Centers for Disease Control and Prevention

National Center for HIV/AIDS, STD, and TB Prevention

Program Evaluation and Monitoring System (PEMS)

Rules of Behavior for PEMS Agency System Administrators

TABLE OF CONTENTS

1. Introduction

1.1 Purpose and Scope

This document specifies the formal rules of behavior which the CDC expects of PEMS Agency System Administrators and communicates policies and procedures to be followed. We will receive formal acknowledgement from you, in the form of a signature, which denotes that you have read, understand and intend to comply with these rules. In addition, you should have read the PEMS System Security Summary.

You will also be responsible for seeing to it that all of your agency's users sign a Rules of Behavior for Grantee Users; and that your agency obtains signatures on the same or a similar document from its directly funded users.

The information presented within the Rules of Behavior for PEMS Agency System Administrators addresses:

- The scope, boundaries, and applicability of the system rules
- The governing law and policy applicable to the system
- Statements of policy related to expected user behaviors and responsibilities
- The range of consequences possible for policy violation
- Statements regarding any PEMS system-specific prohibited actions
- The process for obtaining PEMS system help and a listing of additional resources
- The process for publishing and acknowledging revisions
- A formal acknowledgement and signature mechanism

1.2 Legal, Regulatory, and Policy Requirements

Use of the PEMS system is subject to federal laws and regulations governing at a minimum, the following:

- Freedom of Information Act
- OMB Circular A-130, Management of Federal Information Resources
- Privacy Act
- Standards of Ethical Conduct for Employees of the Executive Branch

With respect to these laws and regulations, prohibited uses include:

- Access or using information inappropriately which is protected by the Privacy Act, or other federally mandated confidentiality provisions and/or by OMB Circular A-130, Management of Federal Information Resources.
- Violating copyrights or software licensing agreements.

References

1. 45 CFR 5, Freedom of Information Regulations
2. 45 CFR 5b, Privacy Act Regulations
3. OMB Circular A-130, Appendix III, Security of Federal Automated Information Resources

1.3 Statement of System Policy

Each system administrator is responsible for preventing unauthorized use of, and access to, PEMS system resources. This duty includes complying with all stated policy requirements, taking due care and reasonable precautions when handling system data or using system resources, and in the management and protection of system authentication controls (passwords, certificates, etc.). When in doubt, administrators are strongly encouraged to contact the PEMS Service Support Center for assistance.

1.4 No Expectation of Privacy

CDC or local agency administrators may periodically monitor both the system and user activities for purposes including, but not limited to, troubleshooting, performance assessment, usage patterns, indications of attack or misuse, and the investigation of a complaint or suspected incident. Users are provided system access for the purpose of facilitating Federal, state, local, and agency public health missions only.

1.5 Penalties for Non-Compliance

System administrators who do not comply with the prescribed Rules of Behavior are subject to penalties that can be imposed under existing policy and regulation including reprimands, suspension of system privileges, suspension from duty, termination, and criminal prosecution.

2. System Administrator Responsibilities

2.1 Ethical Conduct

PEMS Agency System Administrators should be held accountable for their use of the PEMS system and the 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. System administrators have

access to client-specific data and are therefore responsible for the protection of confidential information and must report any breaches.

2.2 Authentication Management

Access to PEMS files and software must be restricted to authorized users. System Administrators will establish user accounts, limiting activities within the system, and terminating access when employees leave, change jobs, or breach agency policies. Users who share the same computer must have separate logins and digital certificates.

2.2.1 Granting Access

The system administrator grants access to staff requiring use of PEMS software or data. The steps in this process for CPEMS grantees are as follows:

- application for SDN Digital Certificate
- include letter from agency (refer to PEMS Security Summary)

This is done in writing through the user's supervisor and should include a description of the user's duties related to PEMS. Once a digital certificate is granted, the system administrator then establishes an account in the system for that user, specifying in the system which permissions and levels of access the user will have (which should only be those necessary to perform the duties required by the job). This is called roll-based access. Users are assigned a user ID and a means of authenticating who they are, such as a password. Users of PEMS who have access to confidential data or secured areas should sign a binding, non-disclosure agreement before being given access to PEMS. Other trainings in the policy and procedures concerning security and confidentiality are also recommended.

2.2.2 Levels of Access

The system administrator is responsible for restricting access to various parts of PEMS. These restrictions are based on the roles of the user. All users do not need access to all parts of the system. Access to the various parts of PEMS should be restricted based upon the role of the user. For example, typical roles include data entry, generating reports, system administration, and viewing information. Some people may need to read information about clients but not enter data. Others may need to analyze aggregated data but not view case-specific information. The System Administrator assigns the roles for users of PEMS. Please refer to Chapter 2, Section 5 of the PEMS Security Summary for PEMS Roles and Access Level Table.

