

**CONFIDENTIALITY AND SECURITY POLICIES AND PROCEDURES  
FOR PEMS CLIENT-LEVEL DATA**

**VERMONT HIV/AIDS PROGRAM**

**(2006)**

**VERMONT DEPARTMENT OF HEALTH  
DIVISION OF HEALTH SURVEILLANCE**

**CONFIDENTIALITY AND SECURITY POLICIES AND PROCEDURES  
FOR PEMS CLIENT-LEVEL DATA**

TABLE OF CONTENTS

	<b>LIST OF APPENDICES</b> _____	ii
	<b>DEFINITIONS</b> _____	iii
	<b>INTRODUCTION</b> _____	1
<b>I.</b>	<b>PHYSICAL SECURITY</b> _____	1
	A. PEMS users _____	1
	B. Access to client-level data _____	3
	C. Work site security _____	3
	D. Storing data _____	4
	E. Record retention and disposal Policy _____	5
	F. Breach of security/confidentiality _____	6
	G. Encryption _____	7
	H. Data integrity _____	7
<b>II.</b>	<b>COMPUTER SECURITY</b> _____	7
	A. Login/Password/Challenge phrase _____	7
	B. Computers used for PEMS _____	8
<b>III.</b>	<b>FIELD ACTIVITIES</b> _____	8
	A. Collecting PEMS client-level data _____	8
	B. Handling Paper/Portable electronic records _____	9
<b>IV.</b>	<b>COMMUNICATION</b> _____	9
	A. Mail, e-mail, fax _____	9
	B. Printing and photocopying _____	11
	C. Telephone _____	11
	D. Verbal discussion _____	11
<b>V.</b>	<b>DATA RELEASE</b> _____	12
	A. Data release defined _____	12
	B. Release of data by VDH _____	12
	C. Release of data by VDH grantees _____	14
	D. Submitting data to CDC _____	14

## Appendices:

- I. Instructions for disabling browser password caching
- II. Vermont Department of Health News and Media Policy
- III. Statement of Acknowledgement and Agreement of Confidentiality and Security Policies and Procedures for PEMS Client-Level Data

## Definitions:

**Authorized Individuals** – Those individuals who have a current, signed confidentiality statement and statement of acknowledgement and agreement of PEMS confidentiality and security policies in their files, whose current duties require them to have access to PEMS data, and who are authorized by the System Administrator to have access to PEMS data.

**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.

**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

**Data Release** – The provision of PEMS client-level data to entities outside of either the VDH HIV/AIDS/STD Program or the Centers for Disease Control and Prevention – data release does not include VDH reports back to a grantee with that agency's own data

**PEMS client-level data** – Any record containing PEMS constructive identifying information

**PEMS Client Unique ID** – The state-wide unique identifier which will be used to prevent duplication among clients accessing CDC funded interventions. In Vermont this ID is composed of first letter of first name, second letter of sex at birth, second and third letters of month of birth and last three digits of year of birth.

**PEMS constructive identifying information** – Any single piece of information or combination of several pieces of information from PEMS that could be used to deduce the identity of an individual (e.g, names or pieces of names, addresses, ZIP codes, telephone numbers, ethnicity, gender).

**PEMS User** – Any agency staff member who will have access to PEMS client-level data for the purposes of collecting, processing or analyzing the data

**Portable electronic PEMS client-level data records** – Any records containing PEMS client-level data that are stored on portable electronic devices (laptop, blackberry etc.) or on removable storage media (diskette, CD).

**Secured area** – The physical confinement limiting where PEMS client-level data are stored or where communications involving PEMS client-level data are permissible. A secured area consists of a room that has floor-to-ceiling walls and a door with a lock. For the purpose of storing paper records and portable electronic records, a secured area consists of a locked file cabinet or other locked receptacle within a locked room. Access to any receptacle (including a computer) storing PEMS client-level data must be restricted to authorized individuals.

**Overall Responsible Party (ORP)** – The official who accepts overall responsibility for implementing and enforcing these security standards and may be liable for breach of confidentiality. The ORP should be a high-ranking public health official; for Vermont, this person is the Director of the Division of Health Surveillance. This official has the authority to make decisions about operations that may affect programs outside the HIV/AIDS program unit and serves as one of the contacts with public health professionals and the HIV-affected community on policies and practices associated with HIV/AIDS program. The ORP is responsible for protecting HIV/AIDS prevention data as they are collected, stored, analyzed, and released and must certify annually that all security Program Requirements of the Centers for Disease Control and Prevention (CDC) are being met.

## Confidentiality and Security Policies and Procedures For PEMS Client-Level Data

### **Introduction:**

The following document outlines the VDH HIV/AIDS Program's policy concerning privacy, confidentiality and security of PEMS client-level data. This policy assures the ability to collect, process and analyze PEMS client-level data while at the same time maintaining strict standards for data confidentiality and security. In addition, the policy requires uniform practices among all users of PEMS client-level data.

### **I. Physical Security:**

#### ***A: PEMS Users:***

##### **Authorization**

All PEMS users must sign a **confidentiality statement and statement of acknowledgement and agreement of PEMS confidentiality and security policies**, and keep copies of both. The original documents shall be submitted to the PEMS System Administrator. Signing these documents indicates that the employee has been made aware of the policies and procedures in this document, understands the need to maintain client confidentiality and is aware of the penalties for failing to do so. These documents will be kept on file for six years from the date that the individual ceases to be a PEMS user. Only individuals who have signed these documents will be considered authorized individuals for the purpose of handling PEMS client-level data.

