

Centers for Disease Control and Prevention

HIV Program Evaluation and Monitoring System (PEMS)

PEMS Security Summary

February 2006



TABLE OF CONTENTS

- ABSTRACT 3**
- CHAPTER ONE 5**
 - PEMS User Interaction and Security Architecture5**
 - CPEMS5**
 - DPEMS, XPEMS and Scanning Interaction6**
- CHAPTER TWO 7**
 - The PEMS Security Model.....7**
 - 1. CDC’s Secure Data Network (SDN).....7**
 - 2. Digital Certificate and Challenge Phrase9**
 - 3. Secure Sockets Layer (SSL).....11**
 - 4. PEMS Username and Password14**
 - 5. User Roles and Granular Security18**
 - 6. JAVA-based Encryption.....21**
 - 7. Public Health Information Network Messaging System (PHIN MS)21**
- CHAPTER THREE..... 22**
 - Other Security Measures for PEMS.....22**
- CHAPTER FOUR..... 29**
 - Agency Responsibilities.....29**
 - Account Management29**
 - Signed Agreements29**
 - Incident Response29**
 - Training.....31**
 - Security Recommendations for Your Agency32**
- APPENDIX A – SECURITY AGREEMENTS..... 38**
 - PEMS Security Agreements.....39**
- APPENDIX B – GLOSSARY AND REFERENCES..... 43**
 - Glossary44**
 - References.....46**
- APPENDIX C – DIGITAL CERTIFICATE LETTER 47**
- APPENDIX D – SIGNATORY DOCUMENTS..... 49**

ABSTRACT

Key Objectives

The objective of this document is to inform readers about the security components of the CDC HIV Prevention Program Evaluation and Monitoring System (PEMS). This document identifies the various components of security within PEMS, describes details surrounding oversight of the security components of PEMS software, briefly discusses activities related to the Certification and Accreditation (C&A) process, explains user responsibilities regarding the use of the application, and discusses requirements for the execution of security agreements between CDC and the users of PEMS.

Introduction

We understand that, as a PEMS user, the privacy of client data as well as the security of that data and the application is important to you. This document is intended to give you assurance of data security and system security.

In an effort to address security concerns shared by all users of public health applications, the federal government has established data security policies and standards that govern application security and data storage. PEMS is compliant with these policies and standards. In order to facilitate PEMS compliance with government policies and standards, and to protect client privacy, the PEMS security framework incorporates the following five categories:

- System Certification and Accreditation (C&A) resulting in an Authorization to Operate (ATO)
- Identification and monitoring of the security components of PEMS
- Examination of security issues and events related to PEMS
- Documentation of software/hardware security assessments
- Involvement of a CDC-appointed security steward
- Execution of security agreements between CDC and the PEMS users

PEMS users can contribute to the security of PEMS by:

- Acknowledging agency responsibilities
- Implementing the security recommendations
- Maintaining agreements with system users which protect the system and your data

Acronym Definitions

Please refer to the following table for acronyms used within this document.

Acronym	Term
ATO	Authorization to Operate
C&A	Certification and Accreditation
CBO	Community-Based Organization
CDC	Centers for Disease Control and Prevention
CPEMS	Centralized PEMS
CTR	Counseling, Testing, and Referrals
DHAP	Division of HIV/AIDS Prevention
DPEMS	Decentralized PEMS
FIPS	Federal Information Processing System
GUI	Graphical User Interface
HHS	Department of Health and Human Services
IRMO	Information Resources Management Office
ITSO	Information Technology Services Office
JRE	JAVA Runtime Environment
MOU/MOA	Memorandum of Understanding/Agreement
NIST	National Institute for Standards and Technology
OCISO	Office of the Chief Information Security Officer
PEMS	HIV Prevention Program Evaluation and Monitoring System
PHIN MS	Public Health Information Network Messaging System
ROB	Rules of Behavior
SDN	Secure Data Network
SSL	Secure Sockets Layer
SLA	System Level Agreement
SRA	Security Risk Assessment
XPEMS	External PEMS

CHAPTER ONE

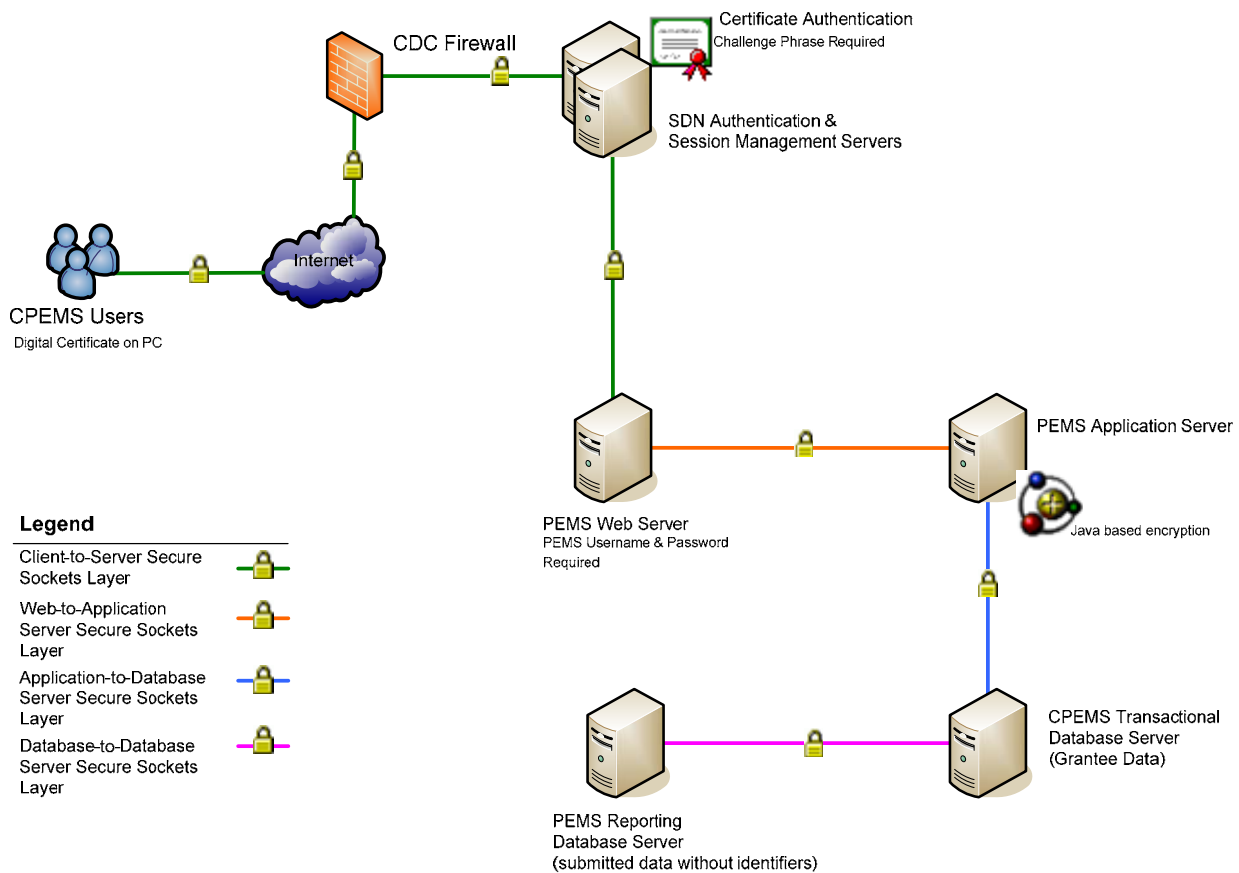
PEMS User Interaction and Security Architecture

PEMS is deployed in three different ways; therefore, the security system diagrams vary depending on whether you are a Centralized PEMS (CPEMS), Decentralized PEMS (DPEMS), or External PEMS (XPEMS) user. The following diagrams show how users interact with the different systems and the security architecture for each.

CPEMS

CPEMS is a centralized web-based solution consisting of a web server, application server, and a database server that reside on the CDC network. Users process data through the PEMS web interface, interacting with PEMS through a series of screens, progressing from the welcome page to completion through a series of data gathering screens.

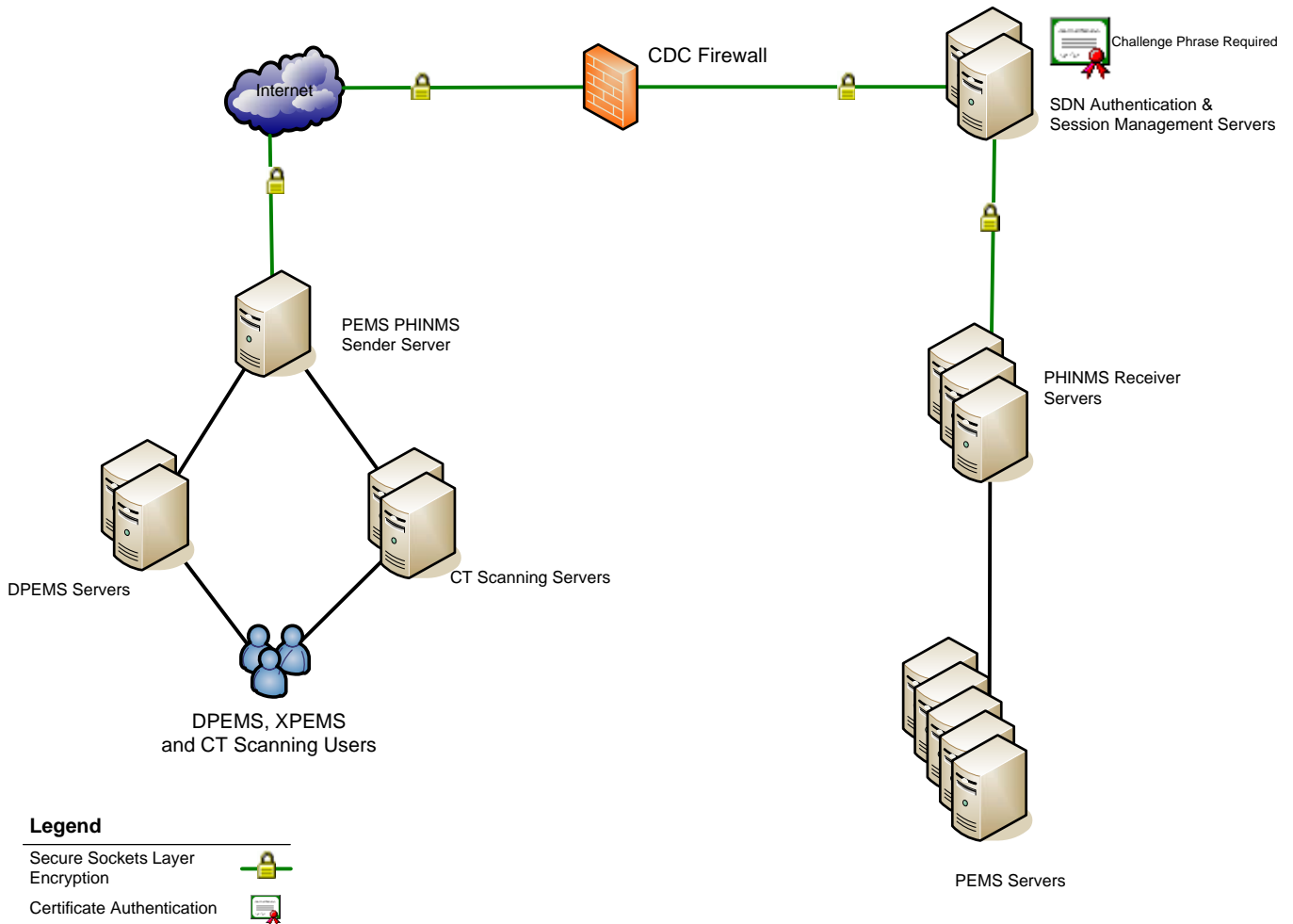
CPEMS Security: A User Perspective



DPEMS, XPEMS and Scanning Interaction

DPEMS is the decentralized solution that is set up within a grantee's own infrastructure. DPEMS users are entirely responsible for system environment, architecture, security, and implementation. XPEMS is an external solution for grantees who prefer not to or who are unable to support the technology required to migrate to other PEMS solutions. Both DPEMS and XPEMS users collect information requested by the CDC, process the data locally, convert the data into a format that complies with the PEMS application, and transfer the requested data using the Public Health Information Network Messaging System (PHIN MS). This system serves as a secure medium of communication to transport data sent via PEMS and scanning servers.

