Centers for Disease Control and Prevention

The National Center for HIV/AIDS, Viral Hepatitis, STD, & TB Prevention

Rules of Behavior for CDC Staff and Contractors

National HIV Prevention Program Monitoring & Evaluation (NHM&E) Data and the Program Evaluation and Monitoring System (PEMS)

July 2010

TABLE OF CONTENTS

1. Introduction

1.1 Purpose and Scope

Personnel are as much a part of a data collection and reporting system as computer hardware and collection forms, and, unfortunately, people are usually the weakest link in any security system. CDC enforces policies and procedures to assure data confidentiality and security of data systems, which indicate that authorized users are responsible for being familiar with the confidentiality and security policies and procedures, challenging unauthorized users, reporting possible breaches, and protecting equipment and data.

The purpose of this *Rules of Behavior for CDC Staff and Contractors* (*ROB-CDC*) is to provide security guidelines to CDC staff and contractors who have access to National HIV Prevention Program Monitoring and Evaluation (NHM&E) data and to the Program Evaluation and Monitoring System (PEMS). All CDC Staff and Contractors (henceforth referred to as "users") having access to PEMS or to NHM&E data should review the topics discussed in this document. Users are also required to annually review the *ROB* and its associated *Non-Disclosure Agreement*, sign the signature pages of both documents, and return those pages to PEB for documentation and storage. This process will assure to users continued access to NHM&E data.

The information presented within this ROB addresses:

- The governing law and policy applicable to the system
- Statements of policy related to expected users' behaviors and responsibilities
- The broad range of consequences possible for policy violation
- Descriptions of users' responsibilities
- The process for publishing and acknowledging revisions to this ROB
- A formal acknowledgement and agreement mechanism (signature)

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
- U.S. Public Health Service Act , Section 308(d)

With respect to these laws and regulations, prohibited data uses include[1]:

- Inappropriate access to or use of information protected by the Privacy Act, other federally mandated confidentiality provisions, or by OMB Circular A-130, *Management of Federal Information Resources*.
- Violating copyrights or software licensing agreements.

1.3 Statement of Policy Regarding NHM&E Data and Data Systems

Each user is responsible for helping to prevent unauthorized use of and access to system and NHM&E data resources. This duty includes complying with all stated policy requirements and taking due care and reasonable precautions when handling NHM&E data or accessing system resources.

1.4 Penalties for Non-Compliance

Users 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. User Responsibilities

2.1 Ethical Conduct

Persons who have access to NHM&E data or to PEMS will be held accountable for their access. Users may access only the specific data to which they have been given current or updated rights. Using the PEMS system, other CDC data systems, or other resources to copy, release, or view data without authorization is prohibited. Altering data improperly or otherwise tampering with the system is prohibited. Staff authorized to access

[1] Additional References

1. Clinger Cohen Act of 1996 (Public Law 104-106)
2. Federal Information Security Management Act (FISMA)
3. HHS Information Security Program Policy
4. Executive Orders, Directives, Regulations, Publications, Guidance(s)
5. National Institute of Standards and Technology Special Publications 800 Series
6. OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*

NHM&E data are responsible for the protection and confidentiality of that information and must report any breaches.

2.2 Authentication Management

Access to NHM&E data files, PEMS software, and other related CDC data systems must be restricted to authorized users. Authentication of internal data users and of internal staff who otherwise have access to the PEMS system will be verified by CDC employee and contractor IDs.

2.2.1 Granting Access

User signature provided annually on this *ROB* and the *Non-Disclosure Agreement* grants internal CDC staff and contractors access PEMS software or NHM&E data. No one will be provided access to PEMS or to NHM&E data without their first having signed the required data security-related documents.

2.2.2 Terminating Access

As soon as it becomes known that a user is changing duties within the CDC, is leaving the CDC, or has breached CDC policies, their access will be modified or terminated. It is the user's responsibility to inform the PEB data steward about changes in job duties (including termination of employment) that will affect their PEMS access and NHM&E data user rights.

2.3 Information Management and Document Handling

Users are expected to follow data management and handling policies and procedures as indicated in the required annual Security Awareness Training (SAT) provided by CDC and in the *Non-Disclosure Agreement* and in this *ROB*.

The computers (desktop and laptop), servers, and other electronic equipment used to store, analyze, or report NHM&E data should be under the control of the user. The use of equipment allowing access to PEMS or NHM&E data, including internet connections, photocopiers, facsimile machine, or other equipment that might be used to copy, transmit, or process NHM&E data is regulated by CDC policies and procedures. The policies require that computers have screensaver locks that automatically engage when the computer is not used for a set time period. Personnel should 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

All storage media are to be clearly labeled with organization's contact information. Allowable storage media include only CDC owned computers, whether their use is in an office on a CDC campus or in a telework environment. Transfer of sensitive information is allowed only within the CDC LAN or via CDC provided, encrypted thumb drives, which

are issued by the NCHHSTP Security Office. 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 first de-identified. CDC supplied laptops that contain NHM&E data for analyses should have only the minimum data necessary to perform a given task; should be encrypted and stored under lock and key when not in use; and (except for backups on the CDC LAN) should be sanitized immediately following the task completion.

