
        iii. reporting suspected security breaches.

    These responsibilities include but are not limited to:
    b. ~~P~~protecting keys, passwords, and codes that could facilitate unauthorized access to PII; and
    c. exercising reasonable judgement in the use of technology to avoid infecting LPHA computer systems with viruses and other malware; and
    d. 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
    e. 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.
    f. protecting mobile devices and storage from loss and theft; and
    ~~b.~~g. obtaining authorization prior to removal from secure LPHA facilities.
    ~~c. Taking appropriate action to avoid infecting computer systems with viruses or malware~~
    ~~d. Appropriate use of personal computers and storage devices~~
    ~~e. Appropriate removal of data from secure facilities~~
8. Ensure that any PII sent from Orpheus in an e-mail is sent securely using the encryption standard of the LPHA.
9. 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.

~~9.~~10. 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.

Policies, 2) Staff Responsibilities and Requirements page 5

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

Policies, 4) Security Breaches page 5

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.

Policies, 5) Data Access and Use page 6

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 at OPHD (Orpheus.ODPE-Tech@state.or.us or 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.

page 7

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;

page 8

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 presumed 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.").

Record-level access – all others. Page 10

g. Data access or release for purposes defined as human subjects research by the investigator, the Orpheus ORP ~~or~~ the PRT—or the LPHA ORP in the case of requests for data involving residents of a single LPHA—~~or the investigator~~ must be approved by the Oregon Public Health Division's Institutional Review Board, for ~~Oregon Public Health Division.~~

Aggregate-level access – everyone. Page 11

C. Aggregate-level access – everyone
   1. Any person may obtain summary or aggregate de-identified data upon request, as ~~may be~~ allowed under ORS 433.008

Electronic storage and transfer. Page 12

b. Authorized users external to Enterprise Technical Services (ETS) shall use two-factor authentication. ~~Identifying data must be encrypted when not in use, and during transmissions between workstations~~All data are encrypted during transmission via secure socket layer (SSL).

Merged with LPHA ORP Duties

~~d. The LPHA ORP or designee must notify the CPHP ORP within 14 days after an authorized user leaves their position. The CPHP ORP will be responsible for contacting the Orpheus Tech Team to immediately suspend Orpheus access for that user.~~

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. Storage on computer servers or workstations is approved by ORP that are not conveniently portable.~~
   ~~iii.~~ii. Computer servers or workstations storing confidential data must be physically and electronically protected in a manner completely consistent with these policies.
   ~~iv.~~iii. If feasible, data should be be encrypted using FIPS-197-compliant encryption when not in use and during transfer.

December 7, 2017

Overview, Page 1

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/ors/ors433.html ~~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 (CPHP), the Center for Health Protection (CHP), the ~~Oregon Health Authority~~OHA Information Security Office (ISO), 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~~OHA.

Orpheus, designed for public health use, is a ~~public health surveillance~~computer 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

Policies 2) Overall Responsible Party. Page 2

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~~ nine 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~~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

Policies 2) Overall Responsible Party. Page 3

7. In collaboration with ISO, e~~E~~nsure 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. P~~p~~rovide and maintain a list of all personnel at ETS or other co-located sites.(~~State Data Center where off-site backups of Oregon data are housed~~), with the ability to access Orpheus data, and the date of their most recent security or privacy training.
   ~~7.~~b. R~~r~~eview at least annually with OIS all users with privileged access (PA) to relevant servers.

Policies 2) B (5) Overall Responsible Party. Page 4

users and answer any questions those employees might have about these policies and procedures.

   a. Annually provide a list of LPHA IT personnel who have privileged access to Orpheus data and their most recent date of LHPA security and privacy training.

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. User acknowledgement of familiarity with 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. As the need arises, eExercise their right to implement local security policies that are more stringent than these statewide Orpheus security policies and procedures.
8. Ensureing 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 in encrypted form, 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 each user's Orpheus Security Audit Report, including but not limited to, review of 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-

Policies 2) B (11) Overall Responsible Party. Page 5

specific security policies.

11. The LPHA ORP or designee must notify the Orpheus Tech Team (Orpheus.ODPE-Tech@state.or.us) within ~~14~~ 7 days after an authorized user leaves their position.