##### **Training**

All PEMS users must review the Power Point slide presentation entitled "Confidentiality and Security Policies and Procedures for PEMS Client-Level Data - An Overview for PEMS Users" and complete a quiz that tests the user's knowledge of the most important components. The PEMS user will submit his/her completed quiz along with a confidentiality statement and statement of acknowledgement and agreement. The user is then responsible for reviewing the correct answers to the quiz in order to understand errors. The record of the individual's completion of the quiz will be maintained by the System Administrator for six years from the date that individual ceases to be a PEMS user.

Individuals who supervise PEMS users, or PEMS users who are their own supervisors must review the Power Point slide presentation entitled "Supervisor Responsibilities in Regards to Confidentiality and Security of PEMS Client-level Data" in order to understand the role that managing PEMS users plays in maintaining confidentiality of the PEMS data.

## **Staff Separation**

As part of departure/change of duties procedures for PEMS users, the System Administrator shall be notified if a PEMS user will be (1) leaving the agency or (2) changing duties within an agency so that he/she will no longer be a PEMS user. This way, the System Administrator may take proper actions to protect the system and its data.

- If a PEMS user changes duties within an agency but will still be a PEMS user, the System Administrator shall modify his/her PEMS database access privileges accordingly, and the System Administrator or direct supervisor shall modify access to PEMS client-level data (aside from database access) accordingly. This means that a direct supervisor should take any possible steps to make sure that the PEMS user does not have access to data that is unnecessary for the user's new scope of work. However, it is ultimately up to the PEMS user to only access data needed in order to do his/her job.
- If a PEMS user leaves the agency altogether or changes duties within an agency so that he/she will no longer be a PEMS user, the System Administrator or a direct supervisor shall, by the individual's last scheduled work day as a PEMS user, assure that all keys, including keys to offices, filing cabinets and storage areas, have been returned. The direct supervisor and System Administrator will terminate a user's access to PEMS client-level data and to the PEMS database. The departing staff member will discuss with their supervisor the continued need to adhere to the confidentiality statement. These activities would typically occur as a part of a staff "exit interview," conducted by the supervisor of the departing staff member. Staff will be required to sign the following statement: "Upon concluding my work as a PEMS user at [Insert agency name], I hereby agree to return to [Insert agency name] all records and copies thereof that I obtained in connection with my work as a PEMS user. Furthermore, I agree to keep confidential all information contained in the records to which I had access during my work as a PEMS user at [Insert agency name]." A photocopy of this signed statement will be given to the PEMS System Administrator and maintained for six (6) years from the date signed.

## **System Administrator Roles**

The PEMS System Administrator will be responsible for the security of the PEMS client-level data. This person will be responsible for ensuring ongoing staff training and compliance, and reviewing this policy on an annual basis and making changes as is necessary. This person will also be responsible for receiving complaints concerning this policy and PEMS client-level data confidentiality and security compliance issues (including computer use violations).

## ***B: Access to Client-level Data:***

Only staff whose role it is to collect, process or analyze PEMS client-level data shall have access to the data. Persons granted access to PEMS client-level data or the PEMS database will have that access restricted by the roles that correspond to the duties they need to perform.

The process by which a new staff member can gain access to the system or to PEMS client-level data will be as follows. The supervisor of the staff member will first submit a Request for Access to PEMS Client-Level Data form to the PEMS System Administrator. This request includes a description of what the person's duties will be related to PEMS. The System Administrator will next assure that the person completes training on this policy and signs both a confidentiality statement and a statement of acknowledgement and agreement of the PEMS confidentiality and security policies. If the request is being made for a new system user who will need access to the database, the System Administrator will then establish an account for the user, with a login and password, and will specify permissions and levels of access the user will have within the system (which should only be those sufficient to perform the duties required by the job). The System Administrator will also obtain a digital certificate for the new system user.

## ***C: Work Site Security***

PEMS users shall be individually responsible for protecting their own workstations. This responsibility includes protecting keys, passwords, codes and electronic devices that would allow access to PEMS client-level data or the PEMS database.

### **Unauthorized Persons entering the work area**

Non-maintenance visitors must be accompanied at all times after being admitted to any secured area. Program staff will be notified in advance that a visitor will be escorted to their space, allowing time for removal of confidential documents from workspaces, if necessary. Program staff will walk visitors out to the reception area when the visitor departs.

Regular maintenance and cleaning personnel shall be required to sign a confidentiality statement before being admitted to a secured area.

Precautions will be taken to prevent unauthorized people entering the work area from viewing PEMS client-level data (paper or electronic). If unauthorized persons enter a work area containing PEMS client-level data, such data will be immediately removed from view (e.g. clearing computer screens, placing documents in desk drawers).

### **Leaving the work area**

Paper or portable electronic records containing PEMS client-level data shall not be in the work area unless authorized individuals are working with them. Otherwise, records shall be stored in locked file-cabinets or other locked receptacles.

When a PEMS user leaves his/her work area for short periods of time (less than 30 minutes), computers containing PEMS client-level data must be locked so that they will require use of a password to reopen. The monitor must also be turned off if it is still possible to see the screen. In addition, all paper records shall be turned facedown on desks and office surfaces.

When a PEMS user leaves his/her work area for periods of 30 minutes or more, computers must be locked (and monitors turned off if it is still possible to see the screen) and all paper or portable electronic records must be returned to their locked receptacles.

PEMS users who utilize PEMS client-level data throughout the workday will be located in low-traffic areas and will appropriately store data when away from the workstation for 30 minutes or more (as is described above).

All paper or portable electronic PEMS client-level data records will be returned to a locked receptacle when office hours are concluded.

All computers with access to the PEMS database or storing PEMS client-level data will be locked when office hours are concluded.

If the PEMS client-level data is being removed from secured areas for analysis, it should be de-identified first. If a portable electronic record is removed from a secured area, it must be encrypted.

### ***D: Storing Data***

#### **Paper Records**

When not in use, completed client-level data forms and other paper records containing PEMS client-level data (including but not limited to counselor notes, client files, data print-outs) shall be stored in secured areas.