DPEMS, XPEMS & CT Scanning Interaction



CHAPTER TWO

The PEMS Security Model

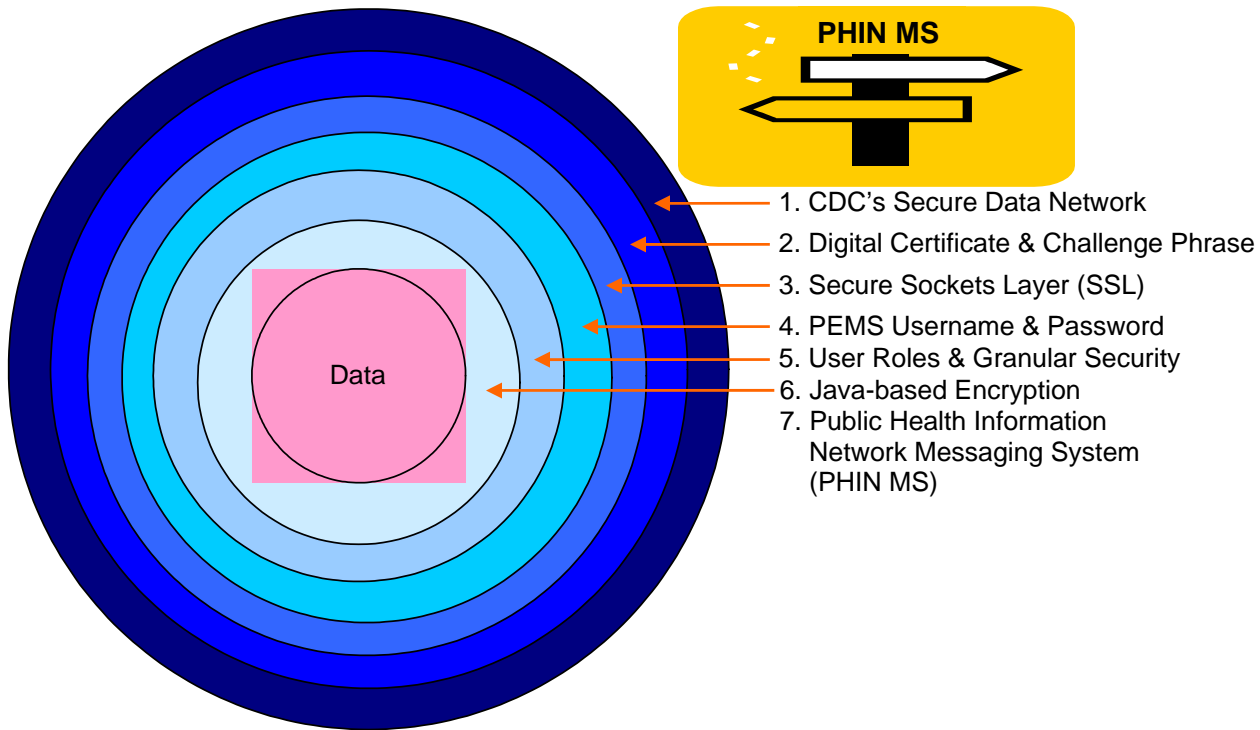


Figure 1: Layered Security Model

The diagram above shows the PEMS security model. Each layer performs a different function and all layers, together, protect client data. Moving from the outside of the diagram to the inside, each layer will be explained.

1. CDC's Secure Data Network (SDN)

The security components of PEMS associated with the SDN are described below.

Session Management

The SDN provides session management capabilities using specific software. The software provides CDC with a centralized security infrastructure for managing user authentication and access to Web applications. When users leave their computers unattended while logged into PEMS, unauthorized individuals could use the system, potentially exposing confidential information. One of the important policy-based controls enforced by the software helps mitigate this risk. Within the SDN, the idle timeout

is set to 15 minutes. Therefore, sessions where no activity¹ takes place for 15 minutes are terminated and further system activity is prevented (until another login occurs).

Intrusion Detection

Most enterprise firewalls act as filters to determine which traffic can enter a network and which cannot. While the firewall examines incoming traffic, it does so only to prevent unauthorized traffic from entering the network; it does not look at the intent of the traffic. If traffic arrives from a single address on each port, the firewall will allow the authorized traffic (blocking the rest), but it may not recognize that this traffic pattern is consistent with port scanning—often the first step in an attack. Intrusion detection software, on the other hand, is designed to recognize unusual traffic patterns and respond, typically alerting administrators and allowing them to take corrective action.

The SDN uses intrusion detection software. This software provides Web intrusion prevention against application-level breaches by identifying legitimate requests and permitting only those actions to take place. By preventing breaches and subsequently alerting administrators to any type of application manipulation through the browser, expected application behavior is maintained.

Vulnerability Testing

Examples of various problems have surfaced due to exploits of information technology – both hardware and software. In order to protect against these attacks, two types of vulnerability assessment were performed on the PEMS infrastructure:

- Server Vulnerability Testing
- Application Vulnerability Testing

Server Vulnerability Testing

This type of testing focuses on uncovering weaknesses in the configuration of the server software. In order to perform server vulnerability testing, various security analysis tools were run on all servers supporting PEMS to scan for common system configurations issues and identify missing security updates.

Application Vulnerability Testing

Often known as buffer overflow attacks, application vulnerabilities have cost businesses and personal users billions of dollars. One step in preventing these attacks is pre-deployment application vulnerability testing. Within the CDC, the SDN provides application vulnerability testing using specific software. This software program detects security vulnerabilities automatically as an integrated component of an enterprise security process review.

¹ Within the context of Web applications, the phrase “no activity” means no activity between the Web server and the Web browser. If users are sitting at their PCs entering data on a Web form, no information is flowing to the server. Therefore, if a user requires 20 minutes to complete a Web form, the session will expire and the user will be required to log in again before saving the form.

2. Digital Certificate and Challenge Phrase

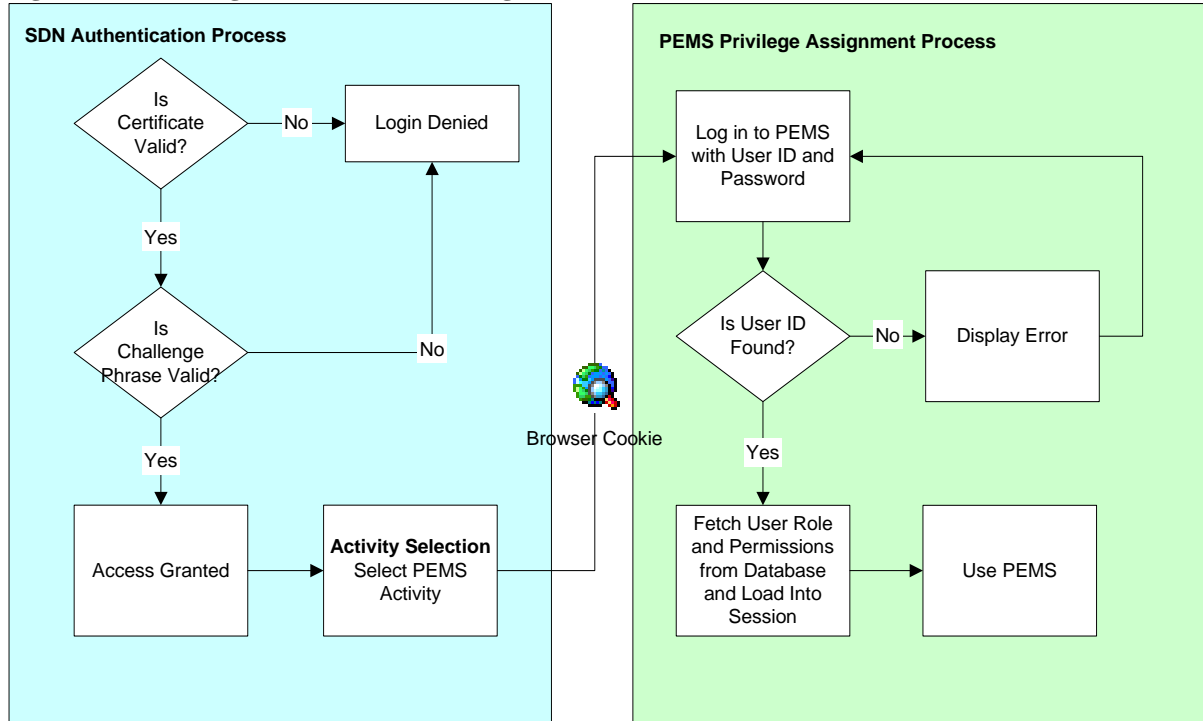
PEMS uses two levels of authentication.

- First, a digital certificate and challenge phrase are used to validate users before providing access to the SDN. After validation, access is granted to PEMS activity and role assignments.
- Second, PEMS requires users to enter a unique username and password in order to log in to the application.

In order for offenders to circumvent these security mechanisms, they would have to possess a valid digital certificate for which they knew the associated challenge phrase and discover a valid username and password combination for the PEMS application.

The following figure depicts the system login and permission assignment process.

Figure 2: PEMS Login and Permission Assignment Process



To guarantee maximum security, digital certificates should not be put on hand-held or laptop computers.