2.2.3 Terminating Access

The system administrator will modify or terminate a user's access as soon as it becomes known that the individual is changing duties within the agency or leaving the agency. It should be part of the job-transition protocol of the agency to notify the PEMS system administrator immediately of any change in employee status so that the proper actions can be taken to protect the system and its data.

2.2.4 Use of Passwords

Passwords must be used to confirm the identity of a user to access the system. Separate passwords may also be used to protect specific data sets or applications within the system. For example, a user may need to enter their individual password to get access to the system, but then may need to enter a second, different password in order to get access to information about a certain set of clients. The PEMS password policy is that the passwords should be at least 8 characters long, contain a mix of at least three of the four types of keyboard elements (upper case letters, lower case letters, numerals, and punctuation marks), and can not be the individuals name (refer to Chapter 2, Section 4 of the PEMS Security Summary for password details). Suggestions are to use the first letters from a phrase or abbreviations of a series of words and intersperse or replace letters with associated symbols or numerals in order to make the password easily remembered. The grantee agency should establish policies for passwords that incorporate the PEMS minimum requirements above, they then can also make more stringent password policies. Passwords should be required by the system to be changed periodically (at least every 90 days) and staff should be trained not to divulge passwords. The number of attempts to gain access to the PEMS system is limited, locking the user out after three unsuccessful attempts to log-in to PEMS. System administrators can reset passwords if users forget their password.

2.2.5 Proxies

PEMS will have 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 user of another user. Only system administrators have permission to grant and delete a proxy. The system administrator should see that all users comply with the rules of proxy administration. Only users who have signed a Rules of Behavior for PEMS Agency Users may be given a proxy.

2.3 Information Management and Document Handling

At the local level data collection for PEMS may not only exist on the PEMS servers. It may also be on data collection forms or counselor notes, client files, floppy disks, CD-ROMS, personal digital assistants (PDAs), or other information storage media. Since all these media may contain confidential information, the agency must develop policies and procedures for the use, storage, and disposal of data on each medium used to record or store PEMS data.

The computers (desktop and laptop), PDAs, servers, and other electronic equipment used to collect, enter, copy, store, analyze, or report PEMS data should be under the control of the grantee. The use of equipment related to PEMS, including internet connections, e-mail, photocopiers, facsimile machine, and other equipment that might be used to copy, transmit, or process PEMS data should be regulated by written policies and procedures. The policies should require that computers have screensaver locks that automatically engage when the computer is not used for a set time period and should require that personnel electronically lock their computers when they leave their desk. (In Windows this is done by depressing the Ctrl, Alt, and Delete keys simultaneously, then depressing the Enter key).

2.3.1 Storage

The grantee agency should establish policies and procedures for outlining when it is appropriate to export PEMS data to storage media other than the PEMS system. All media containing PEMS data, whether paper or electronic, must be stored under lock and key in a secure area. All storage media should be labeled. Any PEMS data that is exported to removable media such as floppy disks, zip disks, CD-ROMS, etc., must be sanitized before the storage media is reused. Removable media used for PEMS data should not be shared or used for other purposes. Removable media, whether paper or electronic, containing PEMS data should be stored in a secured area in a locked container. Cleaning crews, maintenance personnel, and other unauthorized personnel that are allowed access to secured areas must be admitted only during working hours when authorized personnel are present, escorted by designated staff, or under other conditions where the data are protected by security measures specified in the written security policy. Encryption of data during storage is recommended.

2.3.2 Disposal

Many states have laws or regulations concerning how long client records must be stored and also 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 the paper records but the electronic records as well. It should be noted that “deleting” a file or record does NOT actually remove the data from the system; overwriting or reformatting

may not suffice to sanitize a file and make it no longer accessible. Special sanitization programs or physical destruction of the storage media may be required. Agencies must also be sure to sanitize or destroy hard drives of computers that are being disposed of or transferred to staff not authorized to use the PEMS system.

2.3.3 Release of Data

Agencies must develop a written policy and procedure for releasing client and de-identified data. These policies should be periodically reviewed and modified to improve the protection of confidential information.

- Reporting to CDC

  Reporting to CDC should be done according to the schedule specified in the PEMS guidance. While data may be entered in the PEMS system at any time, it is not reported to CDC until the appropriate files are submitted to CDC by the authorized personnel of each grantee. 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/submitting to CDC.