#### **Electronic Records**

When not in use, any portable electronic PEMS client-level data records shall be stored in secured areas. Computers storing PEMS client-level data must conform to policies mentioned in Section II: Computer Security.

If PEMS client-level data is stored on a laptop, the hard drive or diskette, whichever the data is stored on, must be separated from the computer when not in use and stored in a secured area.

All storage media shall be clearly labeled to reflect what data they contain.

Diskettes and other storage media that contain PEMS client-level data should have only the minimum data necessary to perform a given task

All storage areas containing PEMS client-level data are to be locked when authorized individuals are not present. Staff shall be responsible for double-checking that storage areas within their workspace are locked at the end of office hours.

### ***E: Record Retention and Disposal Policy***

Paper records containing PEMS client-level data will be maintained for 6 years from the date created.

Portable electronic records will be maintained for the length of time necessary for task completion.

Paper and portable electronic records will then be disposed of by the following methods.

- If PEMS client-level data has been saved in paper format, these records will be machine shredded. Any paper records which do not need to be retained (notes, statistical output and computer printouts) must be shredded as soon as they are no longer needed.
- If PEMS client-level data has been saved on diskettes and other storage media they shall be sanitized immediately following the task completion (aside from backups) and definitely before being reused.
- If PEMS client-level data has been stored on an electronic device such as a palm pilot or lap top, such devices must be sanitized to ensure that the PEMS client-level data is not retrievable using “undelete” or other data retrieval software.

Electronic records which are stored on the hard drive of a computer, such as any statistical reports, will be maintained indefinitely, and must be destroyed under the following circumstances according to the following method.

- If PEMS client-level data has been saved on the hard drive of a computer, the hard drive must be sanitized before the computer can be disposed of, labeled as

excess or surplus, sent off-site for repair or transferred to staff not authorized to use PEMS.

The sanitizing of electronic devices and hard drives must be conducted by qualified IT staff who completely remove data so that it is “unrecoverable.”

Agency staff must inform the PEMS System Administrator when any equipment that has been used to store PEMS client-level data electronically is being replaced. The PEMS System Administrator is then responsible for ensuring that the equipment is sanitized.

### ***F: Breach of Security/Confidentiality***

#### **PEMS User Responsibilities**

PEMS users are responsible for adhering to the policies and procedures in this document in order to ensure the confidentiality of PEMS client-level data records to which they have access.

PEMS users are prohibited from accessing PEMS client-level data which is unnecessary for the fulfillment of their responsibilities.

PEMS users are prohibited from disclosing or divulging any PEMS client-level data to unauthorized persons in any manner whatsoever

PEMS users are responsible for challenging any unauthorized users of the data and reporting suspected security and confidentiality breaches. Any PEMS user who suspects any breach of confidentiality or security (e.g., possible viruses, hackers, password divulgence, lost or misplaced storage media, improper record disposal/retention methods, release of private information) shall immediately report this information to their direct supervisor, who will then immediately notify the PEMS System Administrator. The PEMS System Administrator will then notify the ORP.

#### **Penalties**

Any person failing to adhere to these responsibilities is subject to the following penalties.

- Reprimands
- Suspension of system privileges / data access privileges
- Suspension from duty
- Civil penalties
- Criminal prosecution

(Title 18, §1001. Reports to the Commissioner of Health, Sec. 2.e., and Confidentiality Statement).

## **Mitigation**

VDH will mitigate, to the extent possible, any harmful effect resulting from a breach of security or confidentiality by an employee or other data user. In the event of a breach of confidentiality, VDH will take reasonable steps to determine how PEMS client-level data was improperly disclosed, how it might be used to cause harm and what steps can be taken to alleviate the effect that resulted from the breach. The PEMS System Administrator will determine if the incident should be reported to the PEMS Security Coordinator via the PEMS Service Support Center.

## ***G: Encryption***

### **Transmission to CDC**

PEMS client-level data must always be encrypted during transmission to CDC via the Secure Data Network. For more information about transmission of data to the CDC see Section V. Data Release, sub-section C: Submitting PEMS client-level data to CDC.

### **Portable Electronic Records**

Portable electronic PEMS client-level data records must be encrypted if they will be used or transported outside of a secured area.

## ***H: Data Integrity***

Persons who have access to PEMS client-level data are prohibited from altering the data for misrepresentation or falsification purposes.

## **II. Computer Security:**

For computers used for PEMS (having access to PEMS or storing PEMS client-level data)

### ***A: Login/Password/Challenge Phrase***

- If a challenge phrase for a digital certificate or a login or password for PEMS software access is written down, it shall be kept in a locked drawer or other locked location.
- Passwords for PEMS software access shall be at least 8 characters long, contain a mix of at least three of the four types of keyboard elements (upper-case, lower-case, numbers, symbols), and can not be the individual's name. Passwords should be changed at least every 90 days (this should be required by the system) and shall not be divulged to others.
- If it is discovered that a challenge phrase or password has been stolen or become known to someone else, staff will immediately notify their direct supervisor who

will notify the PEMS System Administrator (as this would be considered a breach of security protocol).

### ***B: Computers Used for PEMS***

- Computers which have PEMS access (digital certificates) or which are storing PEMS client-level data must have automatic screen saver locks with a 15 minute or less activation time and must be password protected (whereby a username and password is required in order to unlock the screensaver).
- Any computer which is used for PEMS must be locked at all times that it is not in use. This applies even if the user is just stepping away from the computer temporarily.
- If a digital ID certificate is saved to disc and then temporarily saved on a computer in order to access PEMS, the certificate must be removed from the computer immediately following use. While the digital ID certificate is saved on the computer, the computer must be locked at all times that it is not in use (as mentioned above).
- All computers and other portable electronic equipment used for PEMS should be housed or stored in secured areas.
- All computers used for PEMS database access should be protected by surge suppressors and emergency battery power to prevent data loss in case of fluctuations in the power supply.
- Digital certificates should not be loaded onto laptops or other portable equipment.
- Any PEMS user who will be accessing the PEMS Database needs to disable the ability of their web browser to cache (save) their passwords. (Instructions for doing this can be found in Appendix I.)
- Users of computers with PEMS access or storing PEMS client-level data should not download materials from the Internet or other unauthorized software onto the computers.

