

Centers for Disease Control and Prevention

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

Non-CDC Data Systems

Rules of Behavior for the Administration of Non-CDC Data Systems

Agency System Administrators

July 2011



Sensitive but Unclassified (SBU)

This document contains information that may be exempt from public release under the Freedom of Information Act (FOIA) (5 U.S.C. 552), exemption 2 applies. Approval by the Centers for Disease Control and Prevention Document Control Officer (OSEP) and the CDC FOIA Officer, prior to public release via the FOIA Office is required.

This document was prepared by the Data System and Analysis Team (Shubha Rao, swr2@cdc.gov and John Beltrami, hzb3@cdc.gov).

TABLE OF CONTENTS

1. INTRODUCTION	2
1.1 PURPOSE AND SCOPE	2
1.2 LEGAL, REGULATORY, AND POLICY REQUIREMENTS.....	2
1.3 STATEMENT OF SYSTEM POLICY.....	3
1.4 NO EXPECTATION OF SYSTEM USE PRIVACY	3
1.5 PENALTIES FOR NON-COMPLIANCE.....	4
2. SYSTEM ADMINISTRATOR RESPONSIBILITIES	4
2.1 ETHICAL CONDUCT.....	4
2.2 AUTHENTICATION MANAGEMENT	4
2.2.1 Granting Access	4
2.2.2 Levels of Access	5
2.2.3 Terminating Access	5
2.2.4 Use of Passwords.....	5
2.2.5 Administration of Proxies	6
2.3 INFORMATION MANAGEMENT AND DOCUMENT HANDLING	6
2.3.1 Storage	7
2.3.2 Disposal.....	7
2.3.3 Release of Data	7
2.3.4 Encryption.....	8
2.3.5 Backing Up Data.....	9
2.4 SYSTEM ACCESS AND USAGE	9
2.4.1 Portable Equipment	10
2.4.2 Physical Security of Equipment	10
2.4.3 Dial-Up Access	11
2.4.4 Locking Workstations.....	11
2.4.5 Disable Browser Password Caching.....	11
2.5 INCIDENT REPORTING.....	11
2.5.1 Breaches of Confidentiality	11
2.5.2 Unauthorized Intrusions	12
2.6 TRAINING AND AWARENESS	12
2.7 NON-CDC DATA SYSTEM SECURITY AGREEMENTS	13
3. USER ASSISTANCE AND ADDITIONAL RESOURCES.....	13
4. REVISIONS AND RENEWAL.....	13
5. ACKNOWLEDGEMENT AND AGREEMENT OF RULES OF BEHAVIOR FOR NON-CDC DATA SYSTEMS AGENCY SYSTEM ADMINISTRATORS	14

1. Introduction

1.1 Purpose and Scope

The purpose of this “Rules of Behavior” for non-CDC data system Agency System Administrators (ROB-ASA) is to provide administrators of these systems guidelines for policies and practices related to National HIV Prevention Program Monitoring and Evaluation (NHM&E) data collection and reporting. All non-CDC data system Agency System Administrators at grantee sites using non-CDC data systems should review the topics discussed in this guide and sign it. Additional rules of behavior may be appended if required by state or local law or are otherwise necessary.

For purposes of this document, the term “non-CDC data systems” refers to non-CDC-funded Information Technology (IT) systems used for collecting and reporting NHM&E data.

Agency System Administrators will also be responsible for developing Rules of Behavior for non-CDC data system users and ensuring that all users comply with the guidelines in this ROB.

The information presented within the ROB addresses the:

- Scope, boundaries, and applicability of the system rules
- Governing law and policy applicable to the system
- Statements of policy related to expected non-CDC data system administrators’ behaviors and responsibilities
- Broad range of consequences possible for policy violation
- Descriptions of the non-CDC data system agency administrators’ responsibilities
- Listing of any system-specific prohibited actions
- Process for obtaining system help and a listing of additional resources
- Process for publishing and acknowledging revisions
- Formal acknowledgement and agreement mechanism (signature)

1.2 Legal, Regulatory, and Policy Requirements

Non-CDC data systems are used as part of CDC’s NHM&E data support systems and are held to high standards of performance with regard to data collection, reporting, and security. The following standards should be applied to the functionality or operation of non-CDC data systems:

- Clinger-Cohen Act of 1996 (Public Law 104-106)
http://www.cio.gov/documents_details.cfm/uid/1F432CB6-2170-9AD7-F2F9BFC351F83400/structure/Laws,%20Regulations,%20and%20Guidance/category/IT%20Related%20Laws%20and%20Regulations
- OMB Budget Circular A-130, Appendix III, Security of Federal Automated Information Resources
http://www.whitehouse.gov/omb/circulars_a130_a130appendix_iii
- Federal Information Security Management Act (FISMA)
<http://csrc.nist.gov/groups/SMA/fisma/index.html>
- HHS Information Security Program Policy HHS-IRM-2004-0002
<http://www.hhs.gov/ocio/policy/2004-0002.001.html>
- National Institute of Standards and Technology Special Publications 800 Series <http://csrc.nist.gov/publications/PubsSPs.html>
- Executive Orders, Directives, Regulations, Publications, Guidance(s)

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

- Accessing or inappropriately using information 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

1.3 Statement of System Policy

Each System Administrator is responsible for overseeing the prevention of unauthorized use of, and access to, 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 (e.g., passwords, certificates, etc.). When in doubt, administrators are strongly encouraged to contact their respective local Information Technology Support Group or the NHM&E Service Center (phone: 1-888-736-7311, e-mail: pemsservice@cdc.gov) for assistance.

1.4 No Expectation of System Use Privacy

CDC recommends that non-CDC data system Agency System Administrators periodically monitor their systems 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 complaints or suspected incidents or security breaches. Users should be provided system access for the purpose of facilitating federal, state, local, and agency public health missions.

1.5 Penalties for Non-Compliance

Agency System Administrators who do not comply with the prescribed ROB are subject to penalties that can be imposed under existing policy and regulations including reprimands, suspension of system privileges, and suspension from duty, termination, or criminal prosecution.

2. System Administrator Responsibilities

2.1 Ethical Conduct

Agency System Administrators should ensure that non-CDC data system users are only permitted to access: the data that they enter, the data that belong 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 must be prohibited. Altering data improperly or otherwise tampering with the system must be prohibited. Agency System Administrators have access to client-specific data and are therefore responsible for the protection of confidential information and must promptly manage and report any breaches.

2.2 Authentication Management

Access to NHM&E data files, your system files and software must be restricted to authorized users. Agency System Administrators will verify a potential user's need to access NHM&E data, establish user accounts, limit activities within the system, and terminate access when employees leave, change jobs, or breach agency policies. Agency System Administrators must make sure that users who share the same computer have and use separate logins and security certificates. The Agency System Administrator will be responsible for ensuring that all staff members that use the application meet all authentication requirements.

2.2.1 Granting Access

The Agency System Administrator grants access to staff requiring use of non-CDC data system software or NHM&E data. Staff responsible for data transmission to CDC may require additional access to the CDC's secure data network. The steps in this process for CDC grantees that require access to CDC's secure data network are as follows:

- Application for a security certificate
- Application for CDC data system access (to include a letter from your Agency System Administrator)

This is usually done in writing through the user's supervisor and should include a description of the user's duties related to non-CDC data systems. 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 non-CDC data systems 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 non-CDC data systems who have access to confidential data or secured areas should sign binding, non-disclosure agreements before being given access to these systems and confidential NHM&E data (trainings in the policies and procedures concerning NHM&E data security and confidentiality is mandated).

2.2.2 Levels of Access

The Agency System Administrator is responsible for restricting access to parts of their system according to the roles of the user and modifying access within the system when a user's duties change. These restrictions are based on the roles and official duties of the user. All users do not need access to all parts of the system. Access to the various parts of non-CDC data systems 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 aggregate data but not view case-specific information. As the Agency System Administrator, you will assign each system user specific roles and access rights.

2.2.3 Terminating Access

As soon as it is known that an individual is changing duties within an agency, leaving the agency, or has breached agency policies, it is the non-CDC data system Agency System Administrator's responsibility to modify or terminate their access. The job-transition protocol of the agency should include immediate notification to the CDC Data Systems 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 user identity. Passwords should be changed periodically (at least every 60 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 NHM&E 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 (i.e., upper case letters, lower case letters, numerals, and punctuation marks or special characters), and cannot be the individual's name.

