Oregon ESSENCE

Confidentiality Policy

I. Background

Oregon Electronic Surveillance System for the Early Notification of Community-Based Epidemics (ESSENCE) is a statewide syndromic surveillance system. ESSENCE is a web-based application created by the Johns Hopkins University Applied Physics Laboratory that is designed to detect significant patterns in illness and injury from non-traditional or pre-diagnostic sources of data, including emergency department, urgent care and communicable disease reporting records. ESSENCE is used across the country by infection prevention, emergency department (ED), and other healthcare professionals, along with public health professionals at the local, state and federal levels. Data elements available in Oregon ESSENCE include patient-level clinical and demographic variables.

II. Purposes of Confidentiality Policy

This Confidentiality Policy is intended to establish the conditions for use and reporting of syndromic surveillance data in Oregon. Although names, birthdates, and other unique identifiers are not collected in the system, patient zip code, patient city/town of residence, and patient medical record number are collected and may potentially be used to identify individuals. Therefore, these data are considered confidential, and access to them is maintained by this Confidentiality Policy. Under this policy, confidentiality is concerned with how the information provided to ESSENCE is accessed, stored, used and shared with others.

III. Authorized Users and Partnering Entities

A. Partnering Entities

For the purposes of the Oregon ESSENCE Confidentiality Policy and Agreement, "Partnering Entities" are considered to be healthcare facilities, health systems or other organizations that provide data to Oregon ESSENCE.

B. Authorized Users

Individuals meeting the criteria below are considered (in this Confidentiality Policy and Agreement) to be "Authorized Users" and may request access to ESSENCE:

1. Oregon Health Authority (OHA) and Oregon local public health authority (LHPA) employees or contractors.

2. Tribal, and other state and LPHA employees or contractors.

3. Employees of Partnering Entities.

4. CDC or its subcontractors for use in the national BioSense System.

5. Johns Hopkins University's Applied Physics Laboratory (JHU/APL), under U.S. government contract number N00024-03-D-6606/0116, for further development of the Early Notification of Community-Based Epidemics (ESSENCEII) System.

6. Employees, students or contractors of academic institutions in Oregon.

C. Requesting Access

1. Authorized Users must read the Oregon ESSENCE Confidentiality Policy and Agreement and send the signed Agreement to the Oregon ESSENCE Program at Oregon.ESSENCE@state.or.us.

2. Instructions for logging in and changing passwords will be sent to Authorized Users via secure e-mail within two weeks of this request. Signed agreements are kept on file by Oregon ESSENCE.

IV. Confidentiality

Information in Oregon ESSENCE is understood to be confidential in accordance with Oregon Revised Statutes 433.008 and 432.060(1).

V. Minimum Necessary Standards

To the extent use and disclosure of information in Oregon ESSENCE by Authorized Users is authorized, such use and disclosure must be the minimum necessary as that is defined in Oregon Administrative Rule (OAR) 943-014-0040:

> "'Minimum Necessary' means the least amount of information, when using or disclosing confidential client information, that is needed to accomplish the intended purpose of the use, disclosure, or request."

VI. Accessing and Viewing Data

A. Accessing Data

1. Account access to Oregon ESSENCE is granted to individuals only – not to clinics, hospitals or healthcare facilities.

2. If no user activity is documented for 90 days, access will expire and will need to be re-requested by sending an email to Oregon ESSENCE (Oregon.ESSENCE@state.or.us) to unlock the account.

B. Login and Password

1. After an initial password is assigned by Oregon ESSENCE, Authorized Users should log into the system and change their password. Authorized Users will be prompted to change their password at regular intervals (90 days or more frequently).

2. Authorized Users are prohibited from sharing their username and password with any other individual or entity, including co-workers. Violations of username login and password security will result in revocation of the user's access and may result in the termination of access for all Authorized Users at the user's organization or facility.

C. Viewing Data

1. All computer workstations, desktop computers, laptop computers and other portable storage devices used to access, transfer or store Oregon ESSENCE data must be controlled by unique user identification and passwords.

2. When leaving an area where Oregon ESSENCE is being accessed or Oregon ESSENCE data viewed or analyzed, Authorized Users must lock access to their computers (e.g., by using <Ctrl><Alt><Del> on a PC), regardless of how quickly they intend to return.

3. Each workstation that accesses Oregon ESSENCE must be configured so that it reverts to screen-saver mode no more than 5 minutes after last activity, and requires a password to resume activity.