## **III. Field Activities:**

### ***A: Collecting PEMS client-level data***

When a provider is collecting PEMS client-level data verbally from a client, steps shall be taken to ensure that client privacy is maintained and that data is collected confidentially. Client-level data shall only be collected verbally under the following conditions:

- A door can be closed

- The Provider and client are alone in a room or
- Only authorized individuals are present

If data collection is not administered by the provider, but rather clients are completing forms individually, providers shall assure that the client or group of clients are in a room with a door and will do their best to honor client requests to complete forms in a more private location.

At all times other than during data collection, transport, and use, PEMS client-level data shall be stored according to guidelines in Physical Security, Section D: Storing Data.

### ***B: Handling Paper and Portable Electronic Records In the field***

When PEMS client-level data records are being transported by a PEMS user from a field setting (such as an outreach intervention) or an agency site to an office where the records will be stored and/or entered, records will be kept in a manila envelope that is sealed and marked 'confidential,' or in a locked briefcase.

While in the field, paper and portable electronic PEMS client-level data records will not be out of sight of the PEMS user at any time unless they are in a locked field office storage area.

Paper and portable electronic PEMS client-level data records will not be left unattended in public access areas or in unlocked cars.

Except in the case that a staff member has obtained prior approval from the System Administrator, paper and portable electronic PEMS client-level data records will not be kept overnight by PEMS users but rather returned to either a field office or headquarters and appropriately stored.

Portable electronic PEMS client-level data records must be encrypted if they will be used or transported outside of a secured area.

## **IV. Communication:**

### ***A: Mail, Email, Fax***

All PEMS client-level data sent through U.S. mail shall be placed in envelopes stamped "Confidential" and must be addressed to the System Administrator or this person's designee. Staff must ensure that the correct address is used. The System Administrator should let senders know immediately if mail is improperly sent. The System Administrator or whoever is responsible for receiving PEMS client-level data shall check his/her mailbox each day to avoid confidential information sitting in the mail

slot. A confirmation must be sent to verify that the data was received (either by voice, email or fax).

<b>System Administrator Address:</b> Ashley Dutro Vermont Department of Health 108 Cherry Street, PO Box 70 Drawer 41-HAST Burlington, VT 05402	<b>System Administrator Phone and Email:</b> (p) 802-651-1534 ashley.dutro@ahs.state.vt.us
--	--

PEMS client-level data should not be sent using electronic mail. If such mail is received, the recipient should immediately inform the sender that this is not permitted. The exception to this would be a random referral code used to track client referrals. Since this code does not contain any client identifying information, emailing of the codes is permissible.

Because of the potential for unintended receipt, all PEMS referral codes transmitted by email shall contain the following confidentiality notice:

*“Confidentiality Notice:* This email message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, or an authorized agent of the intended recipient, please immediately contact the sender by reply email/ fax and destroy/delete all copies of the original message. Any unauthorized review, use, copying, disclosure, or distribution by other than the intended recipient or authorized agent is prohibited.”

Fax machines used to send or receive PEMS client-level data must be located in secured areas. The sending or receiving of faxes containing client-level data must follow this procedure:

- A coversheet should be used and the fax should not be sent unless:
  - The receiving party is given prior notice by telephone immediately before the fax is sent
  - The fax number of the recipient is confirmed and re-checked on the view screen prior to sending
  - The recipient is called by telephone to verify transmission/receipt after the fax is sent

No individual shall use a fax machine to send PEMS client-level data unless previously authorized by the System Administrator.

Because of the potential for unintended receipt, all PEMS client-level data transmitted by fax shall contain the following confidentiality notice:

***Confidentiality Notice:*** This fax message, including any attachments, is for the sole use of the intended recipient(s) and may contain confidential and privileged information. If you are not the intended recipient, or an authorized agent of the intended recipient, please immediately contact the sender by reply email/fax and destroy/delete all copies of the original message. Any unauthorized review, use, copying, disclosure, or distribution by other than the intended recipient or authorized agent is prohibited."

If client-level data that has been transmitted (by regular mail, email or fax) was not received, the sender must work to determine the destination of the data and retrieve it if possible. If the data was transmitted by email or fax, it may be possible to work with the VDH IT staff to do this.

### ***B: Printing and Photocopying***

Printers and photocopiers used to print or photocopy data must be located in secured areas.

If documents containing PEMS client-level data are being printed, the individual printing the confidential information must wait by the printer while printing. Data should only be printed when there are no unauthorized persons in the area.

If documents containing PEMS client-level data are being photocopied, the individual photocopying the confidential information must wait by the photocopier until the job is complete. Data should only be photocopied when there are no unauthorized persons in the area.

### ***C: Telephone***

PEMS users will ensure that telephone communication concerning PEMS client-level data is made only to familiar, authorized individuals (e.g. PEMS System Administrator and his/ her designee, referral agency, etc.) and that the communications take place from within a secured area. Attempts should be made to prevent unauthorized individuals from overhearing.

### ***D: Verbal Discussion***

Authorized individuals must not discuss PEMS client-level data with anyone who is not authorized to have access to that information

Authorized individuals must not discuss PEMS client-level data when unauthorized individuals may be able to overhear.

