Centers for Disease Control and Prevention

National Center for HIV/AIDS, Viral Hepatitis, STD, and

TB Prevention

Program Evaluation and Monitoring System (PEMS)

Rules of Behavior for PEMS Agency System Administrators

December 2009

TABLE OF CONTENTS

1. INTRODUCTION....3

1.1 PURPOSE AND SCOPE....3
1.2 LEGAL, REGULATORY, AND POLICY REQUIREMENTS....3
1.3 STATEMENT OF SYSTEM POLICY....4
1.4 NO EXPECTATION OF PRIVACY....4
1.5 PENALTIES FOR NON-COMPLIANCE....4

2. SYSTEM ADMINISTRATOR RESPONSIBILITIES....5

2.1 ETHICAL CONDUCT....5
2.2 AUTHENTICATION MANAGEMENT....5
2.2.1 Granting Access....5
2.2.2 Levels of Access....6
2.2.4 Use of Passwords....6
2.2.5 Administration of Proxies....7
2.3 INFORMATION MANAGEMENT AND DOCUMENT HANDLING....7
2.3.1 Storage....7
2.3.2 Disposal....8
2.3.3 Release of Data....8
2.3.4 Encryption....9
2.3.5 Backing up data....10
2.4 SYSTEM ACCESS AND USAGE....10
2.4.1 Portable Equipment....11
2.4.2 Physical Security of Equipment....11
2.4.3 Dial-up Access....112
2.4.4 Locking Workstations....12
2.4.5 Disable Browser Password Caching....12
2.5 INCIDENT REPORTING....12
2.5.1 Breeches of Confidentiality....12
2.5.2 Unauthorized Intrusions……..13
2.6 TRAINING AND AWARENESS....13
2.7 PEMS SECURITY AGREEMENTS....14

3. USER ASSISTANCE AND ADDITIONAL RESOURCES....14

4. REVISIONS AND RENEWAL....14

5. Acknowledgement and Agreement....15

1. Introduction

1.1 Purpose and Scope

The “Rules and Behavior for PEMS Agency System Administrators” 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 theSecurity 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

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)
- National Institute of Standards and Technology Special Publications 800 Series

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 system 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. Users of PEMS are only able to access: the data that they enter, the data that belongs to their individual organization and specific data to which they have been given rights. 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. Agency 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 SDN digital certificates.

2.2.1 Granting Access

The agency 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 certificate is granted, the Agency System Administrator establishes an account with levels of access and permissions for that user which should only be necessary to perform their required duties. Users are assigned a user ID and a means of authenticating who they are, such as a password. An Agency System 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.
Users of PEMS who have access to confidential data or secured areas should sign binding, non-disclosure agreements (Rules of Behavior and Memorandum of Understanding and Assurance of Confidentiality) 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 Agency System Administrator is responsible for restricting access to parts of PEMS according to the role of the user and modifying access within the system when a user's duties change. 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 Agency System Administrator assigns the roles for users of PEMS. Please refer to Chapter 2, Section 5 of the Security Summary. **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, leaving the agency or breach agency policies The job-transition protocol of the agency should include immediate to notification to the PEMS system administrator 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 user identity. Passwords should be changed periodically (at least every 90 days) and not shared among staff. 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 and Chapter "Security Recommendations for Your Grantee Agency" Security Summary). 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 Agency System Administrators have 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. The Agency 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 National HIV Prevention Program Monitoring and Evaluation (NHM&E) variables may not only exist on the PEMS servers. It may also be on data collection forms or counselor notes, client files, CD-ROMS, personal digital assistants (PDAs), or other information storage media. Since all of these types of media may contain confidential information, the agency must develop policies and procedures for the use, storage, and disposal of data for each medium used to record or store NHM&E data.

The computers (desktop and laptop), PDAs, servers, and other electronic equipment used to collect, enter, copy, store, analyze, or report NHM&E 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

Agencies should establish policies and procedures that outline when it is appropriate to export NHM&E data to storage media. All storage media should be clearly labeled. Removable media such as zip disks, CD-ROMS, etc., should be destroyed or sanitized with disk wiping tools before reuse or disposal. Storage media, whether removable or fixed, paper or electronic, containing NHM&E data should be stored in a secured area. Data removed from secured areas for analysis should be de-identified first. Diskettes, laptops, thumb drives and other storage media that contain NHM&E data should have only the minimum data necessary to perform a given task; should 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.

2.3.2 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.

2.3.3 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.

Reporting to the CDC:
Reporting to the CDC should be done according to the schedule specified by the CDC. While data may be entered into PEMS at any time, it is not reported to the CDC until the appropriate files are submitted to the CDC by the authorized personnel of each agency over the SDN. 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 data to the CDC.

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.

2.3.4 Encryption

NHM&E data is sensitive, confidential information that may have legal and personal implications for clients; therefore, it should be protected from unauthorized access. NHM&E data should always be encrypted during transmission and often should be encrypted during storage, such as during collection in the field. Data transmitted to the CDC through the SDN is secured through the use of several security controls (See chapter 2 of Security Summary for detailed description of security controls). 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 by PEMS in the process of transferring data to CDC.

If an organization decides to send data to anyone other than the CDC, the data should be encrypted. All NHM&E data is encrypted using the Self Decrypting Archive function of PGP. An encrypted SDA file is generated and sent to CDC over the SDN. The data remains encrypted until it enters the CDC network and reaches the validation team at which time it is decrypted PGP meets the Federal Information Processing Standards 140-2 (FIPS 140-2) requirements and the CDC central key requirement for CDC.

In addition to NHM&E data being encrypted with a Secure Socket Layer (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 R3.1:

Client Information	Partner Information
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 regularly backs up all NHM&E 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 (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 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, complex password, and sensitive data should be encrypted). Laptop computers and other portable hardware that receive NHM&E data should store that data in encrypted formats. Laptops should employ whole disk encryption in order to protect any sensitive data that may be stored on the hard drive.

2.4.2 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 to areas containing computers holding NHM&E 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 and physically attached to an immovable object, if possible. All rooms where NHM&E data is stored, either on paper, computer or other storage media should be locked at all times when not in use and it should be known with whom the keys reside.

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 NHM&E 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 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.

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

2.5 Incident Reporting

2.5.1 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.

2.5.2 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 (XPEMS) and anti-virus software, making backup copies of software (XPEMS), saving data at regular intervals so that the system can be restored to a previous state (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

All agency staff dealing with NHM&E data and the PEMS system 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. Grantee 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 NHM&E data should receive PEMS training including security updates.

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 NHM&E 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.

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 Technical Guidance for HIV Program Evaluation and Monitoring System (PEMS) Grantee Security Guidelines.

3. User Assistance and Additional Resources

For assistance in using PEMS, contact your local PEMS administrator, the PEMS Service Center through the CCID Informatics Customer Support Help Desk via e-mail at dhapsupport@cdc.gov or via telephone at 877-659-7725, or your PEMS Regional Lead.

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 Center via the CCID Informatics Customer Support Help Desk at dhapsupport@cdc.gov.

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 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)