VII. Limitations on Data Access

A. Role-based Access

Authorized Users will access Oregon ESSENCE according to their role:

1. Healthcare Authorized Users will have record-level access to data from their own health system and aggregate data from the rest of the state.

2. LPHA Authorized Users will have record-level access for residents of their county and EDs in their county and aggregate data from the rest of the state. If these users have reportable disease data access through Orpheus, they can request access to these data in ESSENCE as well.

3. OHA Authorized Users will have statewide record-level access. If these users have reportable disease data access through Orpheus, they can request access to these data in ESSENCE as well.

B. Project-based Access

1. Tribal public health agency Authorized Users will be granted Oregon ESSENCE access according to the scope, timeframe, region and variables of the approved project.

2. Academic institution Authorized Users will be granted Oregon ESSENCE access according to the scope, timeframe, region and variables of the approved project.

C. Discrepancies

1. User access will be periodically checked through an auditing process by the Oregon ESSENCE Program.

2. Authorized Users are responsible for checking their access in Oregon ESSENCE and reporting any discrepancies as soon as possible to the Oregon ESSENCE Program.

VIII. Data Management and Security

Authorized Users must employ appropriate safeguards to protect the security of the data and prevent access to them for any purpose not expressly permitted by this policy.

A. Data storage

1. All exported Oregon ESSENCE data must be stored on workstations, laptops, secure networks, removable hard drives or external devices that are password-protected.

2. Laptop computers, removable hard drives or external storage devices containing ESSENCE data must be locked in a secure cabinet when not in use.

3. All external storage devices must be encrypted using real-time FIPS 140-2 compliant encryption using an AES 256-bit encryption or its equivalent. Decryption keys must not be stored on or with the portable device.

4. Oregon ESSENCE data stored on portable devices must include no more than the minimum amount of information necessary to accomplish assigned tasks.

5. Any compromise of data or loss of hardware containing sensitive data will be managed as a data breach. The Information Security and Privacy Office will be alerted for all such data breaches and will be the primary security office for managing such incidents with OHA employees.

B. Encryption

All transmissions of Oregon ESSENCE data outside of the OHA network must be transmitted in a secure manner. Acceptable technologies for transmission include: HTTPS using Secure Sockets Layer (SSL) or Transport Layer Security (TLS), secure file transfer protocol (sFTP), secure virtual private networks (VPN), secure email, or other FIPS 140-2 compliant technology.

C. Disposition/Destruction of Data

Exported data must be destroyed after use or 6 months after export, whatever comes first regardless of where they are stored. Use of file shredding or file wipe utilities should be considered for highly sensitive data.

IX. Permitted Use

Authorized Users are not allowed to use Oregon ESSENCE data (including running reports, viewing data or any other activity that requires accessing the interface) other than as authorized in this policy or required by law.

A. Permitted Uses

1. To facilitate the interchange of information that can be used to coordinate responses and monitor events routinely and during a potential health event.

2. For early detection and characterization of events (or health-related threats) by building on state and local health departments systems and programs.

3. To provide health-related information for: (i) public health situation awareness, (ii) routine public health practice, or (iii) public health evaluation.

4. To improve the ability to detect emergency health threats by supporting the enhancement of systems to signal alerts for potential problems in collaboration with federal, state and local health jurisdictions and other potential stakeholders.

5. Participating Entities are allowed to use their own data for quality assurance, business improvement or other purposes.

B. Data Identification

Authorized Users SHALL NOT:

1. Disclose any information that may allow identification of individuals represented in the data. This includes not disclosing information that might identify healthcare providers, physicians or other healthcare personnel.

2. Use the identity of any person or entity discovered inadvertently.

C. Linking

Authorized Users must complete an ESSENCE project proposal before linking data in the ESSENCE system to any other source.

X. Restrictions and Conditions of Reporting

A. Oregon ESSENCE Data Dissemination and Reporting

The following types of data are NOT allowed to be disseminated or reported:

1. Patient-level data (individual records).

2. From DHS-100-107:

"I. Names;

II. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geo codes. However, the initial three digits of a zip code may remain on the information if, according to current publicly-available data from the Bureau of the Census, the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and the initial three digits for all such geographic unit containing 20,000 or fewer people is changed to 000;

III. All elements of dates (except year) for dates directly relating to an individual, including birth date, dates of admission and discharge from a health care facility, and date of death. For persons age 90 and older, all elements of dates (including year) that would indicate such age must be removed, except that such ages and elements may be aggregated into a single category of 'age 90 or older;'"

"VIII. Medical record numbers" … or, "Any other unique identifying number, characteristic, or codes, except as permitted under Section (3.) of this policy…"

3. Data from a sole health care facility or health care system (reports must aggregate data from two or more health systems).