- Releasing data to partners (Data Release Agreements)

  In order to assist other agencies in tracking referrals or other 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 should be clearly spelled out to clients as to how their confidential information will be treated/shared with other agency partners. Agencies must also develop policies and procedures that comply with state regulations.

- Releasing data to the public (Data Release Agreements)

  Only authorized staff members who have signed a binding non-disclosure agreement and have a need to know should be allowed access to identifying data, except under conditions specified in writing, such as memoranda of agreement with other agencies, and explained in assurances of confidentiality provided to clients. However, agencies should have a policy and protocol for releasing de-identified data and aggregate data for use in analysis, grant applications, reporting to stakeholders, administrative functions, and other purposes. 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.

2.3.4 Encryption

Agencies should develop a policy for when data should be encrypted. PEMS data is sensitive, confidential information that may have legal implications for clients and should be protected from unauthorized access. PEMS data should always be encrypted during transmission and often should be encrypted during storage, such as during collection in the field. Transmission of data to CDC through the Secure Data Network (SDN) is made secure through the use of Secure Socket Layer (SSL) to a secure CDC database server. The use of digital certificates to restrict access and identify users of the secure data network further secures access to the PEMS application and PEMS data transmission. However, it is the responsibility of the grantee to assure security until the data is submitted to CDC. This includes counseling and testing data using the ReadSoft Scanning Solution, which is not encrypted by the scanning software, but is encrypted in the process of transferring data to CDC.

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 all sensitive, 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 specific fields will not be encrypted. The following is a list of client variables that will be encrypted in PEMS R2.0:

Client Information	Partner Information
G103 - Local Client Unique Identifier	
G105 - Last Name	PCR203 - Last Name
G106 - First Name	PCR204 - First Name
G107 - Middle Initial	PCR205 - Middle Initial
G108 - Nick Name	PCR206 - Nickname
G109 - Aliases	
G110 - Date of Birth-Month	PCR210 - Date of Birth-Month
G111 - Date of Birth-Day	PCR211 - Date of Birth-Day
G125 - Physical Description	PCR219 - Physical Description
G128 - Address Type	PCR220 - Address Type
G129 - Street Address 1	PCR221 - Street Address 1
G130 - Street Address 2	PCR222 - Street Address 2
G131 - City	PCR223 - City
G132 - County	
G133 - State	PCR224 - State
G134 - Zip Code	PCR225 - Zip Code
G135 - Phone Number (Day)	PCR226 - Phone Number (Day)
G136 - Phone Number (Evening)	PCR227 - Phone Number (Evening)
G137 - Primary Occupation	PCR228 - Primary Occupation
G138 - Employer	PCR229 – Employer
"Table G1 Notes"	"Table PCR2 Notes"

2.3.5 Backing up data

CDC will regularly back up all PEMS data stored on CDC database servers. PEMS data that is not yet transmitted, either because it has not yet been entered in the system or because the data is 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.

2.4 System Access and Usage

As a System Administrator, you will review all grantee accounts yearly to make sure they are appropriate and current.

As a System Administrator you agree to only access the system when authorized.

As a System Administrator you have the authority to create and manage all administrators for all of you directly funded agencies.

As a System Administrator, you have the ability to manage permissions to all modules and sub-modules, both Administrative and Non-Administrative for your users.

2.4.1 Portable Equipment

While the use of portable computers, such as laptops and PDAs has many advantages, such as allowing direct input of data in the field or telecommuting, it also creates additional security risks, such as loss or theft of the computer and its data in addition to unencrypted transmission of sensitive data. Grantees should establish policies regarding restricting dial-up access to only staff with absolute necessity for such access, maintaining physical security of computers in the field (such as removing diskettes or removable hard drives and keeping them separate from the computer when not in use, keeping all equipment locked up when not in use), and working from home (removing PEMS data from secure office space is not recommend except for backup storage purposes). If computers are used outside the office, unauthorized access to the data should be prevented through using separate passwords for the operating system and the various data files, encryption of data files, and sanitization of storage disks after the data has been transferred to the main storage system. No digital certificates should be put on laptops or other portable equipment.

2.4.2 Physical Security of Equipment

Grantee system administrators should maintain an inventory of all system hardware and software provided to system users for the execution of their duties. Equipment should be checked periodically to ensure that all equipment is accounted for. Equipment not assigned to an individual should be stored in a secure area to prevent theft or vandalism. Visitors or unauthorized personnel should not be allowed access to areas containing computers holding PEMS data without an escort. 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 at all times and if possible physically attached to an immovable object.