Policies 3) B (11) Overall Responsible Party. Page 5

E. ~~Confidentiality training of non-surveillance~~Staff who are not involved in public health data collection, case investigation or related activities ~~staff~~, e.g., system administrators, must – also ~~include~~ review ~~of~~ these policies and other policies related to 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 Orpheus users will be subject to periodic random audits of Orpheus logs performed by other 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.

Staff Responsitilities and Requirements; Security Breaches, Page 5

extreme heat or cold.

E. ~~Confidentiality training of non-surveillance~~Staff who are not involved in public health data collection, case investigation or related activities ~~staff~~, e.g., system administrators, must– also ~~include~~ review ~~of~~ these policies 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 ~~http://www.oregon.gov/oha/Admin/infosec/pages/incdnt_resp.aspx~~).

F. All authorized Orpheus users will be subject to periodic random audits of Orpheus logs performed by other 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, or to ISO.
2. ORP shall ensure that all reports are logged and investigated and oversee the

Security Breaches, Page 6

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 a suspected ~~n~~ intentional breach, the ORP should consult with appropriate legal counsel to determine whether reporting to law enforcement agencies is warranted.

Data Access and Use, Page 6

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 or multiple roles of several available 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.

Data Access and Use, Roles, Page 7

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.~~d. 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.~~e. 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.~~f. Two State workers have the All Records+Scripts role..

Data Access and Use, Resolution of Disputes, Page 10

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~~ disagreement will meet informally and attempt to come to agreement on the data of record to be retained within Orpheus. If an

Record Level Access – All Others (f) Page 11

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),~~Science & Epidemiology Council (SEC) 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

policies and procedures.

~~2.~~ Other purposes (e.g., litigation).

2. 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.
   a. Public record requests will be processed through Orpheus via a "Public Records Request" button located within the Orpheus Case Record. LPHA personnel 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.

C. Aggregate-level access—everyone.
   1. Any person may obtain summary or aggregate de-identified data upon request, as allowed under ORS 433.008 (https://www.oregonlegislature.gov/bills_laws/ors/ors433.html~~http://www.oregonlegislature.gov/bills_laws/lawsstatutes/2013ors433.html~~).
   2. Release of aggregate data shall be ~~compliant~~ consistent 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

Storage or viewing of record level data – Page 13

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~~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

Paper …originating from Orpheus – Page 15

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~~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, ~~r~~ with a cross-cutting feature if feasible, after it is no longer needed.

Re-vamped Signature Page - Page 15

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.

~~ame~~Jurisdiction _____

Overall Responsible Party Printed Name ~~Signature~~ _____

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~~

December 4, 2018

Title and Overview, Page 1

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

Oregon Health Authority
Public Health Division
Center for Public Health Practice

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 n~~, n~~ot subject to public disclosure, and can only be disclosed in certain circumstances (ORS 433.008 ~~§1.a~~; 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~~is document prescribes~~ policies and procedures seek to ~~by which public health employees in Oregon~~ ensure the security and ~~safeguard the~~ confidentiality of public health data contained in the Oregon Public Health Epidemiology User System (Orpheus) operated and owned by the State of Oregon, ~~collected by public health professionals and maintained by Local Public Health Authorities, the Center for Public Health Practice (CPHP), the Center for Health Protection (CHP), the OHA Information Security Office (ISO), and the Oregon Department of Administrative Services/~~Oregon Health Authority (OHA), and the databases linked to Orpheus. ~~Enterprise Technology Services (ETS). It contains security and confidentiality standards, expectations, practices, and corrective procedures.~~

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 ~~The Oregon Public Health Epidemiology User System (~~Orpheus~~)~~ computer application and its data ~~are stored~~ are 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 OHA, Oregon Public Health Division (OPHD), 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~~

Title and Overview, Page 2

~~county of residence of a case and~~ OHA.

Orpheus ~~, designed for public health use,~~ is ~~a computer application~~ intended for use by state, ~~and~~ 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 "Outbreaks," "Case Log," "Napoli," "Shotgun" and "Shiver"—other disease surveillance databases that house confidential, personally identifiable information (PII) related to communicable disease control. These~~is~~ policies and procedures~~y~~ also pertain~~s~~ to authorized users who access these linked databases.

Policies 1) WRITTEN POLICIES AND PROCEDURES, Page 2

Policies

1) WRITTEN POLICIES AND PROCEDURES

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

~~B.~~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) ORP, e.g, local public health authority (LPHA), Oregon Enterprise Technology Services (ETS), Tribal jurisdiction, etc. ~~ORP~~.

