HIV/STD/Hepatitis Program Confidentiality and Security Policies and Procedures for Client-level Data

Updated May 2022
Becoming a Secure User

A secure user is a staff member or volunteer of a grantee organization of the Vermont Department of Health (VDH) HIV/STD/Hepatitis (HSH) program who will have access to client-level data for the purposes of collecting, processing, or analyzing that data.

In order to be authorized to be a secure user, you must:

- Review this slide set
- Take the Confidentiality and Security quiz
- Review the correct answers to assure you understand any errors
- Sign a secure user confidentiality statement
Client-level Data

Client level data is:

• Any record containing constructive identifying information

• Information collected about a particular client while the client is engaged with or enrolled in your program

• Examples include client name and date of birth, client demographics (race, ethnicity, gender, etc.), client risk behaviors (whether the client has had sex or used injection drugs during a certain period of time)
Constructive identifying information is any single piece of information or combination of several pieces of information from information collected by a VDH HSH-funded program that could be used to deduce the identity of an individual (e.g. names or pieces of names, date of birth, addresses, zip codes, telephone numbers, ethnicity, gender)
Client-level Data

Client-level data records can consist of:

- Paper records – ex. client-level data that is on a data collection form

- Electronic records – client-level data stored electronically (most likely on a computer)

- Portable electronic records – client-level data stored on portable electronic devices such as laptops, smartphones, or on removable storage media such as a flash drive
Confidentiality

Confidentiality is the disclosure of personal information in a relationship of trust and with the expectation that it will not be divulged to others in ways that are inconsistent with the original disclosure.

After learning what client-level data is, you can see how it could be possible to use this data to identify a particular client. For this reason, it is very important that this data be kept confidential in order to protect client privacy.
Securing Client-level Data

When client-level data is not being used, it must be stored in a secured area. A secured area is a locked file cabinet or other locked receptable within a room that has floor-to-ceiling walls and a door with a lock.

For the purposes of talking about client-level data, a secured area would be a room with floor-to-ceiling walls and a door with a lock.

Secured areas must be locked when the secure user is not present.
Securing Client-level Data – Passwords, Keys, etc.

As a secure user, you are responsible for protecting any keys, passwords/codes, or electronic devices that would give a person access to client-level data. All of these must be kept in a locked location.

If you discover that a password has been stolen or become known to another person, notify your supervisor immediately. This would be a security breach.
Securing Client-level Data - Computers

If client-level data is stored on a computer, the computer must:

• Have an automatic screen saver lock with a 15 minute or less activation time
• Be password protected (you need a username and password to unlock the screensaver)
• Be locked at all times when not in use
• Be located in a secured area
• Be protected by surge suppressors and emergency battery power to prevent data loss in case of power fluctuations
Securing Client-level Data - Visitors

If a person who is not a secure user is in a secured area, they must be accompanied at all times and client-level data must be removed from view.

Regular maintenance personnel must sign a confidentiality statement before being admitted to a secured area.
Securing Client-level Data - Leaving

If you are leaving a secured area for a brief time (less than 30 minutes), client-level data must be turned face-down on office surfaces and computers storing client-level data records must be locked.

If you are leaving a secured area for a long time (more than 30 minutes), client-level data records must be returned to their locked file cabinet or receptable and computers storing client-level data records must be locked.
Client-level Data in the Field – Collecting Data

If you are in the field and need to collect client-level data from a client verbally, you must make sure a door can be closed and that you are alone in the room with a client (or that only secure users are present).

If you are in the field and a client will be completing a client-level data form individually, you must assure that you are in a room with a door and do your best to honor client requests to complete a form in a more private location.
Client-level Data in the Field – Handling Data

When you have client-level data records in the field:

• Keep records in a manila envelope that is sealed and marked ‘confidential’ or in a locked briefcase

• Do not leave records unattended

• Do not keep records overnight

• Encrypt portable electronic records
Encryption

Encryption is the translation of data into a secret code. Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it.
Client-level Data – Retention and Disposal

**Paper client-level data records**
Grantees must retain client-level data records for twelve months and then through the end of the grant year in which that twelve-month period expires. After that point, they must be machine shredded.

**Portable electronic records**
These should be kept for as long as it takes to complete the task for which they were created. After that point, disks and other storage media must be sanitized.

**Electronic records**
Records stored on a computer harddrive can be kept indefinitely. Before you get rid of a computer that has client-level data stored on it, or give it to someone who is not a secure user, the hard drive must be sanitized.
Communication of Client-level Data: Mail, Email, Fax

Mail
When transmitting client-level data using U.S. mail, you must place data in an envelope stamped ‘Confidential’ and have a second party verify the correct address.

Email
Client names may not be transmitted via email. Date of birth and date of service may be transmitted between service agencies and referral agencies via email to confirm referral linkages.

Fax
Fax machines being used must be located in secured areas. Use a coversheet that displays your program’s confidentiality standard, alert the fax recipient before you send it, confirm and re-check the fax number on the view screen, and call the recipient in order to verify they received it. If data was not received, attempt to retrieve it.
Printing and Photocopying Client-level Data

Printers and photocopiers used for client-level data must be located in secure areas.

To print or photocopy, wait by the machine until the job is completed. Do not print or photocopy if there are people in the area who are not secure users.
Verbal Discussion about Client-level Data

Do not discuss client-level data with anyone who is not a secure user.

Do not discuss client-level data when non-secure users may be able to overhear.

When discussing client-level data on the telephone, only do so with familiar secure users or a referrable agency. Try to prevent non-secure users from overhearing, and only do so within a secure area.
Breaches are infractions or violations 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.

A breach does not necessarily mean that sensitive information was released to the public or that any one person was harmed. A minor infraction, like forgetting to lock a file drawer containing sensitive information – even if inside the secured area – constitutes a breach of security protocol as compared to a breach of confidentiality.

A breach of confidentiality is a security infraction that results in the release of private information with or without harm to one or more individuals.
Secure User Responsibilities

As a secure user, you have the following responsibilities to avoid a breach of confidentiality:

• Adhere to policies in this document to ensure confidentiality of client-level data that you work with
• Do not access client-level data that is not necessary to do your job
• Do not disclose client-level data to non-secure users
• Challenge unauthorized users of data
• Report suspected security and confidentiality breaches to your supervisor
Secure User Responsibilities

Not adhering to these responsibilities could result in the following penalties:

- Reprimands
- Suspension of system and data privileges
- Suspension from duty
- Civil penalties
- Criminal prosecution
Release of Client-level Data

Releasing client-level data means giving that data to an individual or organization that is outside the secure user’s organization, other than the Vermont Department of Health or the CDC.

The only permissible release of client-level data by a secure user, or the organization under which they work, is for the purpose of confirming linkage to a needed client referral to which the client has agreed. For example, for the purpose of a referral made during an HIV testing session. In such instances, a valid release must be in place that is signed and dated by the client in question.
Thank you!

Please complete the Vermont Department of Health HIV/STD/Hepatitis Confidentiality and Security Quiz, found here:

https://www.surveymonkey.com/r/N5XDBFH

Once you have taken the quiz, be sure to sign the Secure User Confidentiality Statement, found on our HIV surveillance page under the dropdown Confidentiality Training For HIV Services Staff and Volunteers:

https://www.healthvermont.gov/immunizations-infectious-disease/hiv/surveillance

Check with your supervisor or team leader to see if they will keep a copy of this statement on file at your organization.