

The Importance of Ensuring Confidentiality of PEMS Client-Level Data

In the context of HIV prevention and PEMS data collection the assurance of confidentiality is critical for:

- Protecting Clients: It is critical to respect and safeguard individual privacy and protect individuals from harm, discrimination, or other negative implications of having sensitive personal information disclosed. Providers, agencies, and organizations that handle data with identifiers, including those that are collected in PEMS, are on the front lines in ensuring that unauthorized disclosure of personal health information does not occur, and that above all, clients are protected. No client should have reason to fear that behavioral risk information, which may include socially stigmatizing conditions or behaviors, will be disclosed to anyone other than authorized individuals with reasonable need for the information. Neither should a client feel the need to withhold information for fear of the legal liability that could result from unauthorized disclosure of his/her behavioral risk information, such as illicit drug use. In sum, it is essential that clients feel confident that any data collected about them is treated in an appropriate manner.
- Protecting Providers/Agencies: Confidentiality policies and procedures ensure that individuals, agencies, and organizations are in compliance with state and federal laws and regulations regarding individual privacy protections. If individual providers fail to meet basic standards of conduct in protecting confidentiality and data security, or if agencies fail to put into place policies outlining such standards, corrective action may be warranted.
- Facilitating Provision of Appropriate/ Effective Services: The ability of local agencies to use client services data to plan and improve services depends upon the collection of complete and accurate information for program evaluation and monitoring. The chance of obtaining high-quality data in the context of delivering services can be greatly undermined if clients have concerns about confidentiality and data security, and therefore withhold pertinent information. Likewise, data collection can be compromised if providers avoid asking clients about sensitive health information for fear of violating privacy laws. Thus, confidentiality concerns must be addressed in order to facilitate open communication between clients and providers, thereby enhancing the opportunity for collection of high-quality data.
- Meeting Public Expectation: The right to privacy is a fundamental value of all free societies. It is a right that is guarded and protected by the United States Constitution, state constitutions, federal and state statutes, and common law judicial decisions. Those working in HIV Prevention at all levels must strive to meet our society's expectation for a high standard of conduct in the protection of private and sensitive health information.
- Meeting Personal and Professional Expectations: Attending to the details of good public health practice, including assuring that the data collected for PEMS are used only for the purposes for which they were collected, creates a professional standard for all working in HIV prevention. Good HIV prevention practice strengthens and builds trust in our national public health system, both among those working within the system, and those who benefit from it.

In summary, it is critical to protect privacy and respect individual dignity, not only as an end but also as a means to maintaining the quality and integrity of PEMS client-level data.

Confidentiality Defined

Confidentiality pertains to 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.

PEMS User Confidentiality Statement

As a person who will have access to PEMS 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 the PEMS 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 PEMS client-level data
3. I shall not divulge or disclose this information in any manner whatsoever to an unauthorized person without the written permission of the PEMS System Administrator.
4. I shall access only those PEMS 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 PEMS System Administrator

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

Upon concluding my work as a PEMS 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 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)

(PRINT) Last Name

First

MI

Signature

Date

Witness Signature

Date