VERMONT

DEPARTMENT OF HEALTH

HIV/STD/Hepatitis Program

Confidentiality & Security Policies & Procedures For Client-Level Data

VERMONT
DEPARTMENT OF HEALTH

How to Navigate This Presentation

- To move from slide to slide, either click the left button of your mouse or use the scroll on your mouse
- Throughout this presentation, you will see places that say “click here” in order to see more information on the topic.
- When you come to one of these places, click on the word “here” with your mouse and that will bring you to another slide
- Move the mouse over the word “back” until the mouse arrow becomes a hand, and then click the left mouse button on “back.” BE SURE only to click with the hand, otherwise you will be directed to the wrong slide.

VERMONT
DEPARTMENT OF HEALTH

BECOMING A SECURE USER

VERMONT
DEPARTMENT OF HEALTH

BECOMING A SECURE USER

1. A secure user is a staff member 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

2. In order to be authorized to be a secure user, you must review this slide set and then do the following:
   - Sign a secure user confidentiality statement. Click here.
   - Take the Confidentiality and Security Quiz, and review the correct answers to assure you understand any errors

VERMONT
DEPARTMENT OF HEALTH

CLIENT-LEVEL DATA

VERMONT
DEPARTMENT OF HEALTH

CLIENT-LEVEL DATA IS:

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

2. This data could be:
    - Client name and date of birth
    - Client demographics – such as the race, ethnicity, gender
    - Client risk-behaviors – such as whether the client has had sex or used injection drugs during a certain period of time

3. The official definition of Client-Level Data for the purposes of this policy can be viewed by clicking here

CLIENT-LEVEL DATA IS:

4. Client-level data records can consist of either:

   - **Paper Records –** client-level data that is on a data collection form for example
   - **Electronic Records –** client-level data that is stored electronically (on a computer most likely).
   - **Portable Electronic Records –** client-level data that is stored on portable electronic devices such as a laptop, smart phone etc., or on removable storage media such as a flash drive.

VERMONT
DEPARTMENT OF HEALTH

CONFIDENTIALITY

VERMONT
DEPARTMENT OF HEALTH

CONFIDENTIALITY

1. After learning what Client-Level Data is, you can see how it could be possible to use this data to identify a particular client.

2. For this reason, it is very important that this data be kept confidential in order to protect client privacy. Click here to see the definition of confidentiality.

VERMONT
DEPARTMENT OF HEALTH

SECURING CLIENT-LEVEL DATA

VERMONT
DEPARTMENT OF HEALTH

SECURING CLIENT-LEVEL DATA

1. 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 receptacle within a room that has floor-to-ceiling walls and a door with a lock.
    - For the purpose of talking about client-level data, a secured area would just be a room with floor-to-ceiling walls and a door with a lock

2. Secured Areas must be locked when the secure user is not present.

VERMONT
DEPARTMENT OF HEALTH

SECURING CLIENT-LEVEL DATA IN A SECURE AREA: PASSWORDS, KEYS, ETC…

1. 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.

2. 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.

VERMONT
DEPARTMENT OF HEALTH

SECURING CLIENT-LEVEL DATA IN SECURED AREA: COMPUTERS

1. 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 <u>all times</u> 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 IN A SECURED AREA: VISITORS

1. 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

2. Regular maintenance personnel must sign a confidentiality statement before being admitted to a secured area

VERMONT
DEPARTMENT OF HEALTH

SECURING CLIENT-LEVEL DATA IN A SECURED AREA: LEAVING

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

2. 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 receptacle
    - Computers storing client-level data records must be locked

VERMONT
DEPARTMENT OF HEALTH

CLIENT-LEVEL DATA IN THE FIELD

VERMONT
DEPARTMENT OF HEALTH

CLIENT-LEVEL DATA IN THE FIELD: COLLECTING DATA

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

2. 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
   - Do your best to honor client requests to complete a form in a more private location

VERMONT
DEPARTMENT OF HEALTH

CLIENT-LEVEL DATA IN THE FIELD: HANDLING DATA

1. 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. Click here for a definition of encryption.

VERMONT
DEPARTMENT OF HEALTH

CLIENT-LEVEL DATA:
RETENTION AND DISPOSAL

VERMONT
DEPARTMENT OF HEALTH

CLIENT-LEVEL DATA:
RENTENTION AND DISPOSAL

1. **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
2. **Portable electronic records**:
   - You should only keep these records for as long as it takes to complete the task that they were created for
   - After that point, disks and other storage media must be sanitized
3. **Electronic records:**
   - Electronic records stored on a computer hard-drive can be kept indefinitely
   - Before you get rid of a computer that has client-level data stored on it, or give to someone who is not a secure user, the hard drive must be sanitized

VERMONT
DEPARTMENT OF HEALTH

COMMUNICATION OF CLIENT-LEVEL DATA

VERMONT
DEPARTMENT OF HEALTH

COMMUNICATION OF CLIENT-LEVEL DATA: MAIL, EMAIL, FAX

1. When transmitting client-level data using the U.S. Mail you must:
   - Place data in an envelope stamped 'confidential'
   - Have a second party verify address

2. 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.

