Memorandum of Understanding (MOU) between the Centers for Disease Control and Prevention (CDC) and Directly Funded Agency(ies) for use of Non-CDC Data Systems

The purpose of this Memorandum of Understanding (MOU) is to serve as a written understanding between the Centers for Disease Control and Prevention (CDC) and the directly funded organizations that use non-CDC data systems to monitor and evaluate CDC-funded HIV Prevention Programs. It provides a framework for cooperation between CDC and directly funded organizations to maintain security and confidentiality, to provide training, access, and technical assistance, and complete other responsibilities related to the non-CDC data systems or other non-CDC software.

Definition of CDC Data Systems and Non-CDC Data Systems

For purposes of this document, the term "CDC data systems" refers to CDC-funded Information Technology (IT) systems used for collecting and reporting National HIV Prevention Program Monitoring and Evaluation (NHM&E) data.

The non-CDC data system is a locally developed and maintained data entry system for collecting NHM&E data, with an external feed to CDC. Grantees will be required to modify their existing software and data collection tools to be in compliance with NHM&E specified data variables, software specifications and associated business rules.

1.0 Non-CDC Data Systems Confidentiality and Security

1.1 External Agency

Your agency agrees to be responsible for protecting NHM&E data security and client privacy at your agency and at the agencies you fund or partner with in fulfilling your mission. Language in this document that refers to "your agency" is inclusive of those grantee locations that are directly funded by CDC and use non-CDC data systems. Security encompasses data confidentiality, integrity, and availability. Client privacy is a right protected by the Privacy Act of 1974 as amended.

1.1.1 Data Collection

a) Your agency agrees to adequately protect paper and electronic records collected by your agency.
b) Your agency agrees to be responsible for ensuring that as data are elicited verbally from clients, client privacy is maintained and data are collected confidentially.
c) Your agency agrees to follow current state HIV testing consent and counseling statutes during data collection.

This document was prepared by the Data System and Analysis Team (Shubha Rao, swr2@cdc.gov and John Betrami, hzb3@cdc.gov).
Revised Date: July 1st, 2011

d) Your agency agrees that when NHM&E data are collected with identifiers, only de-identified data will be submitted to CDC through a secure data network.
e) Your agency agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of security and privacy during data collection.

1.1.2 Data Entry

a) Your agency agrees to ensure that NHM&E data entered into non-CDC data systems by your agency are entered under levels of security commensurate with the security described in the Rules of Behavior (ROB) for system administrators and users.
b) Your agency agrees to ensure that NHM&E data entered directly or indirectly into non-CDC data systems are input only by staff authorized by your agency.
c) Your agency agrees to ensure that NHM&E data integrity is maintained and data entered in non-CDC data systems are not altered for misrepresentation or falsification purposes.
d) Your agency agrees to ensure that whenever NHM&E data are entered indirectly into a non-CDC data system, such as, into a handheld device, those data are encrypted and protected from security breaches and are kept confidential.
e) Your agency agrees that NHM&E data entry will occur in a confidential environment, safeguarding against unauthorized disclosure of client information.
f) Your agency agrees that users of non-CDC data systems will require identification and authentication to access the system for data entry.
g) Your agency agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of security and privacy during data entry.

1.1.3 Data Storage

a) Your agency agrees that NHM&E data in the non-CDC data system repository and paper records will be housed locally at your agency and not at the CDC.
b) Your agency agrees to be responsible for the security of NHM&E data stored in your information systems.
c) Your agency agrees to be responsible for ensuring that NHM&E paper records and NHM&E electronic data at your agency are stored in a physically secure location where access is limited to currently authorized personnel.
d) Your agency agrees to adequately secure NHM&E electronic data that are stored in an electronic format (i.e., CD-ROM, flash drives) or in a data repository.
e) Your agency agrees that upon submission to CDC, your agency's NHM&E data will be securely stored in a data repository at the CDC (See Section 1.2 for CDC Responsibilities).

f) Your agency agrees to create NHM&E data backups based on a locally recommended schedule and to securely store these backups.
g) Your agency agrees to establish, test, implement, and frequently revise a local NHM&E data recovery plan.
h) Your agency agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of security and privacy when storing NHM&E data.

1.1.4 Data Use

a) Your agency agrees to ensure that NHM&E data are accessed only by authorized staff.
b) Your agency agrees to establish, implement, and update procedures for authorizing staff access to and use of NHM&E data.
c) Your agency agrees to use NHM&E data in a manner that adequately protects client privacy.
d) Your agency agrees to use NHM&E data in a manner that is in accordance with federal and state statutes.
e) Where appropriate, your agency agrees to use NHM&E data in accordance with the Institutional Review Board (IRB) of your location and obtain adequate IRB approvals from relevant organizations.
f) Where appropriate, your agency agrees to consult with legal counsel to verify that all reasonable considerations for complying with federal and state statutes are being taken in regards to NHM&E data use.
g) Your agency agrees to be responsible for implementing and updating policies and procedures for the use of NHM&E data in a secure manner that adequately protects client privacy and prevents against unauthorized access to and use of NHM&E data.
h) Your agency agrees to be adequately informed about the current national NHM&E data security policies and guidelines.
i) Your agency agrees to be responsible for assessing whether or not a data release policy is required for access to and use of your NHM&E data.
j) Your agency agrees that users of non-CDC data systems will require identification and authentication to access the system for use of NHM&E data stored in non-CDC data systems at your location.
k) Your agency agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of security and privacy as data are used.