2.2.5 Administration of Proxies

As a requirement for NHM&E data support systems, non-CDC data systems should 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 should log in at a time as a proxy of another user. Only an Agency System Administrator should have permission to grant and delete a proxy. The Agency System Administrator is responsible for developing rules at the site level to determine how long proxies may last and how they should be administered. All non-CDC data system users must comply with the rules of proxy administration.

2.3 Information Management and Document Handling

At the local level, data collection for NHM&E variables will not only exist on the non-CDC data system 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 secure use, storage, transmission, and disposal of data on each medium used to record or store NHM&E data.

The computers (desktop and laptop), PDAs, servers, and all 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 non-CDC data systems, including internet connections, e-mail, photocopiers, facsimile machines, and other equipment that might be used to copy, transmit, or process NHM&E 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 password protected and encrypted storage media. All storage media should be clearly labeled. Removable storage 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. Personal disks, laptops, thumb drives, and other storage media must not be used to store confidential NHM&E data. When used for data storage, these devices must contain only the minimum non-confidential data necessary to perform a given task, must 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 personnel unauthorized to access NHM&E data must be escorted into secured areas by designated staff. Encryption of electronic 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, these should include not only the paper records but also the electronic records. Please note that “deleting” a file or record does not actually remove the data from the system. Even overwriting or reformatting 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 the non-CDC data systems.

2.3.3 Release of Data

Agencies must develop a written policy and procedure for releasing data. This policy 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, and binding non-disclosure agreement currently on file at the agency. These agreements must include discussion of possible employee ramifications and criminal and civil liabilities for unauthorized disclosure of information.

Reporting data to CDC: Reporting data to CDC should be done according to the data submission timelines specified by CDC. Data entered into non-CDC data systems are not reported to CDC until the appropriate files are submitted to CDC through a secure data network by authorized personnel of each agency. Policies and procedures should be developed to specify the data quality assurance process being implemented and the administrative approval and CDC notification processes being followed prior to reporting or submitting data to the CDC.

Releasing data to partners: In order to assist other agencies in tracking referrals or for other related public health 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 advised on how their confidential information will be managed and/or 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 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 data may be released, and who may approve the release of data.

2.3.4 Encryption

NHM&E data are sensitive, confidential information that may have legal and personal implications for clients; therefore, data 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 secure data network are secured through the use of several security controls. However, it is the responsibility of the grantee to assure all NHM&E data security until they are submitted to the CDC.

If an organization decides to send data to anyone other than the CDC, those data should be encrypted. NHM&E data sent to the CDC should be encrypted and sent through a secure data network. The data should remain encrypted until entering the CDC network and reaching the secure data network staff at which time the data are decrypted.

The following is a list of client variables that must be encrypted in non-CDC data system.

Client Information

G105 - Last Name
G106 - First Name
G107 - Middle Initial
G108 - Nick Name
G109 - Aliases
G110 - Date of Birth-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"

2.3.5 Backing Up Data

CDC regularly backs up all NHM&E data stored on CDC database servers. Non-CDC data system data that are not yet transmitted to CDC must be backed up periodically by the grantee. Frequency of backup should depend upon how often the data change and how significant those changes are, but should be done based on a fixed schedule that is part of the normal system maintenance. 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 an Agency System Administrator, you will review all grantee accounts annually to make sure they are appropriately assigned and current.

As an Agency System Administrator you agree to limit system access to authorized users and make users aware of their responsibilities in preventing unauthorized access to system resources.

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

Sensitive but Unclassified (SBU)

Revised Date: July 1st, 2011

As an Agency System Administrator, you should have the ability to manage permissions to all modules and sub-modules, both administrative and non-administrative, for your users.

As an Agency System Administrator, you are responsible for ensuring that all staff members that use the application or data system comply with all system authentication requirements.

As an Agency System Administrator you have the responsibility of ensuring that all agency staff members that access and use the system are properly trained in maintaining the security and confidentiality of NHM&E data.

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 stored data. If computers are used outside the office or usual secure areas, agencies should establish policies regarding physical security (e.g., the computer should be locked to an immovable object) and digital security (e.g., 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 those 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. No security certificates should be saved or stored on portable media.