## **V. Data Release:**

### ***A: Data Release Defined***

Please note that for purposes of this policy, “data release” refers to provision of PEMS client-level data to entities outside of either the VDH HIV/AIDS/STD Program or the Centers for Disease Control and Prevention.

VDH reporting back to a grantee with that agency’s own PEMS data is not considered data release.

In a report of a grantee’s own data back to the grantee:

- All cell sizes will be reported
- The bottom of each page will contain a confidentiality notice such as: “This report contains confidential information and should not be distributed outside of the agency”

### ***B: Release of Data by the Vermont Department of Health***

All internal (within the Agency of Human Services (AHS)) and external (outside of AHS) requests for data release will be handled according to the following process.

Only the minimum amount of information necessary for completing a given task will be released.

#### **Criteria for Data Release**

Internal requests for PEMS client-level data will be contingent upon the individual that will have the access having a signed, current confidentiality statement. External requests will be contingent upon the individual or agency having a signed, current confidentiality statement and a signed data use agreement with the HIV/AIDS Program. The data use agreement will include discussion of possible ramifications and criminal and civil liabilities for unauthorized disclosure of information. It will also specify how the data is allowed to be used.

Once an agency/individual meets these criteria, a data request from that agency/individual will be eligible for review.

In the case that an agency’s own PEMS data will be released back to that agency, there will not be a review of the “request” as is mentioned below. All reports of an agency’s own PEMS data back to that agency will adhere to data release guidelines (below).

## **Process for Data Release**

The PEMS System Administrator shall manage all releases of PEMS client-level data. This person will receive, help to review, respond to and track each data request. In addition, no individual-level data, even without the unique identifier, will be released either internally or externally without written authorization of the Overall Responsible Party (ORP). This is the person holding the position of the Director of the Division of Health Surveillance. For calendar year 2006, the ORP is William Apao, Ph.D.

Research requests for PEMS client-level data must be accompanied by a research protocol and proof of approval by an Institutional Review Board (IRB) formed and maintained in accordance with the U.S. Department of Health and Human Services Code of Federal regulations or Protection of Human Subjects (45 CFR 46, revised March 8, 1983). A protocol and proof of IRB approval must be included with each request for PEMS client-level data.

In most cases news reporters' calls should be directed to the HIV/AIDS Program Director, division directors, program managers, or the commissioner. The AIDS Program follows the established policies of the Vermont Department of Health regarding information release to the news media and public (see the draft VDH News Media Policy - Appendix II).

## **What Data Will Be Released**

The PEMS Client Unique ID is not subject to release.

All other PEMS variables are subject to release according to Data Release Guidelines described below. Each request for the data will be reviewed individually through the above procedure. If a request is made for individual-level data, the recipient would have to show that they have confidentiality and security procedures in place which are equivalent to those described in this document.

The Referral Code variable may be released in individual form between agencies funded by VDH for the purpose of referral tracking.

## **Data Release Guidelines**

The following guidelines will be used when PEMS client-level data is released.

"Cells" refer to the space formed by the intersection of a row and column in a statistical table. For example, a statistical table may include the category "race" in columns and the category "county" in rows. The resulting cells within the table describe a population by race and county. In some instances, cells provide very specific information about a limited number of people. In general, problems with confidentiality and privacy occur when there are small denominators, or population sizes, within a given cell in the table.

In order to reduce the risk of breaching confidentiality, the following guidelines shall be implemented when releasing data:

- Data from multiple agencies combined will be released, regardless of the numerator cell size, if the underlying population of the cell is 5,000 or greater.
- Data from multiple agencies combined with cell sizes of 5 or fewer will be suppressed if the underlying population of the cell is less than 5,000.
- For data from only one agency, regardless of the underlying population size, cell sizes of 5 or fewer will be suppressed.

Suppressing a value of 5 or fewer will work as follows. Suppressed data will be reflected in tables as “five or fewer”, “ $\leq 5$ ”, “fewer than 6” or “ $< 6$ .” The method of “primary cell suppression” is used to withhold the numerator in the cell that does not meet the threshold. In the event that only one cell is too small, two other “complementary” cells also need to be suppressed, including the next-larger cell and the total. This rule applies to both rows and columns whenever totals are presented. Complementary cell suppression must be completed in order to avoid inadvertent disclosure through back-calculation.

### ***C: Release of Data by Grantees of the Vermont Department of Health***

VDH grantees will be allowed to release the Referral Code variable to other VDH grantees for the purpose of referral tracking.

VDH grantees will release all PEMS client-level data to VDH for the purpose of data entry into PEMS. This release of data will be done in a complete and timely manner according to reporting requirements.

If VDH grantees receive external requests for PEMS client-level data (aside from requests from VDH), they will forward these requests on to the PEMS System Administrator and that individual will follow the process outlined above for release of data by VDH.

### ***D: Submitting PEMS client-level data to CDC***

The process for submitting PEMS client-level data to CDC will be as follows. Data extract files will be requested through the PEMS database. These files will then be encrypted using the CDC-supplied SEAL encryption software. The encrypted files will then be submitted to CDC via the Secure Data Network (SDN).

For now, only the PEMS System Administrator will be submitting data to CDC. Before submitting data, the System Administrator will review the data extract files for accuracy and completeness. If anyone other than the PEMS System Administrator will be responsible for reporting/submitting data to CDC, this person would first have to be authorized to do so by the System Administrator. Then the authorized person would review the data extract files for accuracy and completeness before submitting them.