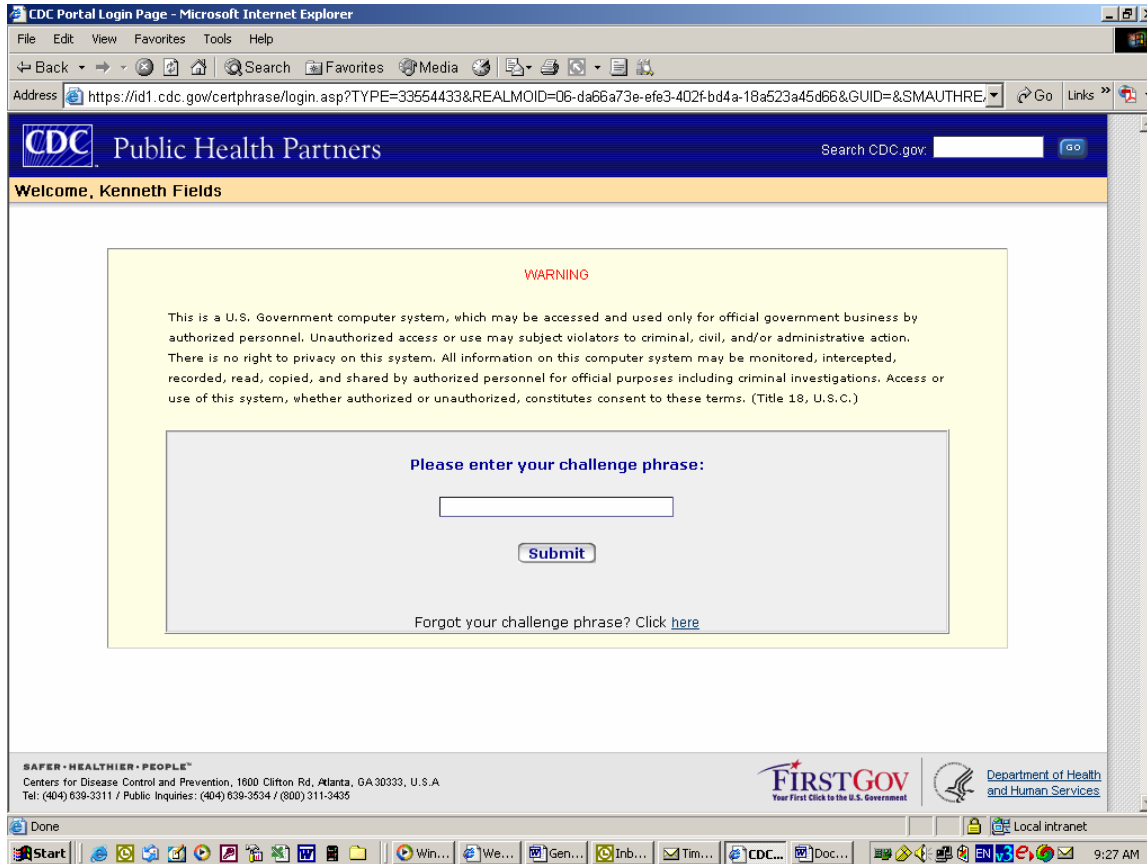
In addition, if a person leaves an organization, that digital certificate should be removed (de-activated), and a new one should be installed by the new user. Contact your PEMS Agency System Administrator, as defined in Chapter Two, Section 5 (page 18), for assistance with digital certificate terminations and requests.

Certificates expire yearly. Each user must apply for a new digital certificate each year.

When signing in to the Secure Data Network (SDN), the first screen that users encounter is the screen below. In order to successfully log in, users must supply the challenge phrase which they established when applying for their digital certificate.

NOTE: The notice displayed is required on all government systems and refers to the fact that administrative and security personnel have access to the SYSTEM, not the DATA. Your client data is protected as described elsewhere in this document.

Figure 3: SDN Challenge Phrase Screen



3. Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) provides encryption throughout the system. Connections are secured by SSL between the client's Web browser and the Web server within the SDN. Additional SSL connections secure message traffic between (1) the Web server and the application server, and (2) the application server and the database servers.

The PEMS application uses Secure Sockets Layer (SSL) between web-browser clients and the web server that accepts data from users. Additional SSL sessions secure data between the web server and the application server, and the application server and the database server. Each of these SSL sessions uses the same type of encryption used by all major financial services and electronic commerce sites today. From a user's perspective, then, confidential information is encrypted from the time it leaves the PC to the time it is stored in the central database.

PEMS also supports persistent encryption of specific data variables (identified as sensitive by the CDC) using the 3DES algorithm. This algorithm is also known as Triple DES, employs a 168-bit encryption key and is FIPS 140-2 compliant. Thus, in addition to being encrypted with SSL during transit, some information remains encrypted within the database, visible only to the agency that entered it. The system encrypts client-identifying variables and includes (in the online help) an encryption indicator for each variable. The online help also includes a warning to users that information entered in non-identifying data fields will not be encrypted. The following is a list of variables that will be encrypted in PEMS:

Client Information

G103 - Local Client Unique Identifier
G105 - Last Name
G106 - First Name
G107 - Middle Initial
G108 - Nick Name
G109 - Aliases - Date of Birth
G110 - Month
G111 - Date of Birth-Day
G125 - Physical Description
G128 - Address Type
G129 - Street Address 1
G130 - Street Address 2
G131 - City
G132 - County
G133 - State
G134 - Zip Code
G135 - Phone Number (Day)
G136 - Phone Number (Evening)
G137 - Primary Occupation
G138 - Employer
"Table G1 Notes"

Partner Information

PCR203 - Last Name
PCR204 - First Name
PCR205 - Middle Initial
PCR206 - Nickname
PCR210 - Date of Birth-Month
PCR211 - Date of Birth-Day
PCR219 - Physical Description
PCR220 - Address Type
PCR221 - Street Address 1
PCR222 - Street Address 2
PCR223 - City
PCR224 - State
PCR225 - Zip Code
PCR226 - Phone Number (Day)
PCR227 - Phone Number (Evening)
PCR228 - Primary Occupation
PCR229 - Employer
"Table PCR2 Notes"

The illustrations below describe how PEMS will manage encryption (Figure 4) and decryption (Figure 5) of the above data variables and note fields.

Figure 4: PEMS Data Encryption

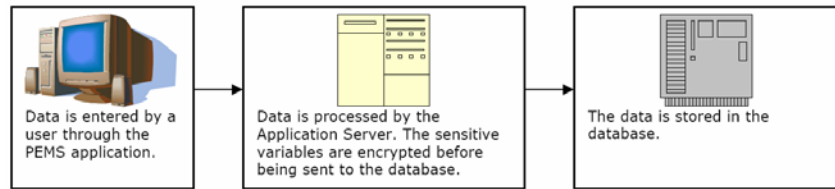
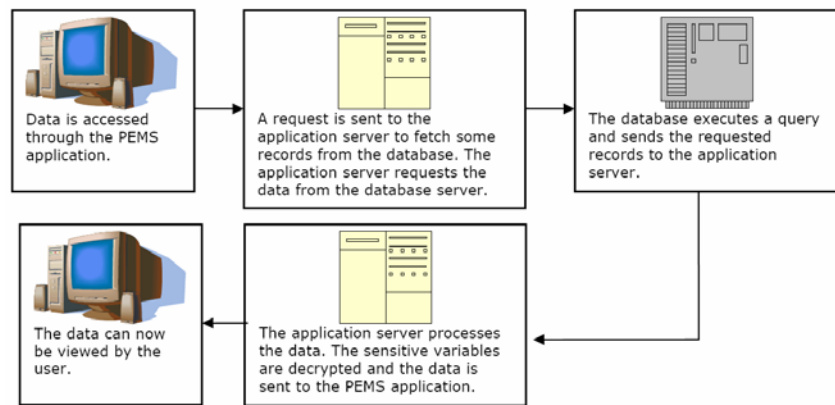
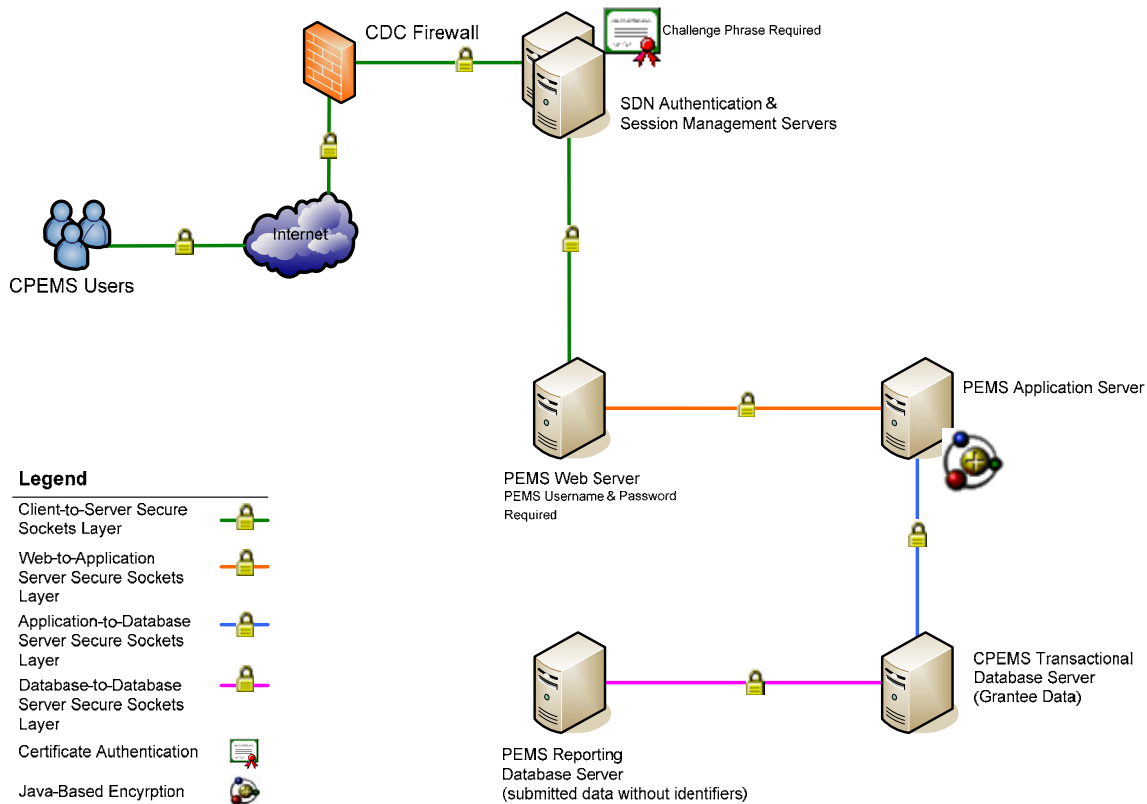


Figure 5: PEMS Data Decryption



The entire encryption system that PEMS uses is best illustrated with a diagram.

Figure 6: Encryption in PEMS



Searching Encrypted Data

An important feature of the application is the ability to search encrypted fields (such as a first name) in order to locate a client. The functionality of encrypted variables introduces certain restrictions regarding the ability to search the database: encrypted data does not allow LIKE searches which would permit users to find a similar match to the specified search criteria. To ensure a quality user experience, the system allows certain wildcard searches with restrictions. A restricted search allows users to search up to the first four characters of a last name, or the entire name, but not the first five characters. In order to perform these searches, PEMS implements a one-way division of the first one, two, three and four characters of the last name of all client entries in the system. These partial last name divisions are stored in a separate column in the PEMS database. When a PEMS user executes a search request for the first four letters of a last name, the system will generate a one-way division from the user input and compare it to the information stored in the separate column in the PEMS database. The system works similarly if users search for the first letter, first two letters, or first three letters of a name. This partial-matching solution allows for some flexibility in user searches while at the same time supporting encrypted identifying data and efficient search algorithms.

4. PEMS Username and Password

Prior to accessing PEMS with a username and password, the SDN authentication (digital certificate / challenge phrase validation) and PEMS activity selection must be complete. PEMS uses role-based access in which user accounts with roles and permissions are set up, usernames are assigned, and a means of authenticating users, such as passwords, is provided. In order to successfully log in to PEMS, a user must supply a valid username and password and agree to the conditions displayed in the pop-up message box, shown below. Users logging in to PEMS for the first time are required to change their password upon first entry into the system. (This password change does not apply to XPEMS users.)

