



ODRS Usage/Training

Original Effective Date:

8/3/2017

Review / Revision Date:

8/3/2017

TLCHD Procedure:

2017.08.049

Maintenance Steward: Epidemiology Supervisor

History: ☒ New ☐ Revised ☐ Archived

Organizational Scope:

☒ Full Agency ☐ Administration ☐ Community Services ☐ Environmental Health ☐ Health Services

Frequency of Review:

☐ Annually ☒ Biennially ☐ 5 Years ☒ As Needed ☐ Other:

Location:

S-Drive: S: → Users → Common → Policies & Procedures

Website: www.lucascountyhealth.com/employee-login/

Hardcopy: Environmental Health and Community Services Director's Office

Archived Version(s):

Requisite Signatures

☒

Medical Director

8-7-17

Date

☒

Health Commissioner

08-08-17

Date

☒

Director of Environmental Health & Community Services

8-4-2017

Date

☒

Director of Health Services

8-4-17

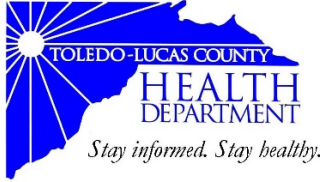
Date

☒

Director of Human Resources

8-7-17

Date



ODRS Usage/Training

I. Policy

It is the policy of the Toledo-Lucas County Health Department (TLCHD) to adhere to all state, federal, and local statutes governing the management and case investigation of individual communicable disease cases and outbreaks within Lucas County.

II. Scope

This procedure/process applies to any/all individuals that utilize or have access to the Ohio Disease Reporting System (ODRS) through the Ohio Department of Health Application Gateway.

III. Purpose

This procedure/process establishes guidelines for appropriate usage of ODRS for infectious disease investigations. Per the Ohio Administrative Code (OAC) 3701-3-06, diseases specified as Class A, B, or C shall be reported to the Ohio Department of Health. The formal mechanism for confidential reporting of infectious disease cases is through the utilization of ODRS.

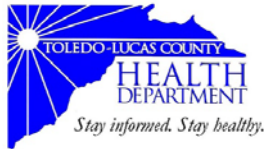
IV. Background

The Ohio Disease Reporting System (ODRS) provides real-time secured access for state and local public health practitioners to report infectious diseases. ODRS allows local health departments with jurisdictional responsibility and relevant ODH program staff to have immediate access to infectious disease reports on a 24/7/365 basis for disease control and disease surveillance purposes. This assures cases of significant public health importance receive immediate attention and public health response. Infection preventionists, individual health care providers and laboratories can also become ODRS users for infectious disease reporting purposes.

ODRS is used by local health departments (LHDs) to report infectious diseases to the Ohio Department of Health (ODH). Class A diseases should also be reported to ODH immediately by phone.

Each LHD has an administrator (and a backup) who sets up access to ODRS for LHD employees in their jurisdiction. ODH sets up users as LHD administrators upon receipt of a fully completed and approved LHD Administrator Agreement. LHD administrators add and remove ODRS user accounts and assign role and program group rights. LHD administrators review user rights on a regular basis to ensure appropriate access to ODRS. ODH recommends LHD administrators have ODRS User Agreements on file for all ODRS users for whom they are the LHD administrator.

When ODRS was rolled out in February 2006, ODH conducted a series of train-the-trainer trainings. Each LHD has a designated trainer within their jurisdiction or region. LHD trainers are responsible for training users in their jurisdiction or region. An online manual is also available in ODRS Help.



ODRS Usage/Training

V. Procedure

A. Obtaining Access to ODRS

- A. TLCHD employees requiring access to ODRS for their position shall request access to ODRS through the LHD Administrator.
 - a. The LHD Administrator reviews user rights on a regular basis to ensure appropriate access to ODRS and also retains ODRS User Agreements on file for all users for whom they are the LHD administrator
 - b. The LHD Administrator verifies that the employee is required to have access to the data system, verifies the needed roles that the employee will be assigned to, and ensures access to ODRS is established for the employee
 - c. TLCHD has a number of staff that have extensive experience with ODRS and therefore can serve as a trainer for the employee.

B. Confidentiality

- A. Security and confidentiality are a matter of concern for all users of the Ohio Disease Reporting System (ODRS) and for all other persons who may have access to data from the system. Every individual who is authorized to access ODRS holds a position of trust relative to this information and must recognize the responsibilities entrusted to him/her in preserving the security and confidentiality of this information. The information is collected for public health disease control and disease surveillance. Information in ODRS, including information that could be used to identify an individual and his or her health status, is considered confidential information. Confidentiality requirements that apply to these data include, but are not limited to ORC Section 3701.17. City or county regulations or ordinances or other laws may place additional restrictions on data use and release.
- B. The inappropriate behavior of an authorized user may threaten the security and confidentiality of this information. ODRS users shall know, understand, and adhere to the following requirements:
 - a. Users must not make or permit unauthorized use of any information in ODRS.
 - b. Users may not exhibit or divulge the contents of any record, except as permitted under Ohio Revised Code and Ohio Administrative Code, for public health activities for disease control and disease surveillance.
 - c. Users must not intentionally input false, inaccurate, or misleading information into ODRS or knowingly allow the input of such information into ODRS.
 - d. Users must not remove or cause to be removed any copies of records from ODRS except in the performance of their public health duties.
 - e. Users must not divulge or share security codes or user authorizations.
 - f. Users must not violate rules and regulations concerning ODRS access or improperly use passwords and user authorizations.
 - g. Users must not access, request others to access, or allow others to access ODRS for non-public health purposes.



ODRS Usage/Training

- h. Users must not seek to benefit personally or permit others to benefit personally by any confidential information in ODRS.
- i. Users must not aid, abet, or act in conspiracy with another to violate any part of this code.
- j. Authorization for access to ODRS terminates when a user's employment is terminated or when access to the data is not required for work related responsibilities.
- k. Users have an obligation to protect the confidentiality and security of the information in ODRS.
- l. Users must report any violations of this ODRS confidentiality and security code to the ODH Information Security Officer immediately.

VI. Maintenance

A. Review

- a. The Infectious Disease standard operating procedures are to be reviewed every other year or as needed to ensure compliance with both agency and accreditation standards.
- b. If guidance/recommendations from the Centers for Disease Control, Ohio Department of Health or law changes regarding this infectious disease, TLCHD will follow the most up-to-date guidance and adjust the SOP(s) as needed.

B. Revision

- A. All changes made to this SOP are to be noted on the **Record of Change**. Substantial changes will require renewed signatures from all applicable parties. This includes changes to the intent, scope, procedures, or policy statement.
- B. Changes in style, format, grammar or minor error correction will not require renewed signatures but must be indicated on the Record of Change.

