

SECURITY, PRIVACY, AND CONFIDENTIALITY RULES OF BEHAVIOR FOR USERS OF COMMUNICABLE DISEASE UNIT DATA AND CASE MANAGEMENT SYSTEMS

Purpose: The purpose of this document is to provide Communicable Disease Unit (CDU) data and case management system users with guidance related to the surveillance, collection, reporting, treatment, reimbursement, and case management of communicable disease patients, partners, and contacts as it relates to statutory reporting and CDU-funded reimbursement programs. Additional policies and practices may be appended and added at any time if required by federal, state, or local law, as required for specific reporting data, in accordance with federal funding guidance, or as deemed otherwise necessary. This document fulfills the requirement to complete an Acknowledgement to Receipt of Training and Expectations for CDU data and case management systems.

Definitions:

Clinic: A private or public health agency where employees are authorized to use one (1) or more of the CDU data and case management systems on behalf of the Clinic

Communicable Disease Unit: The Wyoming Department of Health, Public Health Division, Public Health Sciences Section, Communicable Disease Unit

Unit Data System (UDS): Any CDU data and case management system that is used for the purpose of surveillance, collection, reporting, treatment, reimbursement, and case management of communicable disease patients, partners, and contacts as related to Human Immunodeficiency Virus (HIV) counseling and testing data, HIV case management data, reportable positive viral hepatitis (Hep B or C), sexually transmitted diseases (STDs) (e.g. chlamydia, gonorrhea, syphilis), and tuberculosis records (i.e. PRISM, CAREWare)

UDS Administrator: The CDU staff member in charge of data management for the data or case management system. This person is identified to the User(s) during authorization and orientation to the UDS

User: The individual public health stakeholder(s) who have been authorized or are seeking authorization to utilize one (1) or more of the CDU's data and case management systems

Policy:

CLINIC RESPONSIBILITIES

Clinics are responsible for: **notifying the UDS Administrator of personnel changes.** □

Clinics utilizing a UDS for collecting, reporting, treatment, reimbursement, case-management, or follow-up of HIV counseling and testing data, HIV case management data, reportable positive viral hepatitis (Hep B or C), STDs, and tuberculosis records must notify the UDS Administrator as soon as it becomes known that a User:

- Is changing duties within the clinic such that it would affect their need for access to the UDS; or
- Has breached UDS policy; or
- Is terminating employment or is being terminated from employment with the clinic.

This is critical to ensuring that proper action is taken to protect and maintain the system and its data from potential misuse or unauthorized access.

Clinics are responsible for: **overseeing data within their purview.**

Data collected by the Clinic that are not housed within a UDS, such as client medical records, forms, clinic notes, and/or electronic records may be used for the collection and maintenance of confidential client information. The CDU is not responsible for, or required to oversee, handling of such clinic level data except as entered into a UDS to fulfill reporting and/or reimbursement requirements. Clinics must have policies in place to prevent the misuse, loss, or incorrect disposal of these forms of data, to include procedures for the use, storage, transmission, and disposal of each medium used.

The use of equipment to transmit confidential information (e.g. e-mail, photocopiers, facsimile machines, internet connections) must be regulated by written policies and procedures at the clinic level.

UDS data must never be exported to external storage media, removable media (e.g. zip drives, thumb drives, flash drives, compact discs), or system hard drives.

Clinics are responsible for: **taking precaution against unauthorized intrusion.**

Clinics must have plans and processes to prevent unauthorized penetration of Users' workstations (e.g. hackers, computer viruses, computer worms, malware). Reasonable precautions would include firewalls, currently updated anti-virus software, back-up copies of the workstation, and/or training staff in basic computer security concepts (e.g. not downloading materials from unknown e-mail senders or websites, blocking access to websites identified as potential hosts for these kinds of attacks, opening suspect e-mails from unknown senders).

Clinics are responsible for: **reporting misuse, breaches, and suspected incidents.**

Clinics must comply with all stated usage requirements, taking due care and reasonable precaution in the management and protection of system data.

Access to the UDS is restricted to authorized users only. Suspected incidents, security breaches, misuse, or unauthorized access must be reported promptly to the UDS Administrator for evaluation.

Clinics who utilize a UDS for the collection, management, reporting, reimbursement, case-management or follow-up of communicable disease(s) who do not comply with these Rules of Behavior may be subject to federal, state, local, and department level penalties that can be imposed under existing policy including, but not limited to, reprimands, suspension or termination of system privileges, fines, or criminal or civil prosecution.

All data system requests for release of UDS information are handled by the Wyoming Department of Health and clinics must refer any such requests to the designated administrator of the particular UDS for evaluation and appropriate processing.

USER RESPONSIBILITIES

Each User is responsible for: **helping to prevent unauthorized use of and access to system resources.**

This duty includes complying with all stated Rules of Behavior requirements, taking due care and reasonable precaution when handling system data or using system resources, and the management and protection of system

authentication controls (user ID and password). When in doubt, Users are strongly encouraged to contact the UDS Administrator for additional guidance.

Users of the UDS are only permitted to access:

- Data which are specific to their clinic or facility; or
- Data used for case management, treatment, or follow-up for clients and clients' partners; and/or
- Data assigned by CDU staff.