~~C.~~

Policies 2) OVERALL RESPONSIBLE PARTY Page 2

2) STATE OVERALL RESPONSIBLE PARTY

A. The state ORP for the security of Orpheus data is the CPHP~~enter 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 several ~~ten~~ 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 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 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

Policies 2) OVERALL RESPONSIBLE PARTY Page 3

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 authorized ~~CPHP Orpheus~~ users and answer any questions those users~~employees~~ might have about these policies and procedures.
6. Deactivate authorized users or AE 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. 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 Orpheus users 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 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.
    ~~a. ;~~
    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 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 ~~the department~~OHA, 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 approved entity (AE) ~~e.g., Local Public Health Authority (LPHA), Oregon Enterprise Technology Services (ETS), Tribal jurisdiction, etc.,~~ shall appoint an ORP for the security of Orpheus data within its agency. The ~~LPHA~~AE ORP or their designee shall:
   1. Authorize access for each AE ~~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 AE ~~LPHA~~ adherence to the security policies and procedures in this document upon request of the state ~~CPHP~~ ORP.
   5. Annually review these policies and procedures with all active ~~LPHA~~AE Orpheus users within the AE's jurisdiction and answer any questions those ~~employees~~ users might have about these policies and procedures.
      a. Annually provide a list of AE ~~LPHA~~ IT personnel who have privileged access to Orpheus data and their most recent date of AE ~~LHPA~~ security and privacy training.
   6. Request that ~~Direct~~ the state ORP or designee ~~to~~ de-activate users or ORPs who fail to ~~read,~~ sign~~,~~ and return to CPHP the following~~ir~~ agreements ~~to the following~~ within two months of receipt of a user-specific annual security audit~~s~~:
      a. User acknowledgement of familiarity with 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.

Policies 2) OVERALL RESPONSIBLE PARTY Page 5

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

As the need arises, exercise their right to implement ~~local~~ security policies that apply to users under its jurisdiction that are more stringent than these statewide Orpheus security policies and procedures.

8. Ensure that all Orpheus users 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 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 AE ~~LPHA~~ computer systems with viruses and other malware; and
c. limiting use of personal computers and storage devices to activities directly related to AE ~~LPHA~~ work in a manner consistent with all AE ~~LPHA~~ work and with common sense; and
d. limiting removal of data from secure facilities to circumstances that have been explicitly approved by an AE ~~LPHA~~ supervisor, AE ~~LPHA~~ ORP or a AE ~~LPHA~~ ORP designee and are otherwise consistent with this policy and with AE ~~LPHA~~ policy.
e. protecting mobile devices and storage from loss and theft; and
f. obtaining authorization prior to removal from secure ~~LPHA~~AE facilities.

9. Ensure that any PII sent from Orpheus in an e-mail is sent in encrypted form, using the encryption standard of the AE~~LPHA~~.
10. Ensure that Orpheus Users within the AE's jurisdiction ~~ir purview~~ meet at least annually with the ORP (or designee) to review each user's Orpheus Security Audit Report, including but not limited to, review of the current Orpheus Security Policies and Procedures document, Assurance of Confidentiality (User Oath), current user access privileges, Orpheus data export location(s), and agency-specific security policies.
11. The AE ~~LPHA~~ ORP or designee must notify the Orpheus Tech Team (Orpheus.ODPE-Tech@state.or.us) within seven days after an authorized user leaves their position.

Policies 3) Responsibilities And Requirements Page 5

A. Each ~~state and local public health professional~~user 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~~ user 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

Policies 3) Responsibilities And Requirements Page 6

http://www.oregon.gov/oha/OIS/ispo/Pages/policies.aspx.)

D. Each ~~person~~ user 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. Staff e.g., system administrators, who are not involved in public health data collection, case investigation or re (Ctrl) vities, ~~e.g., system administrators,~~ 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.