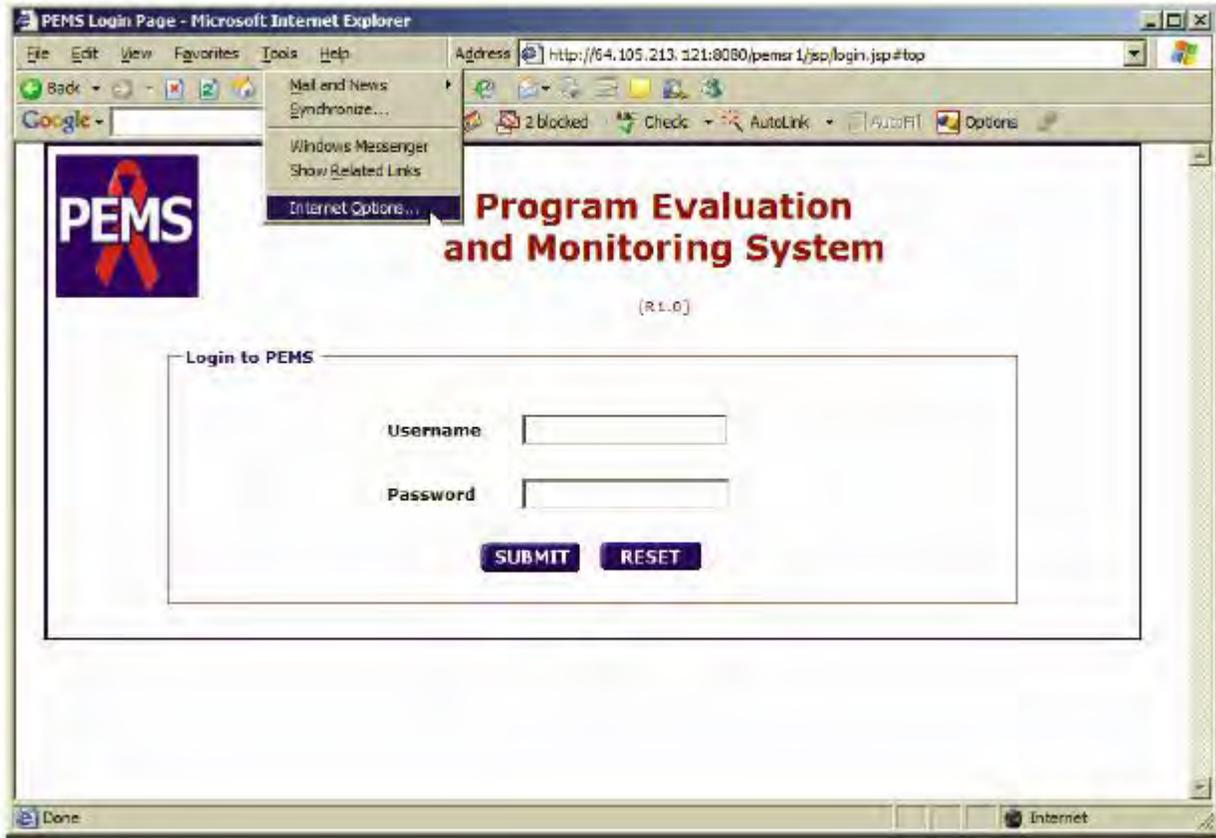
The PEMS Client Unique ID will not be reported to CDC

## APPENDIX I

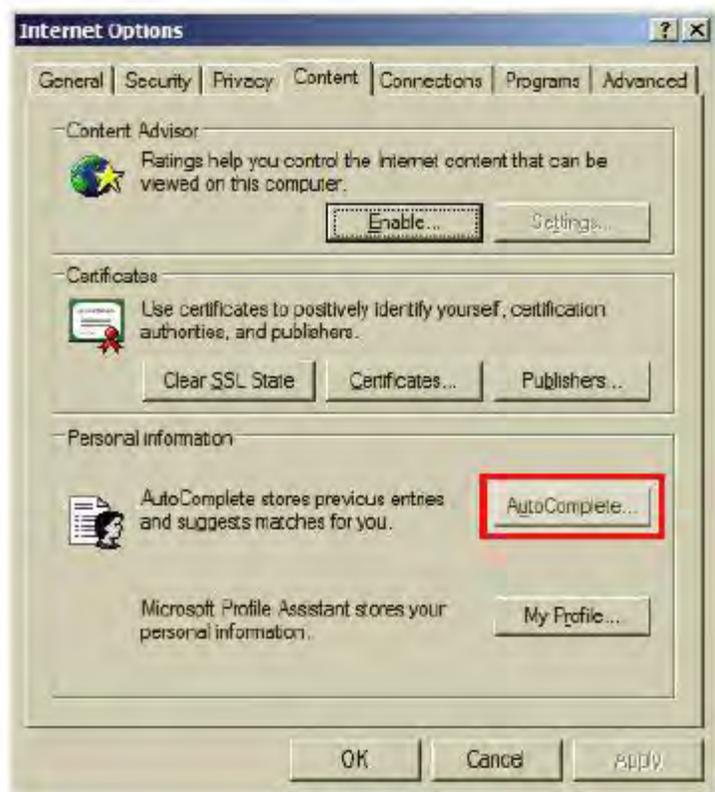
### **Disable Browser Password Caching**

PEMS Users who will be accessing the PEMS Database must disable the function in Windows that “remembers” or caches a password.

**To disable this option, open a new Web browser, and select Internet Options from the Tools menu.**



The Internet Options window appears. Switch to the Content tab, and click the AutoComplete Button.



The AutoComplete Settings window appears. While some of the settings in the “Use AutoComplete for” frame may have been disabled by your System Administrator, you should ensure that only Web addresses remains checked (i.e., clear the checkmark from the other boxes).

Finally, click the Clear Forms and Clear Passwords buttons.

*Note: Clicking these buttons will erase any form and password information your browser has cached for you, so make sure you remember your credentials before you perform this step.*



You will be asked for your password each time you log in from now on because the computer will no longer “remember” it for you

## APPENDIX II



## **News Media Policy • 2005**

The Department of Health has a continuing responsibility to keep the public informed about programs, activities, and matters affecting public health.