Prohibited uses of a UDS and its resources include, but may not be limited to:

- Copying, releasing, or viewing data without authorization or permitted access; and/or
- Altering data improperly, falsely, or otherwise tampering with system resources

Each User is responsible for: **maintaining control of their identity.**

User credentials are used to confirm user identity when logging into the UDS. Passwords must be changed periodically as prompted by the UDS, or as required to ensure privacy, security, and confidentiality. The UDS will default to a password change every ninety (90) days.

User IDs and passwords must not be shared among non-authorized staff. If non-authorized staff and users share a common workstation (computer), user ID and password must not be stored on the workstation. Password caching (automatic fill-in of password by the computer operating system or web browser) must be disabled on any workstation that accesses personally identifiable information.

Each User is responsible for: **maintaining their authorization.**

Each User will complete the UDS Rules of Behavior and UDS training, and sign an Acknowledgement of Receipt of Training and Expectations before given access to the UDS.

This Acknowledgement will provide the user with:

- Information on State statutes regarding the requirements to collect and maintain confidential information for public health purposes;
- Possible ramifications for misuse or disclosure of confidential information and/or PHI; and
- Acknowledgement of receipt, review, and understanding of State statutes, ramifications, and CDU expectations of privacy, security, and confidentiality.

This Acknowledgement will remain on file with the clinic and will be faxed/scanned to the UDS Administrator to be kept on file with verification of successful training completion and User authorization.

Each User will be expected to complete unit-specified training prior to authorization and sign a new Acknowledgement annually (as identified by the UDS administrator) to ensure a current list of authorized Users is available, as well as to maintain contact with users.

Each user is responsible for: **protecting confidential information in their care.** □

Access to a UDS is restricted to authorized Users only. Suspected incidents, privacy and security breaches, misuse, or unauthorized access must be reported promptly to the UDS Administrator for evaluation.

- If breach/incident involves personally identifiable information (names, addresses, phone numbers, dates, etc.) contact the UDS Administrator **immediately** upon discovery. These kinds of breaches will be reported to the CDC Information Systems Security Officer (ISSO) and Wyoming Department of Health Office of Privacy, Security, and Contracts staff for additional processing.
- All other suspected incidents/breaches (e.g. possible virus, hacker, password divulgence, failure to follow secure storage procedures) must be reported within **one (1) hour** of discovery. The UDS Administrator will process cause, implementation of process improvement, and determination if additional action is warranted, in addition to contacting the necessary authorities.

Workstations used for access of the data system must:

- Have screensaver locks that will automatically engage when the computer is not in use for a set period;
- Be manually locked by Users when they leave their desk/workstation (Ctrl+Alt+Del or the Windows Button + L); and
- Require User ID and password to unlock the workstation.

Each User is responsible for: **their own actions.** □

There is no expectation of privacy while using and accessing the UDS and its data.

The UDS Administrator may periodically monitor both system and user activities for the purposes of troubleshooting, performance assessment, usage patterns, indications of attack or misuse, and for the investigation of complaints or suspected privacy or security incidents/breaches.

Users who do not comply with these Rules of Behavior may be subject to federal, state, local and department level penalties that can be imposed under existing policy which may include reprimands, suspension, termination of system privileges, suspension or termination from duty, fines, jail time and/or criminal or civil prosecution.

Data must not be released for any purpose not previously approved by the Director of the Wyoming Department of Health through the CDU Manager, and directly related to the facilitation of federal, state, and local public health missions. The Wyoming Department of Health handles all data system requests for release. Users must refer any such requests to the UDS Administrator for evaluation and processing.

Please proceed to the final page and sign that you have read, understand, and agree to uphold these Rules of Behavior as they pertain to the use of CDU data and case management systems.

ACKNOWLEDGEMENT OF RECEIPT OF TRAINING AND EXPECTATIONS:

All data contained within the CDU data and case management system(s) are the property of the Wyoming Department of Health, Public Health Division, Public Health Sciences Section, Communicable Disease Unit. Its sole purpose is for the surveillance, collection, reporting, treatment, reimbursement, and case management of communicable disease patients, partners, and contacts in an ongoing effort to improve local community health and outcomes pursuant to Wyo. Stat. §§ 35-1-240, 35-4-107, and 35-4-108 (see <http://legisweb.state.wy.us/LSOWeb/wyStatutes.aspx>).

Any other use of these data is prohibited and can result in suspension or termination of access to the CDU data and case management system(s), as well as fines and/or imprisonment under the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Health Information Technology for Economic and Clinical Health Act (HITECH) of 2009.

Signing this document acknowledges clinic personnel who are granted access to the CDU data and case management system(s) have been trained in the appropriate use of these data as well as proper privacy, security, and confidentiality practices, and will abide by these Rules of Behavior.

All Communicable Disease Unit data system Users and Clinics are responsible for:

- **KNOWING THESE PRIVACY, SECURITY, AND CONFIDENTIALITY REQUIREMENTS;**
- **CHALLENGING UNAUTHORIZED USERS AND PROTECTING UDS DATA; AND**
- **REPORTING POTENTIAL PRIVACY AND SECURITY INCIDENTS/BREACHES.**

I, the undersigned, understand my responsibilities as set forth in this document regarding utilization of Communicable Disease Unit data systems. As an authorized User of the CDU data system, I will adhere to these Rules of Behavior.

Printed Name: _____ Date: _____

Signature: _____

Title: _____

Name of Clinic: _____

E-mail Address: _____

Please check User access AND/OR role(s):

- PRISM Communicable Disease Unit Data System Basic User
- Clinic Main Contact (Primary or sole PRISM User)
- CAREWare Case Management System