F. All authorized Orpheus users will be subject to periodic random audits of Orpheus logs performed by other 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 Page 6

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~~AE ORP or designee, or to the CPHP ORP, or to ~~the OHA Information Security and Privacy Office (ISPO)~~.
   2. 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. 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 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 a suspected 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 Page 7

A. Public Health Users

Record-level access without special approval shall be restricted to ~~public health user~~users authorized by the state ORP ~~CPHP~~ or an ~~LPHA~~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 ~~Once an individual has read~~ these policies and procedures and the individual must read these policies and procedures, sign~~ed~~ the confidentiality oath, and~~the user~~ return~~s~~ 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). If the user is approved, ~~W~~within a week the user will receive a Citrix ID number assigned by the Orpheus Tech Team, and using that ID number may obtain access to the Orpheus application from the Orpheus Team at OPHD. An authorized user's access to Orpheus is~~has been designed such that users are~~ restricted by the "privilege set" that the state ORP or AE ORP has authorized for an individual user based on the individual's role within their organization. "Privilege sets" ~~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 ar available in the FileMaker® software. The ~~LPHA~~AE, ~~or~~ state ORP or AE ORP, or designee~~s~~ assign ~~authorizes the assignment of~~ each user to one or more~~multiple~~ roles ~~of several available roles~~ based on whether the user is a ~~LPHA~~AE authorized user or a state authorized 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~~AE authorized user without prior notification to~~of~~ the ~~LPHA~~AE ORP or designee. An authorized user's p~~P~~rogram area and jurisdiction rights are~~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~~AE ORP, as appropriate. The state ORP or an AE ORP is~~s are~~ automatically notified of any changes to its~~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.~~
   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 Outbreak Only role is for managing the Outbreak database only. ~~Only one State user is given has this role.~~
   e. 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.~~.
   f. The Power User role ~~Only T~~two State ~~workers~~ is for higher-level users able to execute scripts view layouts, and modify value lists. ~~are given have the All Records+Scripts role~~.
   ~~f.~~g. The All Records + Scripts role allows for creating, editing and deleting of records, and modification of layouts, value lists, and scripts.

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.

5) DATA ACCESS AND USE Page 8

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, 24 users are designated as User Administrators, and all of these are state level users.~~

5) DATA ACCESS AND USE Page 9

c. The ~~LPHA~~AE 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. Authorized ~~Local~~non-State users may be granted case-record access to one or more disease groups by the local AE ORP or designee. The ~~local~~ AE ORP shall limit case-record access to those disease groups necessary for the user to complete their public health responsibilities.
f. Authorized non-State ~~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. Authorized 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. Authorized State users are permitted by the Orpheus software to access case records for all jurisdictions within disease groups to which they have been

5) DATA ACCESS AND USE Page 10

l. Any ~~LPHA~~AE may ~~elect~~ request to share all of its cases with any other ~~LPHA~~AE upon written request to the Orpheus State ORP from both ~~LPHA~~AEs (Appendix 2, Cross-jurisdictional agreement). However, access to cases of specific diseases by users of the cooperating ~~LPHA~~AEs still requires that the individual user have been granted access to the specific disease group.
m. When an LPHA approved user has a legitimate public-health need to view a case in another jurisdiction (e.g., contact tracing), the user may request transfer of the case from that jurisdiction. ~~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~~AE~~'~~s.

B) Authorized uses and disclosures Page 11

B. Authorized uses and disclosures

Authorized users 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.

If an individual, or an individual's authorized representative requests a copy of their own record in Orpheus, for example a disease outbreakform or a lab result, the

~~B. Record-level access—all others. The following are consistent with ORS 433.008 (https://www.oregonlegislature.gov/bills_laws/ors/ors433.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 LPHAAE may be approved by Orpheus ORP or by the LPHAAE 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 LPHAAE 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 LPHAAE ORP or designee is uncertain about whether all conditions for data access or release have been met, she may~~

B) Authorized uses and disclosures Page 12

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 Science & Epidemiology Council (SEC) meets regularly to consider such topics. The OHA ISPO is another resource for this purpose. These resources shall also be available to a LPHAAE 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 LPHAAE ORP in the case of requests for data involving residents of a single LPHAAE 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, assure that the data will be stored in a secured area, and agree 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 LPHAAE ORP for publications involving residents of a single LPHAAE or the Orpheus State ORP or their designee for publications involving more than one LPHAAE 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.

Authorized uses and disclosures.

Public record requests.

a. Public record requests will be processed through Orpheus via a "Public Records Request" button located within the Orpheus Case Record. An auhorized user LPHAAE personnel 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.