Figure 7: PEMS Login Page

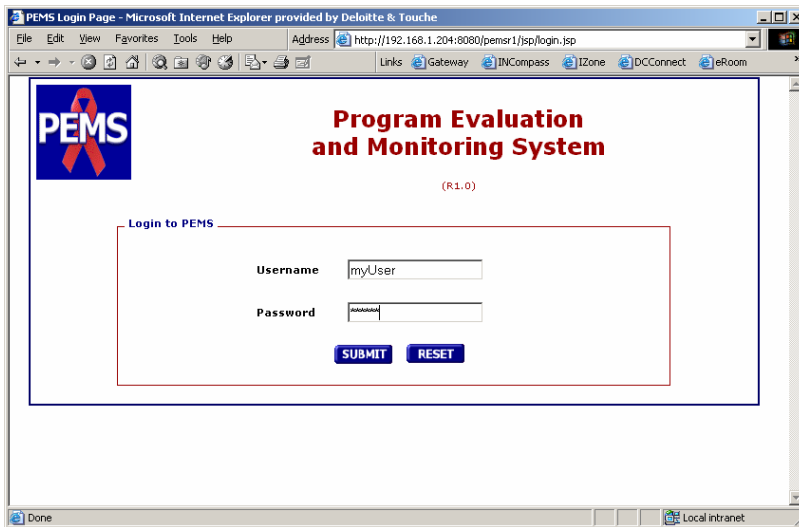
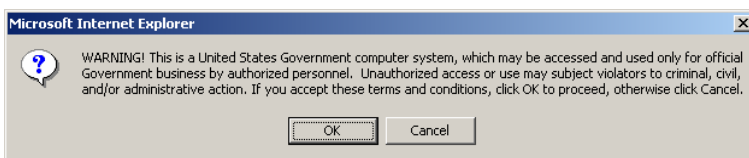


Figure 8: Conditions of Use



For the sake of clarity, the text of the message is displayed to the right of the figure.

WARNING! This is a United States Government computer system, which may be accessed and used only for official Government business by authorized personnel. Unauthorized access or use may subject violators to criminal, civil, and/or administrative action. If you accept these terms and conditions, click OK to proceed, otherwise click Cancel.

The following table provides details regarding user passwords.

Topic	Details
Password complexity	The password must: Be 8 characters or longer Contain three of the following four classes: a-z A-Z 0-9 !, @, #, \$, %, ^, &, *, (,), -, _ =, +, etc. Not contain the user's given name, surname, or system username
Password changes	Users must be able to change passwords in their system.
Password loss	Administrators may reset/change your user passwords.

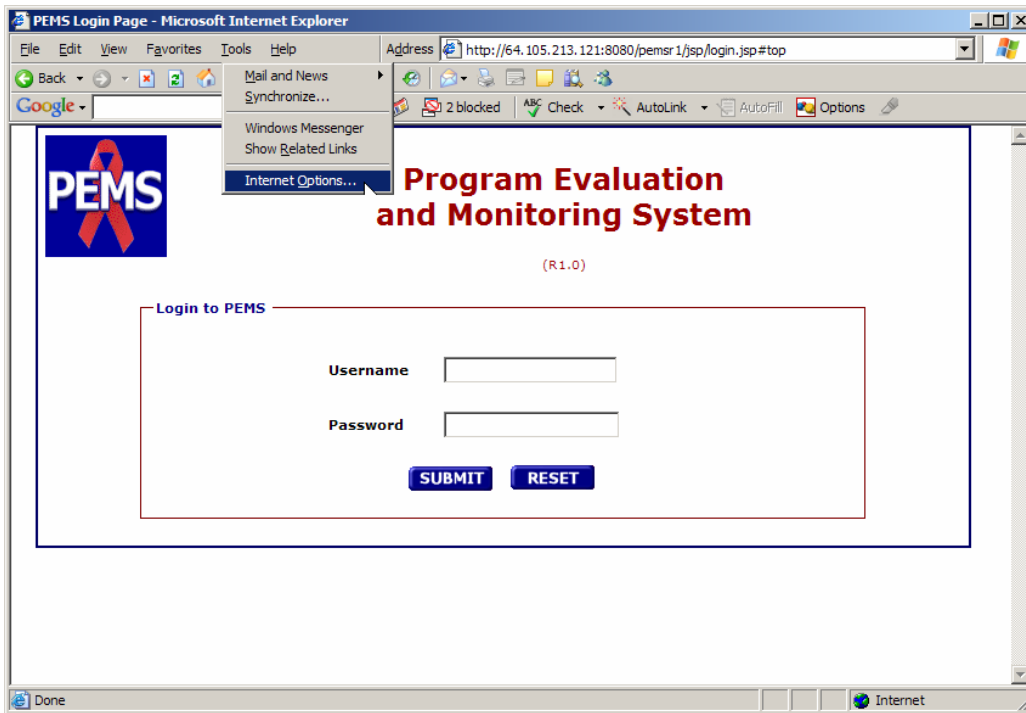
Passwords should be known only to the individual user. **Do not leave passwords written on a “sticky note” on the desk or wall.** No expiration date is automatically set for PEMS passwords. Users should change their password every 90 days.

If a user's employment is terminated at an agency, the passwords should be de-activated, and the Agency System Administrator should be notified.

Disable Browser Password Caching

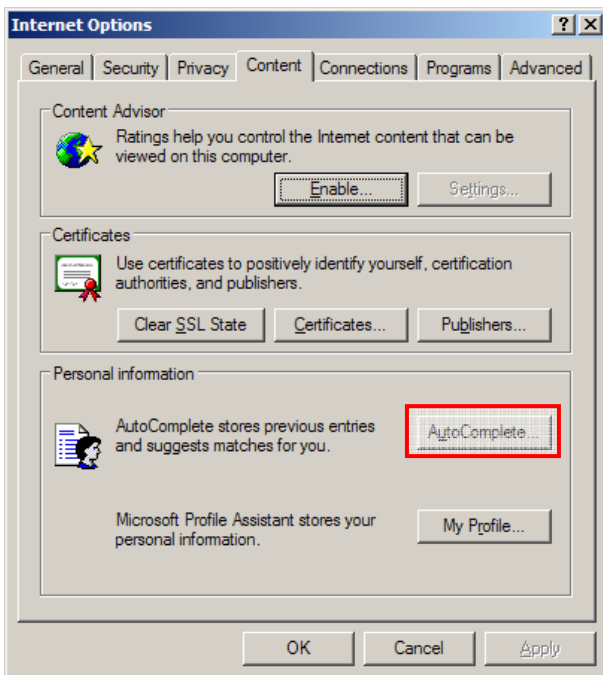
In addition to changing passwords on a regular basis, the function in Windows that “remembers” or stores a password so that the password does not have to be entered each time the user logs in should be disabled. To disable this option, open a new Web browser, and select Internet Options from the Tools menu.

Figure 9: PEMS Login Page



The Internet Options window displays. Switch to the Content tab, and click the AutoComplete button.

Figure 10: Internet Options Window

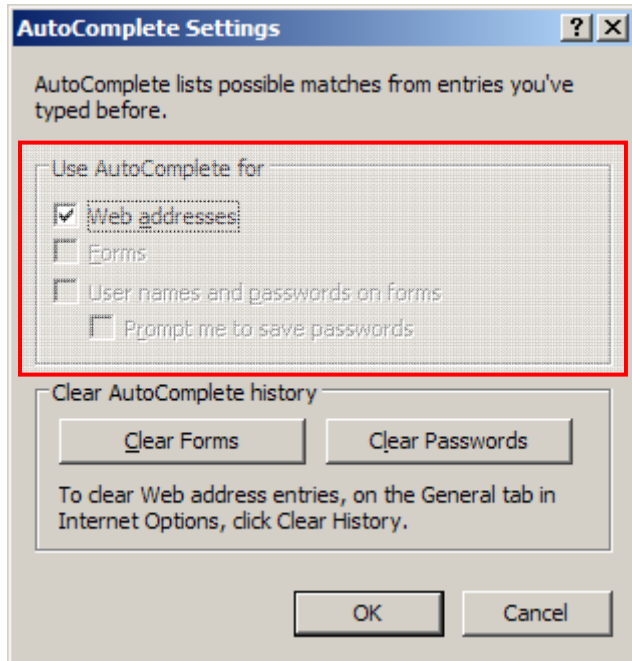


The AutoComplete Settings window displays. While some of the settings in the ‘Use AutoComplete for’ frame may have been disabled by your System Administrator, you should ensure that only Web addresses remains checked (i.e., clear the checkmark from the other boxes).

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.

Figure 11: AutoComplete Settings Window



5. User Roles and Levels of Access

In addition to requiring users to obtain certificates and create challenge phrases and passwords, selecting responsible individuals for various activities associated with the operation and use of PEMS is also required. CDC has designated its responsible parties. Each agency is also required to designate a PEMS Administrator as the overall responsible party for PEMS operations and assigning user roles.

Users of PEMS are only able to access:

1. The data that they enter
2. The data that belongs to their individual organization
3. Specific data to which they have been given rights

Access of other grantee organizations is restricted. Users are treated as having no privileges if not specifically granted a privilege. The responsibility to grant and restrict access is given to the PEMS Agency System Administrator.

The four access privileges available to be given to PEMS users are:

1. View – This level allows users to view data (in read-only format).
2. Add/Edit – This level allows users to add new data and modify existing data (they are also permitted to view data).
3. Delete – This level allows users to delete data (they are also allowed to add/edit and view data).
4. Manage – This level is for PEMS administrators only.

The following table summarizes the PEMS core roles, including tasks and permissions. At health departments and/or at directly or indirectly funded CBO's, all or some of these roles may be the responsibility of a single person.

PEMS Core Roles	Tasks	Permissions
PEMS Super System Administrator	Manages setup information for all directly funded agencies and maintains funding status of all agencies using a specific installation of PEMS; creates and owns the rights to manage all administrators for all directly funded agencies	Manage permission to all modules and sub-modules, both Admin and Non-Admin.
PEMS Agency System Administrator	Manages administration of users, roles, and contract agency administrators	Manage permission to select non-admin modules based on Agency Type (i.e., CDC funded jurisdiction, CDC funded CBO, and not CDC directly funded CBO). Manage permission to the Users, Roles, and Announcements sub-modules of the Admin module.

Agency Budget Role	Maintains program awards data	View, Add/Edit access to Program Awards sub-module under Agency Information; View access to all other non-admin modules.
Agency Information Role	Maintains all agency information data, excluding the program awards data	View, Add/Edit, and Delete access to Agency Information and all sub-modules (except the Program Award sub-module - View access only); View access to all other non-admin modules.
Aggregate Health Communication/Public Information (HC/PI)	Maintains data related to aggregate health communication and public information activities.	Delete rights to the aggregate service module, delete rights to HCPI intervention types, and view rights to all other modules.
Aggregate Health Education /Risk Reduction/Outreach (HE/RR/OR)	Maintains data related to aggregate health education/ risk reduction and outreach activities.	Delete rights to the aggregate service module, delete rights to HE/RR & OR intervention types, and view rights to all other modules.
Aggregate Service	Processes data related to the provision of aggregate services.	Delete rights to the aggregate service module, delete rights to all intervention types, and view rights to all other modules.
Client Service	Maintains client service data.	Delete rights to the client service module, delete rights to all intervention types, and view rights to all other modules.
Community Planning Data Role	Maintains all community planning data	View, Add/Edit, and Delete access to Community Planning module; View access to all other non-admin modules.
Counseling and Testing (CT)	Manages counseling and testing data.	Delete rights to the client service module, delete rights to CT intervention types, and view rights to all other modules.
Data Transfer Role	Creates new data extract requests and initiates data transfers of extracts and data sharing between PEMS and end users; initiates data submission and scanning import	View, Add/Edit, and Delete access to the Data Transfer module, Data Extract, Data Sharing, Data Submission, and Scanning Import sub-module.
Partner Counseling and Referral Services (PCRS)	Maintains data for partner counseling and referral services.	Delete rights to the client service module, delete rights to PCRS intervention types, and view rights to all other modules.
Prevention Case Management (PCM)	Manages data related to prevention case management activities.	Delete rights to the client service module, delete rights to PCM intervention types and, view rights to all other modules.

Program Budget Information Role	Maintains budget information data – only the data filled out at the end of the year	View, Add/Edit, access to Budget Information sub-module under Program Information; View access to all other non-admin modules.
Program Information Role	Maintains all program information data, excluding the budget information data	View, Add/Edit, and Delete access to Agency Information and all sub-modules (except the Budget Information sub-module - View access only); View access to all other non-admin modules.

