

PEMS Security Summary

A. Assurance of Confidentiality Statement

The information in this report to the Centers for Disease Control and Prevention (CDC) is collected under the authority of Sections 304 and 306 of the Public Health Service Act, 42 USC 242b and 242k. Your cooperation is necessary for evaluation of the interventions being done to understand and control HIV/AIDS. Information in CDC's HIV/AIDS Program Evaluation and Monitoring System (PEMS) that would permit identification of any individual on whom a record is maintained, or any health care provider collecting PEMS information, or any institution with which that health care provider is associated will be protected under Section 308(d) of the Public Health Service Act. This protection for the PEMS information includes a guarantee that the information will be held in confidence, will be used only for the purposes stated in the Assurance of Confidentiality on file at CDC, and will not otherwise be disclosed or released without the consent of the individual, health care provider, or institution described herein in accordance with Section 308(d) of the Public Health Service Act (42 USC 242m(d)).

B. PEMS Security Model

PEMS is a highly secure data system that consists of six (6) layers of security, implemented and managed by CDC. A summary of the PEMS security framework is explained in the following section.

1. CDC's Secure Data Network

The Secure Data Network (SDN) is a secure gateway to PEMS-related activities, and uses several security features that limit unauthorized access to the confidential data in PEMS. PEMS does this by:

- Halting usability of the system when there is no activity of the system for 5 minutes.
- Employing intrusion detection software against application-level breaches by identifying legitimate requests and permitting only those actions to take place.
- Server and application vulnerability testing

2. Digital Certificate and Challenge Phrase

The SDN also employs two levels of authentication to determine if the person trying to gain access has the proper authority and credentials. The first level of authentication is by verifying the user has a valid *digital certificate*. The digital certificate is an electronic "pass" to access the SDN. **Every person who needs access to PEMS must have a digital certificate**, and must obtain one through the Statewide PEMS Implementation Coordinator at the bureau. Each user's certificate expires annually, and must be renewed by the bureau. It is the provider's responsibility to prompt the bureau to renew each user's certificate.

In obtaining the digital certificate, the PEMS user will create a *Challenge Phrase*. The Challenge Phrase is used as the second level of authentication and must be entered to gain access to the SDN. This second layer of security is to ensure that the person who is using the digital certificate is the correct person. Once verified, the user gains access to the SDN, and can pass through to PEMS.

3. Secure Sockets Layer and Transport Layer Security

PEMS uses the Secure Sockets Layer and Transport Layer Security (SSL/TLS) of the user's web-browser. The PEMS application will use the SSL/TLS between web-browser clients and the web server that accepts data from users.

4. PEMS Username and Password

During the process of logging into PEMS, and after the user has presented their challenge phrase to enter the SDN, the user will be provided an SDN home screen with the PEMS Software link. Then each user needs to provide the unique PEMS username and password that was assigned to them by the local PEMS Agency System Administrator. Each time the user successfully enters their credentials, they will have to agree to the conditions of using PEMS. This is provided by CDC via a pop-up message box.

The user's password must only be known to them. After the local PEMS Agency System Administrator assigns a password to a user, the user must log in to PEMS and change their password.

5. User Roles and Granular Security

The local PEMS Agency System Administrator will assign each user their individual roles within PEMS. This limits what each user can see and do.

6. JAVA-based Encryption

Java-based encryption is implemented throughout PEMS to secure the data entered into it.

C. Additional Security Recommendations

- In addition to the above six (6) security measures, data that is entered into PEMS is backed up regularly by CDC system administrators.
- Every provider that has a partnered relationship with the bureau to provide services must adhere to the [Department of Health Information Security and Privacy policies](#) or create their own information security and privacy policies that align with or are stricter than the department's policies.
- Any user whose duties do not require them to have access to PEMS or any user who leaves the agency must have their access privileges to PEMS revoked.
- Any breach of confidentiality must be reported to the local PEMS Agency Systems Administrator, who will then report the breach to the Statewide PEMS Implementation Coordinator or the bureau's Information Security and Privacy Coordinator.