2.3.2 Disposal

NHM&E data should be deleted from the workstation when the analysis or project is completed, and the results and datasets of the analysis should be moved to the appropriate place on the secure server. Using CDC supplied encrypted USB drives and CDC supplied encrypted laptops to temporarily store data or reports for analysis is acceptable since no one will be able to access the data if the laptop or USB drive were to be lost or stolen. When NHM&E data 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. Therefore, all CDC users are expected to follow all CDC requirements and policies for protecting the security and integrity of CDC systems in order to avoid external misuse, corruption, or other abuse of sensitive data.

2.3.3 Release of Data

Access to NHM&E data will be contingent on having signed, current, binding *ROB* and *Non-Disclosure Agreement* currently on file. These agreements include discussion of possible employee ramifications and criminal and civil liabilities for unauthorized disclosure of information. Data may be only be shared according to CDC guidelines and only by PEB personnel authorized to do so.

2.3.4 Encryption

The use of the CDC supplied encrypted USB drives for transporting data reports, and presentations is required due to the security the encrypted USB drive provides. NHM&E data are sensitive, confidential information that may have legal and personal implications for HIV prevention program agencies and their clients; therefore, data should be protected from unauthorized access. NHM&E data in PEMS are encrypted during transmission and during storage. Data transmitted to the CDC in XML format through the SDN are secured through the use of several security controls. Likewise, all NHM&E data that are scanned into the CDC- provided scanning data tool by CDC grantees should be encrypted using the encryption function of PGP and then sent to CDC over the SDN. All encrypted data remain encrypted until entering the CDC network and reaching the validation team, at which time the data are decrypted. However, it is the responsibility of the CDC user to assure security of data once they are submitted to CDC. Generally, data within CDC networks and accessed through the LAN and through software such as CITGO (authorized by CDC) are not required to be encrypted.

2.3.5 Backing up data

CDC regularly backs up all NHM&E data stored on CDC database servers. Users are encouraged to back up data files currently in use on the LAN server specified for that purpose. PEB will provide access to specific files for that purpose.

2.4 More on Equipment, Access, and Security Measures

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. CDC supplied laptop computers (e.g., for use during telecommuting) that contain NHM&E data store those data in encrypted formats. CDC supplied laptops 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

CDC maintains an inventory of all PEMS system hardware and software, and periodic audits are conducted to account for all assets. Visitors or unauthorized personnel are not allowed unescorted access to areas containing computers holding NHM&E data. All computers and other equipment used for NHM&E data should be housed or stored in secure areas. All rooms where NHM&E data are stored, either on paper or on computer, should be locked when not in use.

2.4.3 Dial-up and Other On-Line Access

Dial-up or other external access to a users' work location computer system for the purposes of accessing NHM&E data is permitted only via CDC authorized software, which currently is CITRIX.

2.4.4 Locking Workstations

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

2.4.5 Disable Browser Password Caching

All users 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 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.

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 or sensitive 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 CDC/NCHHSTP Security Team Lead. This administrator will determine the cause, develop and implement process improvements, and determine if the incident should be reported to the CDC Office of the Chief Information Security Official (OCISO).

2.5.2 Unauthorized Intrusions

Any computer attached to the Internet is subject to unauthorized intrusions, such as hackers, computer viruses, and worms. In addition, authorized users may attempt to access parts of the PEMS system or files with NHM&E data to which they do not have access authority. Users must take all reasonable precautions to protect their computers and data files from these types of unauthorized penetrations. Typical precautions include using effective passwords, saving data at regular intervals so that the computer can be restored to a previous state, and participating in CDC-required training (the SAT) in basic systems security measures.

2.6 Training and Awareness

All staff dealing with NHM&E data and the PEMS system should be trained on policies and procedures established by the CDC, the legal aspects of data collection, and the ethics of their responsibility to CDC grantees and their clients. Training should cover policies concerning confidentiality, computer security, and legal obligations under non-disclosure agreements. Users 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.

3. Revisions and Renewal

Revisions to this document will be released as needed. Notifications of the availability of the revised documents will be made through established communication channels. Unless notified otherwise, it will be assumed that all CDC users accessing NHM&E data or PEMS accept the revisions. Comments and concerns should be sent to the NCHHSTP/ DHAP/ Program Evaluation Branch Chief.

4. Acknowledgement and Agreement of Rules of Behavior for CDC Staff and Contractors

I have read and agree to comply with the terms and conditions governing the appropriate and allowed use of NHM&E data and access to the PEMS system as defined by this document, applicable agency policy, and state and Federal law.

I agree to abide by the procedures and policies indicated in these documents.

_____/_____

Signature / Date

_____

Printed Name

_____

Title and Agency or Company Name