The user roles allow access only to particular screens and prevent access to other screens. In order for a user to obtain access to PEMS, the following steps must occur:

1. A PEMS Agency System Administrator sends a letter to the CDC requesting access to CPEMS for a set of users.
2. The designated set of users is invited to apply for digital certificates.
3. Digital certificates are granted access to the PEMS Software activity within the SDN.
4. A PEMS Agency System Administrator signs in to CPEMS and creates accounts for designated users.
5. A PEMS Agency System Administrator assigns new users to existing core roles.
6. A PEMS Agency System Administrator may create new roles to remove privileges associated with core roles and assign users to those roles (in order to further restrict access).
7. Designated users (of the grantee) log in to PEMS and the application security component determines which set of roles apply.

6. JAVA-based Encryption

PEMS includes JAVA-based encryption (168-bit, 3DES high level encryption). In addition to this, data is transported at all times using SSL encryption. This is called double-layer encryption. We will supply the encryption application necessary for the transmission of data in the required format. PEMS users should use this application to encrypt the data in a manner that will only allow someone with the appropriate "key" to unlock the data. The CDC DHAP/IT Help Desk can provide assistance with encryption issues.

Encrypted data can only be UN-encrypted if four conditions exist:

- The data must be UN-encrypted at the site where it was entered; no other site would have the algorithms
- The user must have a valid digital certificate and know the challenge phrase
- The user must know the password for that digital certificate
- The user must have been given permission by the Agency System Administrator to access these particular data.

7. Public Health Information Network Messaging System (PHIN MS)

Many public health organizations use the Internet as a secure environment to exchange sensitive data between different public health information systems. This data exchange, also known as "messaging," is enabled through the use of "messages" created using special file formats and a standard vocabulary. Messaging also involves a common approach to security and encryption, methods for dealing with a variety of firewalls and Internet protection schemes, a standard way for addressing and routing content, and a standard and consistent way for information systems to communicate and confirm an exchange. The PHIN Messaging System, PHIN MS, is the software that makes this communication work.

PHIN MS serves as the data transport vehicle for PEMS that securely sends and receives sensitive data for DPEMS and XPEMS users. The messaging system is packaged with the CT scanning application and allows for the secure transfer of Counseling and Testing data from agencies.

CHAPTER THREE

Other Security Measures for PEMS

PEMS is a part of the CDC System Enterprise Architecture and is held to a high standard of performance with regard to security. The following standards were applied to PEMS.

Standards Required by Law for Federal Systems

- Clinger Cohen Act of 1996 (Public Law 104-106)
- OMB Budget Circular A-130
- Federal Information Security Management Act (FISMA)
- HHS Information Security Program Policy
- Executive Orders, Directives, Regulations, Publications, Guidance(s)

Compliance Requirements Include filing/signing documents

- Full Certification & Authentication process = 50 documents
- CDC Capitol Planning Investment Control (CPIC) OMB reporting = 62 forms
- Enterprise Systems Catalogue = 26 pages
- Complete 15 ongoing processes regularly
- 7 agreements that must be executed

System Certification and Accreditation

All federal information systems must receive Certification and Accreditation (C&A). PEMS successfully completed this extensive process and was given an Authority to Operate (ATO) until 08/27/07, prior to which, CDC will have to update its process documents. The table below shows the documents that were required to be filed during the C&A process. The documents themselves are not included here.

Document Name	Description
C&A Questionnaire	<p>The C&A Questionnaire is a comprehensive document completed by the Deloitte technology team and the CDC business users team. The questionnaire collects information necessary to complete the documents (below) that are required for the C&A process. It covers the following topics :</p> <ul style="list-style-type: none"> System Identification and Overview Name & Unique Identifier Functional Description System Environment System Dependencies Data Processing Controls Data Classification and Management

Document Name	Description
	<p>Data Inputs & Outputs Media and Hard Copy Controls Personnel Security Controls Separation of Duties Individual Accountability Training User Policies and Rules of Behavior Administrative Controls Security in the System Development Life Cycle Documentation Operational Controls Change Control Integrity Controls System Monitoring System Verification Incident Preparedness and Response Capability Technical Controls Authentication Control System Access Authorization Network-Based Protections Host/OS-Based Protections Physical Controls Physical and Environmental Protections</p>
<p>Host Characterization and Firewall Worksheets</p>	<p>These documents, completed by ITSO and SDN staff, provide details surrounding machine configurations, firewall rules, and necessary ports.</p>
<p>Risk Assessment Report</p>	<p>This document is the result of the PEMS evaluation by the SRA security consultants at CDC (IRMO). It incorporates the risks identified during the evaluation and the controls required to mitigate them. These risks are presented alone in the Risk Mitigation Worksheet and provided in the appendix of this document as the PEMS Security Risk Register.</p>
<p>Risk Mitigation Worksheet</p>	<p>This worksheet presents, in tabular format, the risks highlighted by the Risk Assessment Report. It also lists the controls required to mitigate each of the identified risks.</p>
<p>Security Plan</p>	<p>This is a living document that evolves with the system and provides details about how the system addresses each area identified in the C&A Questionnaire. This document was developed by SRA/IRMO and revised and approved by PEMS and the Office of the Chief Information Security Officer, OCISO.</p>
<p>System Level Agreements Or System Interconnectivity Agreements</p>	<p>Two agreements exist: one negotiating service levels and responses between DHAP and the SDN; and the second negotiating service levels and responses between DHAP and the</p>

Document Name	Description
	Corporate Square Data Center, where PEMS databases are housed. Other agreements will be maintained as necessary.
Plan of Action and Milestones (POAM)	This document presents the steps that need to be completed before all risks identified in the Risk Assessment Report will be considered mitigated. While not everything needs to be complete before the system is granted ATO, at a minimum, an implementation date must be specified for all required controls.
Memorandum of Understanding/ Memorandum of Agreement (MOU/MOA)	This is a written document which establishes policies or procedures of mutual concern. It provides a general description of the responsibilities that are to be assumed by each party in pursuit of some goal or goals. It is not a contract.
Deloitte Service Level Agreement (SLA)	This agreement, which includes portions of the contract between Deloitte and the CDC, identifies the scope of services to be delivered as well as the boundaries of responsibility between all parties.
Contingency Plan	This is a plan for responding to a system emergency. The plan includes performing backups, preparing critical facilities that can be used to facilitate continuity of operations in the event of an emergency, and recovering from a disaster.
Rules of Behavior (ROB)	Generally, Rules of Behavior dictate an individual's responsibilities as a system user and provide guidelines and policies surrounding what is and what is not acceptable system user behavior. Specifically, the PEMS Rules of Behavior provides system users with information about controlling hardware and managing system access, including granting and revoking privileges, controlling data, and managing personnel.

System Auditing

PEMS supports auditing. Through the application, each record is marked with the following fields:

- Who created
- Date created
- Who updated
- Date updated

Storing this information allows administrators to identify which user entered or modified system data, thus permitting them to associate changes with a given user. These basic auditing features have been included since program inception (i.e., since PEMS R1.0). During the provision of HIV prevention services, there are types of data variables for which service providers must have access to historical data in order to adequately serve their clients. However, the auditing provided by PEMS R1.x does not capture historical changes to records.

Programmatic Tracking

PEMS provides auditing for particular variables using a capability referred to as Programmatic Tracking. This new functionality allows users to create new records and append updated records to a data set without overwriting previously entered records. Where appropriate, the system also allows users to create updated records based on previously entered data. The following client-level data sets shall support programmatic tracking:

- Client Demographics and Locating Information
- Risk Profile Data and Detailed Behavior
- Confirmed HIV Status

The above data sets are captured and then ordered based on the date collected field. The system tracks updates to client demographic information by storing the most recently collected data record in one table and storing all previously collected data records in a separate history table. This table structure allows the system to perform faster searches on client demographic information – an important characteristic given the frequency of client searches. History for Risk Profile, Detailed Behaviors, and Confirmed HIV Status data is maintained in the same table as the most current record. The divergent approaches are related to system behavior; Risk Profile and Confirmed HIV Status data are always accessed for a specific client. Thus, storing current and historic records in the same table allows for faster, more efficient access to a complete overview of a client.

In addition to allowing access to updated records, the system also allows users to view and edit previously entered data. It is important to note the distinction between record updates and record modifications (referred to as Edits in the system). *Record updates* represent the creation of a new record in order to track the evolution of some characteristic over a period of time, whereas *record modifications* represent the correction of incorrect data. As an example, consider a provider collecting information on one of their clients. For the first visit, the provider documents the name of the pregnancy test given and that the client is not pregnant. The next year, the client has a follow-up visit and the provider documents the name of the pregnancy test given and that she is now pregnant. Individually, each entry represents a

snapshot of the client's pregnancy status at a distinct point in time. The second entry represents an update to the record. Now consider the provider is later reviewing the information collected for the client. The doctor notices that the name of the test given in the first visit was misspelled on the documentation. The doctor corrects the name of the test and overwrites the first entry. This represents a modification to the record. Programmatic tracking will not provide a history of record modifications. As with any system record, if the user performs an edit, the system will replace the old version with the new and update the last modified date.

Beyond the audit captured by PEMS, the systems upon which PEMS relies, namely the SDN and Corporate Square data center, provide various auditing on each tier of the system: the authentication system (digital certificates), the web server, the application server, and the database server.

PEMS Database Back-up Procedure

1. A full back-up of the PEMS databases (staging, training, productions support, production) is performed daily at 5am.
2. The SQL back-ups are copied to the SAN, where they are stored for one month.
3. They are then backed-up on to tapes, which are kept in the tape library system (StorageTek L700E).
4. Once backed-up, the tapes are then moved off-site to an Iron Mountain facility and archived. They are stored at Iron Mountain for three months and then are reused.
5. In the event of a disaster or data center failure, back-up tapes could be sent by overnight express. However, there are limitations on the available hardware and server room space.

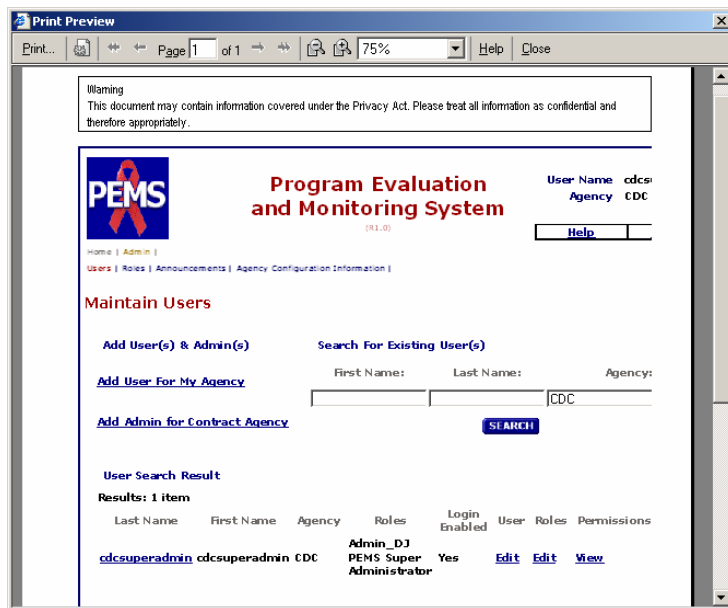
PEMS Application Server (SDN) Back-up Procedure

1. Daily back-up of the application server that hosts PEMS with "App Server Backup" job rotation (tapes retained for 10 days).
2. Weekly back-up is performed every Friday and retained for 2 weeks. Tapes are rotated off-site and held for 2 weeks before being rotated out.
3. Monthly tape back-up is done the last week of the month and is retained for 6 months and archived at Clifton Road (not off-site).
4. For disaster recovery, worst case would be a loss of data for 1 week if loss occurs prior to close-of-business (COB) Friday before back-up is taken and rotated off-site.