3. Fax machines being used must be located in secured areas
   - Use a coversheet that displays your program's confidentiality standard
   - Alert the person the fax is going to before you send it in order to tell them
   - Confirm and re-check the fax number on the view screen
   - Call the person you sent the fax to in order to verify that they got it
   - If data was not received attempt to retrieve it

VERMONT
DEPARTMENT OF HEALTH

Printing and Photocoping Client-Level Data

VERMONT
DEPARTMENT OF HEALTH

PRINTING AND PHOTOCOPING CLIENT-LEVEL DATA

1. Both printers and photocopiers must be located in secured areas

2. 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

VERMONT
DEPARTMENT OF HEALTH

VERBAL DISCUSSION ABOUT CLIENT-LEVEL DATA

VERMONT
DEPARTMENT OF HEALTH

VERBAL DISCUSSION ABOUT CLIENT-LEVEL DATA

1. Do not discuss client-level data with anyone who is not a secure user
2. Do not discuss client-level data when non-secure users may be able to overhear
3. When discussing client-level data on the telephone:
    - Only do so with familiar secure users or a referral agency
    - Attempt to prevent non-secure users from overhearing
    - Only do so within a secured area

VERMONT
DEPARTMENT OF HEALTH

SECURE USER RESPONSIBILITIES

VERMONT
DEPARTMENT OF HEALTH

SECURE USER RESPONSIBILITIES

1. As a secure user, you have the following responsibilities to avoid a breach of confidentiality: (Click here to see the definition of a breach)

   - 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 any 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

VERMONT
DEPARTMENT OF HEALTH

RELEASE OF CLIENT-LEVEL DATA

VERMONT
DEPARTMENT OF HEALTH

RELEASE OF CLIENT DATA

1. 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

2. 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 of a referral made during an HIV testing session and , in such instances, a valid release must be in place that is signed and dated by the client in question.

VERMONT
DEPARTMENT OF HEALTH

END.

THANK YOU!

*please complete the Vermont Department of Health HIV/STD/Hepatitis confidentiality and security quiz now.

Secure User Confidentiality Statement

As a person who will have access to client-level data in order to fulfill my responsibilities, I hereby acknowledge that my access to this data shall be restricted as follows:

1. I understand that all information as to personal facts and circumstances obtained in connection with client-level data must be held confidential and be considered privileged communications
2. I shall hold in confidence any information about persons which comes to my attention through my access to client-level data
3. I shall not divulge or disclose this information in any manner whatsoever to an unauthorized person.
4. I shall access only those client-level data records that I must collect, process or analyze in fulfillment of my responsibilities
5. I shall challenge any unauthorized users of the data and report suspected security and confidentiality breaches to my direct supervisor or the Vermont Department of Health HIV/STD/Hepatitis Program.

Additionally, I understand that I may be subject to reprimands, suspension of system privileges/data access privileges, suspension from duty, civil penalties or criminal prosecution for any of the following acts:

1. Failure to ensure the confidentiality of the client-level data records to which I have access by:
    a. Failing to adhere to the policies and procedures in the document entitled "Vermont Department of Health HIV/STD/Hepatitis Program Confidentiality and Security Policies and Procedures for Client-Level Data"
    b. Otherwise causing the disclosure of any client-level data to an unauthorized person
2. Accessing records that are not necessary for fulfillment of my responsibilities as a secure user
3. Failing to challenge unauthorized use of client-level data
4. Failing to report a suspected breach of security or confidentiality to a supervisor.

Upon concluding my work as a secure user at _____, I hereby agree to
{Insert agency name}

return to _____ all records and copies thereof that I obtained in
{Insert agency name}

connection with my work as a secure user. Furthermore, I agree to keep confidential all information contained in the records to which I had access during my work as a secure user at

_____ .
{Insert agency name}

Secure User Signature:_____ Date _____

_____
{Print First and Last Name}

Witness Signature_____ Date_____

_____
{Print First and Last Name}

back

Client-Level Data

Any record containing constructive identifying information

Constructive Identifying Information

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)

back

CONFIDENTIALITY:

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

back

ENCRYPTION:

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.

back

Breach

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.

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.

Breach of Confidentiality

A security infraction that results in the release of private information with or without harm to one or more individuals.

back