2.4.2 Physical Security of Equipment

Non-CDC data system 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 unescorted access to areas containing computers holding NHM&E 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 non-CDC data systems should be housed or stored in secure areas and physically attached to an immovable object, if possible. All rooms where NHM&E data are stored in computers or on paper or other storage media should be locked at all times when not in use, and it should be known with whom all 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 non-CDC data systems or NHM&E data. Since non-CDC data systems contain sensitive, confidential information, dial-up or other external access to the system is strongly discouraged as this creates more opportunities for unauthorized, often malicious intrusion into the system. If external access is permitted, it should be restricted to the minimum number of 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 (e.g., 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 non-CDC data system users who will be accessing that system should disable the ability (if any) of their non-CDC data systems to cache (save) their passwords. This will prohibit others who use your computer to have access to passwords and forms with personal information that the web browser has cached for you. Please refer to the equipment owner's manual for directions on how users can disable browser 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 or actual breaches of confidentiality or security of NHM&E records or data involving personally identifiable information such as names, addresses, identification numbers, dates (except year), etc., should be reported to CDC Information Systems Security Officer (phone 404.639.1806; e-mail:rxv2@cdc.gov) and the DHAP PEB Data Security Steward (phone: 404-718-8636; e-mail: swr2@cdc.gov) **within one hour of discovery**. All other suspected or actual breaches of confidentiality or security of NHM&E record or data (e.g., possible viruses, hackers, password divulgence, lost or misplaced

storage media, failure to follow secure storage policies, etc.) should be reported immediately to the non-CDC data system Agency System Administrator. The Agency System Administrator will determine the cause, develop and implement process improvements, and/or determine if the incident should be reported to the CDC Information Systems Security Officer and the CDC DHAP PEB Data Security Steward. In determining whether a non-PII breach of NHM&E data or records should be reported to CDC, Agency System Administrators should consider reporting such breaches to CDC if there is a strong possibility that PII will be breached, CDC data and data systems will be compromised, or that CDC's public health mission will be negatively impacted.

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 some non-CDC data system computers, may be 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 and currently updated anti-virus software, making backup copies of software, saving data at regular intervals so that the system can be restored to a previous state, 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 non-CDC data system access).

2.6 Training and Awareness

All agency staff dealing with NHM&E data and non-CDC data systems 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. Every new employee who requires access to confidential NHM&E data and resources must complete data security training conducted by your agency before access is granted. Current employees are also required to complete a refresher course on data security every year. All data security trainings 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 data confidentiality and security, contingency plans for breaches of confidentiality and security, and the penalties

Sensitive but Unclassified (SBU)

Revised Date: July 1st, 2011

associated with breaches of NHM&E data confidentiality and security. Each agency staff member with access to NHM&E data should receive non-CDC data system-specific 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. Each agency should have a policy on NHM&E data confidentiality and security. The confidentiality and security policy must explain 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 annually 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 Non-CDC Data System Security Agreements

In an effort to provide maximum protection of the data that are entered into non-CDC data systems, in addition to the physical and system security measures explained in this document, Agency System Administrators will develop and make available an ROB for non-CDC data systems agency system users covering all of the additional duties of the non-CDC data systems users. CDC also will be executing a Memorandum of Understanding (MOU) with each directly funded grantee organization.

3. User Assistance and Additional Resources

For assistance in using non-CDC data systems, contact your local Information Technology Support Team. If assistance is not readily available from that office you may contact the NHM&E Service Center at pemsservice@cdc.gov or 1-888-PEMS-311 (1-888-736-7311) for assistance.

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 non-CDC data system announcement function and other established communication channels. Unless notified otherwise, it will be assumed that all grantees using non-CDC data systems accept the revisions. Comments and concerns should be sent to the NHM&E Service Center at pemsservice@cdc.gov.

5. Acknowledgement and Agreement of Rules of Behavior for Non-CDC Data Systems Agency System Administrators

I have read and agree to comply with the terms and conditions governing the appropriate and allowed use of non-CDC data systems and the NHM&E data, 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 non-CDC data system users at our agency have signed rules of behavior for non-CDC data system agency users.

(Signature / Date)

(Printed Name)

Name of Non-CDC Data System covered by this agreement

(Title) Non-CDC Data System Administrator

(Agency Name)