This policy establishes expectations for staff in their communication with the news media. It applies to all staff who represent the department, as well as those who because of their position may be seen as representing the department.

Communication with the news media includes: news releases, media advisories, formal statements, interviews, news conferences and briefings, letters to the editor, opinion editorials (“op eds”), corrections, announcements, and any other information provided to reporters, editors, and writers for newspapers, magazines, scientific journals, and trade publications; radio or television stations or networks and online news services; and any other electronic or print media related to news distribution.

All department communication, both verbal and written (including email), should be polite, clear, concise, timely, reasoned, free of jargon, and professional in tone and presentation.

### **A. Purpose**

1. To standardize and maximize the management and coordination of media relations and public relations activities.
2. To ensure accurate, credible and timely release of information and to maintain positive working relationships with the Vermont media.
3. To avoid competing or conflicting VDH media messages.
4. To clarify VDH media relations responsibilities, expectations and procedures.

### **B. Definitions**

1. AHS – Agency of Human Services
2. VDH – Vermont Department of Health
3. VSH – Vermont State Hospital
4. PIO – Public Information Officer – Communication Office staff charged with overseeing media relations. The PIO may be a different person for different issues.
5. Spokesperson – Individual designated by PIO to represent the VDH to the news media on a given topic, issue or incident.

### **C. Contacting the VDH Communication Office**

1. To notify the Communication Office of a media inquiry or to consult on a media issue:
  - a. Call 951-1276 and your call will be forwarded to the PIO; or
  - b. Email “Communication Office” in the Outlook Global Address List and the PIO will respond to you directly.

### **D. Media Message Categories**

The VDH places messages in the following categories, according to urgency of public health message and severity of risk. Any news release, health advisory, health alert, op ed or letter to the editor must be approved by the Communication Office prior to release and in most cases will be released by the Communication Office.

1. News Release – Announces new data, program, issue, ranking, report, award(s), change in leadership, position clarification, health awareness messages, etc., or announces an event such as an award ceremony, conference or public appearance.
  - a. To be worthy of a News Release the information must be determined by the Communication Office to be timely and warranting of public exposure and widespread distribution.
2. Health Advisory – Information about something of importance to the public’s health but with no immediate need to act. This is generally proactive/preventive information or advice, e.g. *“VDH advises parents to be alert for signs of ABC disease.”*
3. Health Alert – Information about a specific health issue where immediate action is required to protect public health, e.g. *“Anyone who ate at ABC restaurant may have been exposed to xyz and should contact the VDH.”* (Alerts would be used cautiously).
4. OpEd (Opinion/Editorial) or Letter to the Editor – Timely information, often provided in response to an article or statement that has been published in a newspaper.

### **E. News Release**

It is the responsibility of division directors, district directors and program managers to notify the Communication Office of potentially newsworthy events and information. The Communication Office will determine whether a news release is appropriate.

1. For a news release about a planned event, conference or ceremony, provide the following information:
  - a. Name, time and location of event.
  - b. Key speakers, audience, attending dignitaries.

- c. A short paragraph describing why this is important and what you would like to see in a news story about this event. Describe what you hope a general audience will do with this information.
  - d. Name and phone number of the subject matter expert.
- 2. For a news release about new data, program activity or report, provide the following information:
  - a. A short paragraph (or bullets) describing the subject and why it is important.
  - b. If data or report: the source of data or name of report and date of publication.
  - c. Key stakeholders, partners or interested parties.
  - d. Name and phone number of the subject matter expert.
- 3. For a news release about new personnel or change in leadership, provide the following information:
  - a. A short bio that includes previous relevant jobs, terminal academic degree, other relevant activities.
  - b. Date that the person will begin or end and job title.
  - c. If appropriate, one sentence about the person previously in the position.

## **F. Health Advisory or Health Alert**

It is the responsibility of the division director or program manager to notify the Communication Office of any perceived need to issue a health advisory or health alert. Working closely with the Commissioner and the subject matter expert, the Communication Office will determine the spokesperson, write the release, and manage media relations.

## **G. Op Ed (Opinion Editorial) or Letter to the Editor**

In most cases, only the commissioner or deputy commissioner will submit Op Eds to media outlets. No VDH employee shall submit an Op Ed or Letter to the Editor about VDH issues without the approval of the Communication Office.

- 1. Prior to release, the Communication Office shall review any Op Ed or Letter to the Editor. In addition to the draft, provide the following information:
  - a. A copy of the article or editorial that the Op Ed or Letter is in response to, and the name of the media outlet.
  - b. A short paragraph describing the reason for responding in this way.
- 2. To request that VDH respond to an article or issue in the news media, contact the Communication Office.

## H. Corrections

In most cases, only the Communication Office will contact reporters in response to errors or to requests corrections. No VDH employee shall do so without first informing the Communication Office.

1. To request that VDH respond to an article or issue in the media, contact the Communication Office.
2. If you believe that you were misquoted or incorrectly portrayed in a news story, contact the Communication Office.
3. Timing is important, so the earlier the contact is made, the better.

## I. News Media Relations

The news media is an important partner in public health. The media provides information to the public through television and radio broadcasts, in print and on line. A strong working relationship with the media is essential for furthering the mission of public health; however proper protocols must be followed to protect the credibility of VDH and to make sure that a concise, consistent and informative message is issued.

Proactively, the department is committed to providing the media with regular public health information. Reactively, the Communication Office will strive to adhere to press deadlines after careful review and consideration of the proper response.