System Data Output

All information printed from PEMS is marked with a banner explaining to users the sensitivity of the data and the need for appropriate handling. If an organization needs additional wording, such as local identifiers for the banner statement, the PEMS Service Support Center can be contacted to assist with the request.

Figure 12: Confidentiality Warning Banner on Printed Output



Warning
This document may contain information covered under the Privacy Act. Please treat all information as confidential and therefore appropriately.

For the sake of clarity, the text of the message is presented to the right of the figure.

Physical and Environmental Protection

Physical and environmental controls are in place to protect the computing components that make up PEMS. The CDC and NCHSTP data centers that house PEMS computing resources are protected with a cipher lock and card reader. All visitors must sign a visitor log when entering and exiting the computer room. The CDC & NCHSTP Information Security Officers maintain a copy of the visitor log, which includes the name of each visitor and the date and time of each visit. Physical security of the building and computer room is enhanced through the use of guards, video cameras, and surveillance equipment. All visitors must sign in at the front desk and present a positive form of identification. The guard issues a badge to each visitor, who must be escorted by a CDC employee while in the building.

Environmental controls, including thermostats, hydrometers, sprinklers, emergency power-off switches, alarms, and uninterruptible power supplies, are used to protect PEMS computing resources from system damage or failure.

The data centers that house PEMS computing resources have a backup cooling system in addition to the air conditioning provided in the buildings.

The fire alarms located in the computer rooms are protected to prevent accidental triggering. Evacuation plans and fire drill plans are in place and are handled at the CDC enterprise level to ensure compliance with building re-entry procedures. Additional monitors are on hand during the drills to account for CDC employees and to ensure that only authorized employees re-enter the building.

Help Desks

The DHAP IT Help Desk and PEMS Service Support Center have been established to support PEMS. The help desk is staffed jointly by CDC employees and contractors. The DHAP IT Help Desk will assist users with SDN, Digital Certificates, PHINMS, encoding, and decoding. The PEMS Service Support Center functions to answer questions about PEMS. Guidance regarding the handling of an incident response in PEMS can be found in Chapter Four.

Security Awareness Training

For CDC employees, security awareness training must be completed prior to gaining access to the CDC network. The CDC provides security awareness training programs for all employees to emphasize the importance of security to the organization. By educating employees and keeping a high level of security consciousness, the importance of preventing and avoiding many serious security breaches is emphasized. Security awareness training is mandatory and must be completed each year. If not completed, network access is disabled and the offender's reinstatement must be confirmed by a supervisor.

Multiple sessions of security awareness training will be provided to CDC staff and HIV prevention grantees who will be PEMS users. These training sessions will be held prior to the first release of PEMS, during the implementation phase, and will be repeated with each new version released. Training curricula will include the following:

- Confidentiality definitions.
- Strategies to ensure confidentiality during data collection, storage, and disposal.
- Examples of state and agency confidentiality policies that can be adopted/adapted.
- Strategies for addressing client and staff resistance to the collection of client-level data.
- Sessions to engage participants in thinking about how to prepare their providers to ensure confidentiality with a focus on 1) key points to be communicated to providers, 2) challenges providers may experience, and 3) strategies for overcoming those challenges (using or adapting materials from this session).
- DHAP policies related to data security, storage, and confidentiality.
- HIPAA regulations as they relate to PEMS data, identifying strategies for storing and managing data before it is entered into PEMS, including managing large volumes of paper data between the beginning of data collection and the go-live date.
- Action planning related to storing and managing data and ensuring confidentiality.

CHAPTER FOUR

Agency Responsibilities

Agencies that use PEMS have responsibilities that help ensure confidentiality and security of the system and its data. The responsibilities of an agency include:

Account Management

An agency's System Administrator is responsible for managing account access for their users. The account access process includes applying for the SDN digital certificate and signing the Rules of Behavior (ROB). This is usually done in writing through a user's supervisor and should include a description of the user's duties related to PEMS. Once a certificate is granted, the System Administrator establishes an account with levels of access for that user that should only be necessary to perform their required duties. An administrator's responsibility also includes restricting access to parts of PEMS according to the role of the user; modifying access within the system when a user's duties change; and terminating access when employees leave, change jobs, or breach agency policies. User accounts should be reviewed yearly in order to ensure that all accounts are current. In addition, digital certificates expire yearly and must be renewed. PEMS accounts that are inactive for two reporting periods (180 days) will be automatically disabled.

Each agency's System Administrator is accountable for their use of PEMS and the data. Using system resources to copy, release, or view data without authorization is prohibited. Altering data improperly and tampering with the system is also prohibited. Any breaches of security, confidentiality, and unethical conduct related to PEMS must be reported.

Signed Agreements

Agencies with access to PEMS and the data must sign ROB and MOU agreements specifically tailored to their responsibilities. These agreements should be kept on file at the agency and a signed copy should be sent to CDC. PEMS users who request access to confidential data and secured areas must sign a binding, non-disclosure agreement before being given access to PEMS data.

Incident Response

Detect the Incident

The key to incident response is the ability of the Incident Reporter to distinguish between an incident and a routine event. Common indications of an incident include the following:

- Antivirus software detects a host infected with a virus or worm
- Intrusion Detection System identifies Phishing, SPIM, Spyware, or other malicious code
- Web server crashes
- Users complain of slow access to hosts on the Internet or Intranet
- System Administrator sees a filename with unusual characters

- Host records an auditing configuration change in its log
- Logs increase in size in shorter than usual timeframes
- Logs show multiple failed login attempts from an unfamiliar remote system.

There are many such indications; therefore, this list is not exhaustive. Furthermore, some of these indications may turn out to be benign events. For example, slow connection speeds may be due to a faulty modem or network card or to problems at the local ISP. Multiple failed login attempts may be the result of a user having forgotten his or her password and trying repeatedly to guess it. On the other hand, a defaced Web page is very clearly an indication that an incident has occurred.

First Response for PEMS Agency System Administrators

The role of a Agency System Administrator is vital in ensuring all aspects of network security and maintenance. This individual also plays the most important role in the event a computer is used in a security incident or unlawful act. The Agency System Administrator will be the primary point of contact for individuals that need to make a report of computer use violations. In addition, an Agency System Administrator may come across a violation during the normal course of their duties. The actions taken by the Agency System Administrator after discovery of a potential computer violation will play a vital role in the investigation, forensic evaluation of the computer system, and potential prosecution or administrative actions. From a forensic standpoint, the ideal situation is to isolate the computer from additional use or tampering.

In the event of a suspected security incident, great care must be taken to preserve evidence in its original state. While it may seem that simply viewing files on a system would not result in alteration of the original media, merely opening a file changes it. In a legal sense, it is no longer the original evidence and at that point may be inadmissible as evidence. Opening a file also alters the time and date it was last accessed. No attempts should be made to recover or view files except by qualified IT professionals.

Once it is determined that an incident is occurring (or has occurred) or could possibly be occurring, appropriate personnel should be notified immediately. At this point in the process, making the appropriate contact, and only the appropriate contact, is critical.

The hierarchy of notice regarding a suspected or determined security incident in PEMS is as follows:

1. PEMS user (also known as Incident Reporter) reports suspected incident to Agency System Administrator (who will help determine if an incident has occurred)
2. Agency System Administrator reports to Local IT staff (who will determine, if possible, what occurred; what should be done about it; and what should be investigated or reported further)
3. Local IT staff notifies PEMS Service Support Center, if necessary
4. PEMS Service Support Center notifies PEMS Security Steward, if necessary
5. PEMS Security Steward informs OCISO, if necessary.

Training

All agency staff dealing with PEMS data should be trained on policies and procedures established by the agency, the legal aspects of data collection, and the ethics of their responsibility to the clients. Training should cover state regulations and the agency's policies concerning confidentiality, computer security, and legal obligations under non-disclosure agreements. Agency staff should be aware of common threats to confidentiality and security, contingency plans for breaches of confidentiality and security, and the penalties associated with breaches of confidentiality and security. Each agency staff member with access to PEMS data should receive PEMS training, and security updates.

Security Recommendations for Your Agency

Grantees are expected to have written security and confidentiality policies and procedures to protect their data. Here is a checklist of items that grantees should consider when writing policies and procedures regarding the secure and confidential implementation of PEMS at their agency.

Accountability

Users of the PEMS system should be held accountable for their use of the system and its data. Using system resources to copy, release, or view data without authorization is prohibited. Altering data improperly or otherwise tampering with the system is prohibited. Employees authorized to access client-specific data are responsible for the protection of confidential information and must report any breaches.

Administration of Proxies

PEMS provides the ability to identify and assign proxies, i.e., the ability to assign one person's permissions to someone else. Although multiple users can be granted proxies for an individual, only one user can log in at a time, as a proxy of another user. Only an administrator has permission to grant and delete a proxy. Rules should be developed at the site level to determine how long proxies may last and how they should be administered. All users will comply with the rules of proxy administration.

Agency Responsibility

Each agency directly funded by CDC should identify a person with the ultimate responsibility for the PEMS system. This person will sign the MOU with CDC and maintain the terms of the agreement with agencies they fund with CDC grant money. In addition, agencies must maintain ROB agreements with users who directly access the system. Agencies must submit signed copies of system agreements to CDC and renew these agreements annually. Certification of current certificates, accounts, and activity assignments must be done, and annual security training for the system must be completed.

Backing-Up Data

CDC regularly backs up all PEMS data stored on CDC database servers. PEMS data that are not yet transmitted, either because they have not yet been entered in the system or because the data are not being stored on CDC servers (DPEMS, XPEMS) must be backed up periodically by the grantee. Frequency of backup should depend upon how often the data changes and how significant those changes are, but should be done based on a fixed schedule that is part of the normal maintenance of the system. Backup copies should be tested to make sure they are actually usable and stored under lock and key in a secure area and a separate copy of data kept at a secure off-site location, if possible.

Breaches of Confidentiality

A breach of confidentiality is any failure to follow confidentiality protocols, whether or not information is actually released. This includes a security infraction that results in the release of private information,

with or without harm to one or more individuals. All suspected breaches of confidentiality or security (e.g., possible viruses, hackers, password divulgence, lost or misplaced storage media) should be reported immediately to the PEMS Agency System Administrator. This administrator will determine the cause, develop and implement process improvements and/or determine if the incident should be reported to the PEMS Security Coordinator via the PEMS Service Support Center.

At the local level, sanctions for violations of confidentiality protocols should be established in writing, as part of the organizational policies and should be consistently enforced.

Controlling Access to PEMS

Access to PEMS files and software must be restricted to authorized users. Usually this involves establishing user accounts, limiting activities within the system, and terminating access when employees leave, change jobs, or breach agency policies. Typically, those assigned duties that require access to PEMS software or data must be granted those privileges by the PEMS Agency System Administrator. Ideally, this process should come through the user's supervisor as a documented request. The request should include a description of the user's duties related to PEMS. The PEMS Agency System Administrator can then establish an account for the user, specifying permissions and levels of access the user will have (which should only be those sufficient to perform the duties required by the job). General training regarding security and confidentiality is also recommended.