B. Re-release/Secondary Use of Data

Authorized Users are not allowed to release nor permit others to release the data or any part of them to any non-authorized users.

C. The following categories of users must submit a proposal request to Oregon ESSENCE:

1. Any user who wishes to report, present or publish ESSENCE data

2. Any user who wishes to re-release or share ESSENCE data outside of a public health authority, hospital or health system

3. Any user who is an employee, student or contractor of an academic institution (regardless of plans to release or publish data)

4. Any user who is submitting an IRB proposal

See ESSENCE proposal guidelines for detailed information about submitting a proposal.

XI. Responsibilities and Consequences of Violation of Agreement

A. Responsibilities

1. Authorized Users accept full responsibility and liability for any violations of this policy.

2. Authorized Users must report any breach of this policy to the Oregon ESSENCE Program within 48 hours to Oregon.ESSENCE@state.or.us.

B. Consequences

1. In the event an Authorized User fails to comply with any of the terms of this policy, the Oregon ESSENCE Program has the right to immediately revoke the Authorized User's access, at the sole discretion of the Oregon ESSENCE Program staff. User privileges may also be revoked for all other users at the same organization.

2. Civil and criminal penalties may also apply; in addition, OHA and Department of Human Services (DHS) employees are subject to disciplinary action up to and including dismissal from state service. See DHS|OHA policy, DHS|OHA-090-005.

XII. Termination of Authorization

A. It is the responsibility of the Oregon ESSENCE Account Manager to notify the Oregon ESSENCE Program by e-mail (Oregon.ESSENCE@state.or.us) within five business days when an individual no longer needs access to Oregon ESSENCE.

B. Oregon ESSENCE Authorized Users must agree to maintain the confidentiality of Oregon ESSENCE data, as specified in this Confidentiality Policy and Agreement, even after they no longer have access to Oregon ESSENCE.

XIII. Review of Confidentiality Policy

The manager for Oregon ESSENCE will review and revise this policy as needed, but not less than annually. The review of this policy will include consultation with the Oregon ESSENCE Advisory Team.

Oregon ESSENCE Contact Information: **Oregon.ESSENCE@state.or.us or 971-673-1111**

Oregon ESSENCE
Confidentiality Agreement

I understand that I have access to confidential information in the Oregon ESSENCE system. This information consists of emergency department and urgent care clinic records or Oregon reportable disease records (Orpheus) records. By signing this statement, I acknowledge that I understand my responsibility to protect this information and agree to the following:

- I have carefully reviewed and will remain familiar with all confidentiality policies described in the Oregon ESSENCE Confidentiality Policy (referred to as "the Policy").
- I will adhere to all security policies and procedures described in the Policy.
- I will access information only for the purposes described in the Policy.
- I will release information only as permitted in the Policy.
- I will not discuss confidential information found in Oregon ESSENCE with unauthorized individuals.
- I will immediately report any suspected breach to the Oregon ESSENCE Program staff.
- I will maintain the confidentiality of these data as specified in the Policy even after I no longer have access to Oregon ESSENCE.
- I will consult with Oregon ESSENCE before publishing or reporting these data.

Failure to abide by this agreement may result in immediate termination, suspension, or revocation of access to Oregon ESSENCE for yourself and other Authorized Users at your facility.

**********Complete all areas below to request access to ESSENCE **********

1. Data request details.

Data Source	Requesting access?	What do you intend to do with access to ESSENCE? *Describe in the space below*	How long do you need access? *Project end date*
Emergency Departments & Urgent Care Clinics	☐ **Yes** ☐ **No**		
Orpheus *Current Orpheus users only*	☐ **Yes** ☐ **No**		

2. Do you plan to publish or report these data? ☐ **Yes** ☐ **No**

3. User Details

Name:	**Job title:**
Phone number:	**Email:**
OR# or P# *(if you have one)***:**	
Are you a contractor for this Partnering Entity, LHD, or OHA? ☐ **Yes** ☐ **No**	

4. Authorized User signature: _____ **Date**:_____

Request initiated: Initials Date Notes

Access verified: Initials Date Notes