1. Responding to media inquiries
  - a. All media inquiries should go first to the VDH Communication Office where a PIO will determine the reporter's needs and designate the spokesperson. *(The one exception is when a staff person has been designated by the Communication Office as spokesperson on a specific topic and is providing information within prior approved parameters.)*
  - b. When a reporter contacts VDH staff—
    - Ask for the reporter's name, telephone number, the subject of the call, and the deadline. Let the reporter know that you or someone else from VDH will get back to him or her shortly. Contact the Communication Office right away with the information.
    - The PIO may ask you to conduct the interview or refer it to another spokesperson.
    - Contact the Communication Office before making any statements to the press.
    - If interviewed in the field or on location, call the Communication Office to inform them of the interview and the content that was shared within 30 minutes of the interview.

- If you are designated by the PIO to respond to the reporter inquiry, email or call the Communication Office [863-7281 - or email group Communication Office] within 30 minutes with a short summary of the interview.
- c. When you are spokesperson—
- Spokesperson(s) should work with a PIO to prepare for the interview.
  - When communicating your title, provide your title in its shortest form. Reserve the term “Health Department Spokesperson” for the PIO.
2. Contacting the Media
- a. Prior to contacting a reporter or media outlet, call the Communication Office to discuss the purpose of the contact (e.g. to correct an error, to submit a letter to the editor, etc.)
- b. The Communication Office may approve the request, assign the task to another staff member, or recommend against action.

## **J. Data Requests**

Requests from reporters for VDH data (e.g. vital records, youth risk behavior survey, behavioral risk factor survey, food inspections, etc.) may come directly to program staff. Follow the procedures outline above unless you have been designated by the Communication Office and your supervisor as the appropriate person to provide the data.

## **K. Crisis and Emergency Communication**

Within 30 minutes following notification of a public health emergency, all media calls must be routed to the Communication Office. VDH will follow communication procedures outlined in the VDH Crisis and Emergency Risk Communication Plan. [See CERC Policy.]

## **L. Vermont State Hospital**

If the media contacts staff or a patient at Vermont State Hospital, VDH will follow communication procedures outlined in the VSH Media Policy. [See VSH Media Policy.]

## **M. Access to Public Records Law**

The media and the public shall be provided with requested information in a timely and thorough manner that is consistent with current law. [See 1 V.S.A. Sections 315-320.]

1. Requests from the Media
- a. Any response to a media-related Access to Public Records Law request should be coordinated with the Communication Office.
- b. The Communication Office will confer with the VDH legal counsel as needed, especially with regard to patient information.

## **N. Protection of Patient Information**

The Vermont Department of Health strives to protect the identity and the privacy of the people who are infected with diseases of public health concern such as SARS, and does not release confidential patient information in accordance with state and federal law.

1. The following list identifies the information that the department may release to the media and/or the public in such cases:
  - a. Aggregate data
  - b. County of residence
  - c. If the person was hospitalized or not; if the person was released from the hospital
  - d. Current status: improving, stable, deceased, etc.
  - e. General symptoms
  - f. Risk factors (travel to disease-affected area, exposure to infected patient, etc.)
  - g. Age range, e.g. teens, 20s, 30s, etc. or child younger than 13
2. In the event of a public health threat or emergency, it may become necessary to identify an individual or individuals to protect public health. Such action requires the approval of the Commissioner of Health.
3. It is the legal and ethical responsibility of the Vermont State Hospital to protect each patient's right to confidentiality with respect to information regarding the patient's care and treatment.
  - a. No statements or information released to the media shall disclose individually identifiable patient information. [See VSH Media Policy.]

## **O. Open Meetings Law**

The news media's right to attend public meetings and to receive copies of agendas and minutes is basically the same as the right of any other member of the public.

Vermont law says that all portions of all meetings of a "public body" must be open to the public unless there is a specific authorization set out in law that allows a meeting, or a portion of a meeting, to be closed. The law defines a public body, in part, as any board, council or commission of any agency of the state, as well as any committee of such boards, councils or commissions.

As a rule of thumb, if a committee is created by law or by promulgated rule, it is a public body. If not, it probably is not.

The following are examples of Health Department entities that are public bodies:

- The Vermont Board of Medical Practice.

- The Vermont Comprehensive Tobacco Control Program.
- The Vermont State Hospital Future Planning Advisory Group.

By policy, the department may admit the public to meetings of other groups or committees, and post notice of such meetings. The right of the public to attend these meetings, however, is discretionary, and there are few if any legal requirements regarding the closing of a particular meeting or portion of a meeting. Examples of meetings that might be open to the public at the discretion of the department, but are not subject to the open meetings law:

- A meeting of the infant mortality study committee.
- A training session for first responders or town health officers.
- A work session of the executive committee of the Vermont Blueprint for Health.

Examples of meetings that generally would be closed to the public and are not subject to the open meetings law, but which could be opened upon occasion at the discretion of the department:

- Any department, division or program staff meeting.
- A meeting of staff members and health care providers to discuss a developing public health threat.
- A meeting of staff members and representatives of professional organizations concerned with a particular legislative or policy matter.

Meetings of public bodies have special legal requirements, including:

- The requirement to give public warning of meeting dates, times and locations in a prescribed manner.
- The prohibition against taking action with less than a quorum.
- The notice of a meeting that is not subject to the Open Meetings Law should not be called a “warning.”
- The word “quorum” should be avoided in relation to the meeting.
- The meeting notes should not be called “minutes.”

---

**Acknowledgement and Agreement of Confidentiality and Security Policies and Procedures for PEMS Client-Level Data**

---

I have reviewed the Power Point slide presentation entitled “Confidentiality and Security Policies and Procedures for PEMS Client-Level Data – An Overview for PEMS Users” and completed the related quiz and I agree to comply with the terms and conditions governing the appropriate and allowed use of PEMS client-level data as defined by the Confidentiality and Security Policies and Procedures for PEMS Client-Level Data.

I agree to abide by the procedures stated in this document.

---

**(Signature)**

---

**(Printed Name)**

---

**(Date)**

---

**(Title/Role related to PEMS)**

---

**(Agency Name)**