Controlling Data

PEMS-related data does not exist on PEMS servers alone. Such data may exist on collection forms, counselor notes, floppy disks, CD-ROMS, and other information storage media. Use of dial-up access, modem for data collection activities, or working from home with PEMS data should be prohibited or restricted to specifically authorized personnel working under carefully defined circumstances only. Since all these media may contain confidential information, the agency must develop policies and procedures for the use, storage, and disposal of all media used to record or store PEMS data. Emails should not be used to transfer data to the CDC.

Controlling Personnel

Personnel are as much a part of a data collection and reporting system as computer hardware and collection forms. People are usually the weakest link in any security system. All personnel dealing with PEMS data should be trained on the policies and procedures established by the agency, the legal aspects of the data collection, and the ethics of their responsibility to the clients. Furthermore, they should also be aware of the penalties associated with breaches of confidentiality or security. Each agency should have a policy on confidentiality and security. The confidentiality and security policy must make clear that authorized users are responsible for knowing the confidentiality and security policies and procedures, challenging unauthorized users, reporting possible breaches, and protecting equipment and data. Staff should be required to sign a statement acknowledging that they have been made aware of the confidentiality and security requirements for the agency. The signed statement should be kept in the employee's file.

Encryption

PEMS data is sensitive, confidential information that may have legal and personal implications for clients; therefore, it should be protected from unauthorized access. Data transmitted to CDC through the SDN is secured through the use of all security controls described in this document. If an organization decides to send data to anyone other than CDC, using the secure methods provided, the data should be encrypted.

Levels of Access

Many users are unlikely to need access to all parts of PEMS. Access to the various components of the system should be restricted based upon the user's role. For example, typical roles include data entry, generating reports, system administration, and viewing information. Some users may need to read information about clients but not enter data. The PEMS Agency System Administrator should develop a security policy that allows for appropriate access rights for individuals based on their assigned roles within PEMS.

Locking Workstations

All users should secure their workstations before leaving them. Automatic screen saver locks should also be set to engage whenever the system is left idle (15 minutes of inactivity). In order to unlock the screensaver, the system should require entry of the user's ID and password.

Physical Security of Equipment

PEMS Agency System Administrators should maintain an inventory of all system hardware and software provided to system users, and periodic audits should be conducted to account for all assets. Visitors or unauthorized personnel should not be allowed access without an escort to areas containing computers holding PEMS data. All computer equipment should be protected by surge suppressors and emergency battery power to prevent data loss in case of fluctuations in the power supply. All computers and other equipment used for PEMS should be housed or stored in secure areas and physically attached to an immovable object, if possible.

Records Disposal

Many states have laws or regulations concerning how long client records must be stored and when and how they must be destroyed. Agencies must develop policies and procedures that comply with these state regulations. When client records are to be destroyed, this should include not only paper records but also electronic records. Please note that "deleting" a file or record on the computer does not actually remove the information from the system. Even overwriting or formatting the media may not sanitize it; special sanitization programs or physical destruction of the storage media may be required. Agencies must be sure to sanitize or destroy hard drives of computers scheduled for disposal or transfer to staff not authorized to use PEMS.

Release of Data

Agencies must develop a written policy and procedure for releasing data. These policies should be periodically reviewed and modified to improve the protection of confidential information. Policies concerning the release of de-identified and aggregate data that prevent indirectly identifying clients through small denominators should also be established. Access to any data containing confidential information or case-specific data should be contingent on having a signed, current, binding non-disclosure agreement currently on file at the individual agency. These agreements must include discussion of possible employee ramifications and criminal and civil liabilities for unauthorized disclosure of information.

Releasing Data to Partners

In order to assist other agencies in tracking referrals or other related purposes, agencies may enter into agreements with other agencies to share limited information about specific clients. Data sharing should be based upon written agreements and clients should be helped to understand how their confidential information will be treated/shared with other agency partners. Agencies must develop policies and procedures to comply with state regulations regarding release of data.

Releasing Data to the Public

Except under conditions specified in writing and explained to clients, only authorized staff members who have signed a binding non-disclosure agreement (and who have a need to know) should be allowed access to sensitive client identifying data. Agencies should have a policy and protocol for releasing de-identified and aggregate data for use in analysis, grant applications, reporting and administrative functions. This policy should specify what data may be released, in what form, to whom the data may be released, and who may approve the release of data.

Reporting to CDC

Reporting to CDC should be done according to the schedule specified by CDC. While data may be entered in to PEMS at any time, it is not reported to CDC until the appropriate files are submitted to CDC by the authorized personnel of each agency. There should be policies and procedures developed to specify the data quality assurance process that should be implemented and the administrative approval process that should be followed prior to reporting/submitted data to CDC.

Storage Media

Agencies should establish policies and procedures that outline when it is appropriate to export PEMS data to storage media. All storage media should be clearly labeled. Removable media such as floppy disks, zip disks, CD-ROMS, etc., should be destroyed or sanitized with disk wiping tools before reuse or disposal. Removable media, whether paper or electronic, containing PEMS data should be stored in a secured area. Data removed from secured areas for analysis should be de-identified first. Diskettes and other storage media that contain PEMS data should have only the minimum data necessary to perform a given task, be encrypted or stored under lock and key when not in use, and (except for backups) be

sanitized immediately following the task completion. Cleaning crews, maintenance staff, and other unauthorized personnel must be escorted into secured areas by designated staff. Encryption of data during storage is recommended.

Terminating Access

As soon as individuals change duties within an agency or leave the agency altogether, their access privileges should be modified. As part of the transition or departure procedures, the Agency System Administrator should be notified of changes to employment status so the proper actions can be taken to protect the system and its data.

Training on Confidentiality

Each staff member with access to PEMS data must receive training on confidentiality and security. Training should cover the state regulations concerning confidentiality, the basics of computer security, the agency's confidentiality and security policies and procedures, the roles and responsibilities of various staff positions regarding protecting confidentiality and security, contingency plans for breaches of confidentiality or security, common threats to confidentiality and security, legal obligations under non-disclosure agreements, and potential effects on clients and the agency to breaches of confidentiality.

Unauthorized System Intrusion

Any computer with external connectivity (especially one connected to the Internet) is subject to unauthorized penetration from hackers, computer viruses, and worms. Agencies must take all reasonable precautions to protect their systems from intrusion. A plan must be developed and implemented to prevent and, if necessary, recover from changes to the system caused by unauthorized access. Typical precautions include using effective passwords, installing firewalls and anti-virus software, making backup copies of the data at regular intervals so that the system can be restored to a previous state, making shredding equipment available, and training staff in basic computer security such as password confidentiality and the risks of unauthorized installation of software.

Use of Equipment

The computers, servers, and other electronic equipment used to collect, enter, copy, store, analyze, or report PEMS data should be under the control of the agency. The use of equipment related to PEMS, including Internet connections, e-mail, photocopiers, facsimile machines, and other equipment that might be used to copy, transmit, or process PEMS data should be regulated by written policies and procedures. These policies should require personnel to electronically lock unattended computers and ensure that computers have screensaver locks that are activated after 15 minutes (or less) of inactivity.

Use of Passwords

Passwords must be used to confirm the user identity. Passwords should be changed periodically (at least every 90 days) and staff should be cautioned not to share passwords. The PEMS application will lock-out a user after three consecutive unsuccessful log-in attempts. De-identified databases should be held

securely (e.g., password protected) until authorized for public use. Similar security measures should be incorporated into the operating system user policy.

Use of Portable Equipment

While the use of portable computers has its advantages, it also creates additional security risks, such as loss or theft of the computer and data it stores. If computers are used outside the office, agencies should establish policies regarding physical security (the computer should be locked to an immovable object), and digital security (the computer should be protected with a unique username and complex password, and sensitive data should be encrypted). Laptop computers and other portable hardware that receive PEMS data should store that data in encrypted formats.

APPENDIX A – SECURITY AGREEMENTS

PEMS Security Agreements

A recent survey of PEMS users² revealed that, among 235 respondents, 1) the number one security issue was system vulnerability or unauthorized access to data and 2) that most grantees already have policies/protocols in place to address this and other security measures.

Some of the measures in place which were listed by PEMS users include:

- Protocols regarding securing data
- Protocols to address electronic data
- Protocols regarding staff practices
- Confidentiality of data and HIPAA compliance

Data system security consists of two facets. The first is the security of the system and the second is the confidentiality of the data. The chart below explains the differences and the overlaps.

SECURITY DEFINITION	SECURITY RISKS
Maintaining the integrity of the PEMS system to insure the existence and confidentiality of data by taking measures to detect, document and counter accidental data loss or damage or threats to the integrity of the system	<ul style="list-style-type: none"> • Physical systems and facilities <ul style="list-style-type: none"> ○ Acts of nature or disaster ○ Human intruders or insiders • Security intrusion or system breach • System unavailability/ maintenance • Corruption of data • Loss of data
CONFIDENTIALITY DEFINITION	CONFIDENTIALITY RISKS
Maintaining critical information in a confidential environment and preventing unauthorized access to sensitive data	<ul style="list-style-type: none"> • Autonomous intrusion (viruses/hackers) • Unauthorized access to data • Inappropriate release of data

In an effort to provide maximum protection of the data that is entered into PEMS, in addition to the physical and system security measures explained in this document, there are Rules of Behavior for PEMS Agency Users (ROB-AU) regarding appropriate and allowed use of PEMS. There are also Rules of Behavior for PEMS Agency System Administrators (ROB-ASA) covering all of the additional duties of the Agency System Administrators. CDC also will execute a Memorandum of Understanding (MOU) with each directly funded organization. The process will work as follows:

1. Rules of Behavior for PEMS Agency Users (ROB-AU) will be provided to each CDC directly funded organization.
 - a. Each PEMS user of the directly funded CDC grantee will sign a ROB-AU. Organizations with a CPEMS or DPEMS deployment model are asked not to modify or omit existing language in the ROB-AU but may add information relevant to their organization. Organizations with an XPEMS deployment model may execute the same or similar document with their users. The ROB-AUs will be retained by the CDC directly funded grantee.

² PEMS User Survey of class participants, March, 2005
 Sensitive but Unclassified (SBU)