~~a.~~ 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. R

~~C. Aggregate level access – everyone.~~

~~1. Any person may obtain published summary or published aggregate de-identified data upon request, as allowed under ORS 433.008 (https://www.oregonlegislature.gov/bills_laws/ors/ors433.html).~~

~~2.~~ Release of any report or information must ~~aggregate data shall~~ be consistent 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. An authorized user

~~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~~AE ORP or the ~~Orpheus S~~state ORP if they are uncertain whether a ~~the requested~~ release is compliant with state law and this ~~program~~ 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 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 state or AE ORP or their designees.
2. A limited-access, physically secure surveillance area shall be available ~~and maintained by~~to authorized 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~~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

6) DATA SECURITY page 13

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 state or AE ORP or their designees.
2. A limited-access, physically secure surveillance area shall be available ~~and maintained by~~to authorized 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~~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

6) DATA SECURITY page 14

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~~Orpheus~~ ORP in the case of state-level surveillance areas or the ~~LPHA~~AE ORP in the case of surveillance areas overseen at the ~~LPHA~~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.

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 ~~Orpheus~~ ORP or ~~LPHA~~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 ~~ISPO approved~~ vendor, e.g. assuring that all data are inaccessible or destroyed in the process.

6) DATA SECURITY page 15

f. Unless explicitly authorized by the Orpheus ORP, ~~LPHA~~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 Orpheus ORP for DHS personnel or affiliates or the ~~LPHA~~AE ORP for ~~LPHA~~AE personnel or affiliates or their designees.

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, when possible. 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~~AE ORP.
   ii. Computer servers or workstations storing confidential data must be physically and electronically protected in a manner completely consistent

Definitions page 16

User changed to authorized user (see below)

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.

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).

Appendix – Disaster Recovery page 17

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~~ 60 minutes) to minimize loss of data. Additionally, the Orpheus FileMaker Pro® Server has the following back up schedule in place:

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

Recovery Point Objective (RPO) – ~~30~~ 60 minutes. Orpheus leverages FileMaker Server 12 technology and automatically conducts a progressive backup every 30 minutes.

July 4, 2020

(Overview)

Removed Citrix refrence based on ISPO recommendation.

The Orpheus computer application and its data are 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 OHA, Oregon Public Health Division (OPHD), Center for Public Health Practice (CPHP). All surveillance data contained within Orpheus are owned by OHA.

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)
xvi. Pertussis;
xvii. STD (Gonorrhea & Chlamydia);

July 26, 2021

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;

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*). ~~Furthermore, Orpheus leverages native FileMaker Pro® progressive backup processes throughout the day (every 60 minutes) to minimize loss of data.~~ Additionally, the Orpheus/Opera FileMaker Pro® Servers haves 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. Orpheus/Opera leveragess FileMaker Server ~~12~~ 18 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.

August 10, 2021

1. Roles (privilege sets):

a. ~~The~~ **Citrix – Orpheus**: Standard non-state user (access restricted by jurisdiction and disease group)~~Full Access role allows the AU to view all records, manage privilege sets (including creating new accounts), edit data tables, create new fields, etc~~.

~~a.~~

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)

~~b. The Super User role allows state AUs to modify layouts, and scripts, but does not allow field creation.~~

~~c.~~ **Citrix – Orpheus Super User:** Tech Team state user (enhanced system functionality) ~~The Orpheus All Data role allows state AUs to do advanced functions like merge people, but cannot modify layouts or scripts. Not limited by disease group.~~

d. **Citrix – Opera**: Standard non-state user (access restricted by jurisdiction and disease group)

~~d. The Orpheus Read Only role allows read-only access to Orpheus.~~

e. **Citrix – Opera State**: Standard state user (access restricted by disease group)

~~e. The County Data Entry role allows county AUs to enter and edit data about cases, providers and facilities, and run pre-formatted reports. All County AUs have this role.~~

~~f.~~ **Citrix – Opera Super User:** Tech Team state user (enhanced system functionality) ~~The Outbreak Only role is for managing the Outbreak database only.~~

f. **Citrix – Dude**, which is an application launcher, will automatically provides access to the appropriate outbreaks databases, such as Outbreaks, and Opera Outbreaks.

July 21, 2022

Added Orthopox disease group.

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*). ~~Furthermore, Orpheus leverages native FileMaker Pro® progressive backup processes throughout the day (every 60 minutes) to minimize loss of data.~~ Additionally, the Orpheus/Opera FileMaker Pro® Servers haves 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. ~~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.