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 CPHP ORP**;

(Section 4 B 1) Breaches of Confidentiality
Revised: All must be reported ~~immediately~~ **within one working day** to **the** CPHP 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 CPHP ORP within 14 days after an authorized user leaves their position. The CPHP 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.

(Policies|Overall Responsible Party|2B)

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;
    ~~, 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~~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 _____

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

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

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

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

User: a person with a valid Orpheus account.

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

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 90 minutes) to minimize loss of data.

Recovery Point Objective (RPO) – 90 minutes. Orpheus leverages FileMaker Server 12 technology and automatically conducts a progressive backup every 90 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.