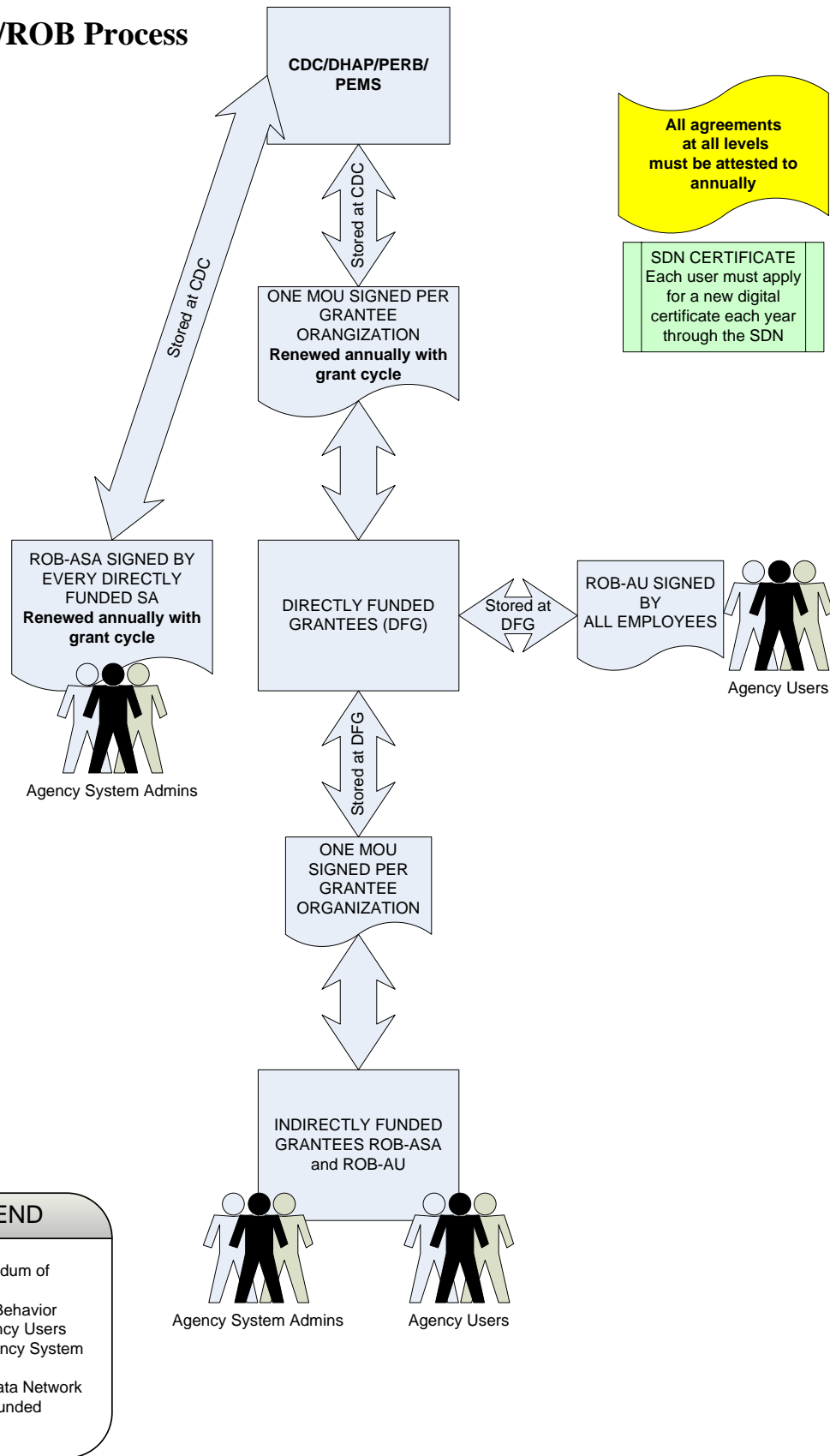
- b. Each directly funded CDC grantee will also execute the same or similar document with their funded organizations to cover their users and notify the CDC when this process is complete. The ROB-AUs will be retained by the CDC directly funded grantee.
2. Rules of Behavior for PEMS Agency System Administrators (ROB-ASA) will be provided to each directly funded organization.
 - a. Each directly funded CDC organization, regardless of deployment model, will have their designated Agency System Administrator sign one ROB-ASA to attest to system administration compliance, including that all users of PEMS have signed the ROB-AU. The signed ROB-ASA will be submitted to the CDC.
 - b. Each directly funded CDC grantee will be responsible to ensure that each of their funded organizations complete a ROB-ASA to document system administration compliance. CDC will be notified by the directly funded grantee when this process is complete. The ROB-ASA should be retained by the CDC directly funded grantee.
3. Memorandum of Understanding (MOU) for CPEMS, DPEMS, and XPEMS
 - a. For each directly funded grantee, an authorized representative who can bind the organization will sign an MOU on the use of PEMS with CDC. The grantee organization will submit the signed MOU to the CDC.
 - b. Each directly funded CDC grantee will also execute the same or similar MOU with all of their funded organizations and notify the CDC when this process is complete. The MOUs should be retained by the CDC directly funded grantee.
4. Certification of current digital certificates, accounts, and activity assignments (roles and permissions).
5. Certification that security training for all users is conducted yearly.

If you have any questions regarding these documents, please see your PEMS regional lead or call the PEMS Service Support Center.

These documents are explained in the following table.

DOCUMENT	DEFINITION	HOW EXECUTED
Rules of Behavior, PEMS Agency Users	Generally, Rules of Behavior dictate an individual's responsibilities as a system user and provide guidelines and policies surrounding what is and what is not acceptable system behavior. Specifically, the PEMS Rules of Behavior provide system users with information about controlling hardware and managing system access including granting and revoking privileges, controlling data, and managing personnel, among other things. The contents are defined by the NIST guidelines. This is required by the C & A process.	<ul style="list-style-type: none"> • Between CDC and directly funded grantees • Between grantees and their users • Renew annually
Rules of Behavior, PEMS Agency System Administrators	Rules of Behavior dictate Agency System Administrator responsibilities and provide guidelines and policies surrounding what is and what is not acceptable Agency System Administrator behavior with regard to PEMS. The contents are defined by the NIST guidelines. This is required by the C & A process.	<ul style="list-style-type: none"> • Between CDC and directly funded grantee Agency System Administrators • Between CDC grantees and their grantee Agency System Administrators • Renew annually
MOU, CPEMS	This is a written document which establishes policies and procedures of mutual concern to CDC and CPEMS users. It provides a general description of the responsibilities that are to be assumed by each party in pursuit of some goal or goals. It is not a contract. It is used to define areas of mutual interest. This is required by the C & A process.	<ul style="list-style-type: none"> • Between CDC and CPEMS user organizations • Between CPEMS users and their agencies • Renew annually
MOU, DPEMS	This is a written document which establishes policies and procedures of mutual concern to CDC and DPEMS users. It provides a general description of the responsibilities that are to be assumed by each party in pursuit of some goal or goals. It is not a contract. This is required by the C & A process.	<ul style="list-style-type: none"> • Between CDC and DPEMS user organizations • Between DPEMS users and their agencies • Renew annually
MOU, XPEMS	This is a written document which establishes policies and procedures of mutual concern to CDC and XPEMS users. It provides a general description of the responsibilities that are to be assumed by each party in pursuit of some goal or goals. It is not a contract. This is required by the C & A process.	<ul style="list-style-type: none"> • Between CDC and XPEMS user organizations • Between XPEMS users and their agencies • Renew annually

PEMS MOU/ROB Process



LEGEND

- MOU- Memorandum of Understanding
- ROB- Rules of Behavior
- ROB-AU = Agency Users
- ROB-ASA= Agency System Administrators
- SDN- Secure Data Network
- DFG- Directly Funded Grantee

APPENDIX B – GLOSSARY AND REFERENCES

Glossary

Term	Definition
Access control	A set of procedures intended to assure that a person is who he or she claims to be and has been authorized to perform a set of functions or access a dataset.
Aggregated data	Information, usually summary statistics, that may be compiled from personal information, but is grouped to prevent the identification of any individual case.
Assurance of confidentiality	A guarantee that identifying information (confidential data with and without identifying information) will be held in strict confidence, will be used only for the stated purposes, and will not otherwise be disclosed or released without the consent of the individual.
Authorized access	The permission granted to individuals to see full or partial data that could be linked to an individual.
Authorized personnel	The individuals employed by the grantee who, in order to carry out their duties, have been granted access to confidential data. Authorized personnel must have a current, signed, approved, and binding non-disclosure agreement on file.
Breach of data security	Any unauthorized use of data, even data without names, intended or unintended, including failure to follow security protocols, even if no data is released.
Breach of confidentiality	A security infraction that results in the release of private information, with or without harm to one or more individuals.
Case-specific information	Any combination of data elements that could identify a person.
Confidential information	Any information about an identifiable person when the person or establishment providing the data or described in it has NOT given consent to make the information public
Confidentiality	The protection of private information collected for the system.
Confidential record	A record containing private information about an individual or establishment.
De-identified	The removal of personal data (e.g., names, addresses, ZIP codes, and telephone numbers) so that a record cannot be linked to an individual, but still allows the remaining data to be analyzed.
Encryption	The manipulation or encoding of information so that only parties intended to view the information can do so.
Management controls	Controls that include policies for the operation of information technology resources and for authorizing the collection, processing, storage, and transmission of information. These controls may also include the training of staff, oversight, and appropriate response to infractions.
Personal identifier	A datum, or collection of data, that allows the possessor to determine the identity of an individual with a specified degree of certainty. A personal identifier may permit the identification of an individual within a database (e.g., client code number).
Personnel controls	Staff member controls such as training, separation of duties,

Term	Definition
	background checks, etc.
Physical controls	Controls using barriers, such as locked doors, sealed windows, password-protected keyboards, entry logs, guards, etc.
Quality assurance	Activities to enhance or maintain performance levels of a process; usually involves measurement of the current level of performance, development of methods to maintain or improve that level, and implementation of those methods.
Records retention policy	Assigning a length of time records must be maintained and a date at which paper or electronic records should be archived or destroyed.
Role-based access	Access to specific information or data granted or denied based on the user's job status or authority. Roles typically group users by their work function. This control mechanism protects data and system integrity by preventing access to unauthorized applications and data. Defining access based on roles within an organization, rather than by individual users, simplifies an organization's security procedures.
Sanitize	Also known as disk-wiping, sanitizing is the act of completely destroying the information on a hard disk, floppy disk, or other storage media to ensure that all traces of the files are unrecoverable.
Secured area	A physically contained area where confidential data are available. Only authorized staff members have access to this area. The secured area is usually defined by a hard, floor-to-ceiling wall with a locking door and may include other measures (e.g., alarms, security personnel).
Security	The protection of data and information systems, with the purpose of preventing unauthorized release of identifying information (e.g., preventing a breach of confidentiality) and protecting the integrity of the data by preventing accidental data loss or damage to the systems.
Technical access controls	Controls involving technology, such as requirements for password use and change.

References

The following sources were referenced during compilation of this document:

Document Name	Document Title
NIST Special Publication 800-12	An Introduction to Computer Security: The NIST Handbook
NIST Special Publication 800-14	Generally Accepted Principles and Practices for Securing Information Technology Systems
NIST Special Publication 800-18	Guide for Developing Security Plans for Information Technology Systems
NIST Special Publication 800-30	Risk Management Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology
NIST Special Publication 800-34	Contingency Planning Guide for Information Technology Systems: Recommendations of the National Institute of Standards and Technology
NIST Special Publication 800-37	Guide for the Security Certification and Accreditation of Federal Information Systems
NIST Special Publication 800-53	Recommended Security Controls for Federal Information Systems
NIST Special Publication 800-59	Guideline for Identifying an Information System as a National Security System
NIST Special Publication 800-60 v1	Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories
NIST Special Publication 800-60 v2	Volume II: Appendices to Guide for Mapping Types of Information and Information Systems to Security Categories
CDC Information Security Policy	CDC Information Security Policy
CDC Standard Policy	A Set of Standard Policies at CDC
CDC/ATSDR Policy on Releasing and Sharing Data	CDC/ATSDR Policy on Releasing and Sharing Data
CDC Information Resources Management, Protection of Information Resources	CDC Information Resources Management, Protection of Information Resources
HHS Automated Information Systems Security Program Handbook	HHS Automated Information Systems Security Program Handbook
HHS Baseline Security Requirements Guide	Information Technology Security Program: Baseline Security Requirements Guide
FIPS 46-3	Data Encryption Standard (DES)
FIPS 140-2	Security Requirements for Cryptographic Modules
FIPS 197	Announcing the Advanced Encryption Standard (AES)
FIPS 199	Standards for Security Categorization of Federal Information and Information Systems
Guidelines for HIV/AIDS Surveillance	Appendix C: Security and Confidentiality
OMB Appendix A	Rules of Behavior
PEMS Evaluation Guidance Data Collection Training Facilitators Handbook	PEMS Evaluation Guidance Data Collection Training Facilitators Handbook
Technical Guidance for HIV/AIDS Surveillance Programs, Volume III	Security and Confidentiality Guidelines

APPENDIX C – DIGITAL CERTIFICATE LETTER

APPENDIX D – SIGNATORY DOCUMENTS
(Under Separate Cover)