2.4.3 Dial-up Access

The grantee must develop a policy regarding dial-up or other external access to their work location computer system for the purposes of accessing PEMS or PEMS data. Since the PEMS system contains sensitive, confidential information, dial-up or other access to the system from outside is strongly discouraged as this creates more opportunities for unauthorized intrusion into the system. If external access is permitted, it should be restricted to the fewest persons possible and additional security measures should be taken to ensure identification and authentication to obtain access in addition to restricting access to as few as possible.

2.4.4 Locking Workstations

All users should lock their workstations when they are away from their desk if the computers/workstations have that capability. Automatic screen saver locks should be set to engage whenever the system is not used for a preset number of minutes (suggestion is 15 minutes of inactivity). It should require at least entry of the user ID and password to unlock the system.

2.4.5 Disable Browser Password Caching

All PEMS users will be accessing the application through a web browser (i.e. Internet Explorer) and should disable the ability of their web browser to cache (save) their passwords. This will prohibit others who use your computer to have access to passwords and other personal form information that the web browser has cached for you. Please refer to Chapter 2, Section 4 of the PEMS Security Summary for directions on how users can disable browser password caching.

2.5 Incident Reporting

A breach of confidentiality is any failure to follow confidentiality protocols, whether or not information is actually released. All suspected breaches of confidentiality or security (e.g., possible viruses, hackers, password divulgence, mislaying of diskettes) should be reported immediately to your Security Steward. Breaches of confidentiality must be immediately investigated by the Security Steward to determine causes and implement corrections. Sanctions for violations of confidentiality protocols should be determined in writing as part of the agency policies and should be enforced.

2.5.1 Unauthorized Intrusions

Any computer attached to the Internet, such as a PEMS system computer is subject to unauthorized intrusions, such as hackers, computer viruses, and worms. In addition authorized users may attempt to access parts of the system for which they do not have access authority. Grantees must take all reasonable precautions to protect their systems from these types of unauthorized penetrations. A plan must be developed and implemented to prevent and, if necessary, recover from changes to the system caused by unauthorized penetrations of the computer system. Typical precautions include using effective passwords, installing firewalls (DPEMS and XPEMS) and anti-virus software, making backup copies of software (DPEMS and XPEMS), saving data at regular intervals so that the system can be restored to a previous state (DPEMS and XPEMS), and training staff in basic computer security (such as keeping passwords secret and not downloading materials from the Internet or other unauthorized software onto computers that have PEMS access).

2.6 Training and Awareness

Personnel are as much a part of a data collection and reporting system as computer hardware and data 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, on the legal aspects of the data collection, and on the ethics of their responsibility to the clients. They should also be aware of the penalties associated with breaches of confidentiality or security.

Each user with access to PEMS data must receive training on confidentiality and security. This training must be documented in the employee's personnel file. 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 users 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 of breaches of confidentiality.

2.7 PEMS Security Agreements

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 will also be a Rules of Behavior for PEMS Agency Users regarding appropriate and allowed use of PEMS. CDC also will execute a Memorandum of Understanding (MOU) with each directly funded grantee organization. The process for completion of security agreements is described in the PEMS Security Summary.

3. User Assistance and Additional Resources

For assistance in using PEMS, contact your local PEMS administrator, the DHAP IT Help Desk, PEMS Service Support Center or your PEMS Regional Lead (877-659-7725 or pemshelpdesk@cdc.gov.)

4. Revisions and Renewal

Revisions to this document will be released as needed. Notifications of the availability of the revised documents will be made through the PEMS announcement function and other established communication channels. Unless notified otherwise, it will be assumed that all grantees using PEMS accept the revisions. Comments and concerns should be sent to the PEMS Service Support Center.

5. Acknowledgement and Agreement of Rules of Behavior for PEMS Agency System Administrators

I have read and agree to comply with the terms and conditions governing the appropriate and allowed use of PEMS as defined by this document, applicable agency policy, and state and Federal law. I understand that infractions of these rules will be considered violations of CDC and agency standards of conduct and may result in disciplinary action including the possibility of supervisory notification, official reprimand, suspension of system privileges, suspension from duty, termination, and/or criminal and civil prosecution.

I certify that all PEMS system users at our agency have signed the Rules of Behavior for PEMS Agency Users.

I certify that I have read the PEMS Security Summary and my agency's Memorandum of Understanding with the CDC and I agree to abide by the procedures stated in these documents.

_____

(Signature / Date)

_____

(Printed Name)

_____

(Title) PEMS System Administrator

_____

(Agency Name)