1.1.5 Data Sharing

a) Your agency agrees that NHM&E data collected by your agency will be shared with CDC in the form of an electronic file which will follow a specified file format provided by CDC.
b) Your agency agrees to comply with all current policies and procedures that are necessary for the electronic submission of NHM&E data via a secure data network.

c) Your agency agrees to ensure that all security certificates held by staff at your agency are authorized and current.
d) Your agency agrees to be responsible for implementing and updating policies and procedures for the publication and redistribution of NHM&E data and ensuring that client confidentiality will be maintained during this process.
e) Your agency agrees to adequately protect NHM&E data transported within your agency or to external agencies when data are not being transmitted through CDC data systems.
f) Your agency agrees to adequately protect NHM&E data transmitted electronically within the agency or to external agencies when data are not being transmitted through CDC data systems.
g) Your agency agrees that NHM&E data submitted to the CDC will be used for CDC's public health mission.
h) Your agency agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of security and privacy when data are shared.

1.1.6 Data Retention and Disposal

a) Your agency agrees to update and maintain NHM&E data retention and disposal policies and procedures to assure that data cannot be inappropriately accessed.
b) Your agency agrees to be responsible for staying abreast of state and federal statutes on data retention and disposal and to fully comply with all applicable statutes.
c) Your agency agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of security and privacy for data retention and disposal.

1.1.7 Policies and Procedures

a) Your agency agrees to be responsible for establishing, publishing, implementing, and making available policies on NHM&E data security and client privacy at your agency. These policies should be informed by federal and state statutes, regulations, and case laws regarding the protection of HIV data.
b) Your agency agrees to document NHM&E data security policies and procedures and annually train staff on procedures pertaining to NHM&E data security and client privacy.
c) Your agency agrees to be responsible for communicating policy and procedures to those expected to abide by them.
d) Your agency agrees to establish policies and procedures that accommodate participation in CDC site visits conducted to determine compliance with this MOU and other recommended data security measures.
e) Your agency agrees to be responsible for ensuring that a sanction policy is in place to hold individuals responsible for their actions.

f) Your agency agrees to take measures through policies and procedures as necessary, in addition to those mentioned in this document, to maintain high levels of security and privacy.

1.1.8 Agreements

a) Your agency agrees to be responsible for implementing NHM&E data security and client privacy agreements that are meant to be signed annually by agency staff assigned to work with NHM&E data.
b) Your agency agrees to comply with this MOU signed by your agency and the CDC.
c) Your agency agrees to develop and implement any necessary NHM&E data release/use agreements with collaborating agencies, institutions, or individuals.
d) Your agency acknowledges that failure to abide by this MOU may result in termination of this and other related agreements.

1.2 The CDC

Upon submission, the CDC agrees to be responsible for protecting NHM&E data and assuring system security as defined in the Assurance of Confidentiality (AOC). Security encompasses data confidentiality, integrity and availability.

1.2.1 Data Storage

a) The CDC agrees to be responsible for ensuring that CDC data systems and supporting infrastructure are housed in a physically secure location where access is limited to authorized personnel.
b) The CDC agrees to store NHM&E data submitted by your agency in a central secure data repository at the CDC.
c) The CDC agrees that NHM&E data stored in the central data repository will be accessible to only a select few individuals (e.g., database administrator, CDC IT staff).
d) The CDC agrees that safeguards to protect data stored in CDC data systems have been implemented.
e) The CDC has implemented encryption technology to ensure that sensitive client-identifying data are encrypted while stored on the CDC database server.
f) The CDC has implemented controls in CDC data systems to protect data stored in CDC data systems from being accessed by unauthorized users.
g) The CDC has implemented controls in the form of application and data backup, disaster recovery, and contingency planning.
h) The CDC agrees to take other measures as necessary, in addition to those mentioned in this document, to maintain high levels of security and privacy of data stored at CDC.

1.2.2 Data Use

a) The CDC agrees to ensure that only authorized staff at CDC that have signed confidentiality agreements will have access to NHM&E data submitted to CDC.
b) The CDC agrees to use NHM&E data in a manner that is in accordance with federal statutes.
c) The CDC will use NHM&E data submitted to CDC data systems for analysis, report generation, evaluation, and monitoring of the CDC-funded HIV prevention programs.
d) The CDC agrees to be responsible for implementing and regularly updating policies and procedures for the use of NHM&E data at the federal level.
e) The CDC has implemented data and system access safeguards to control access to NHM&E data submitted to CDC.
f) The CDC has implemented data and system access safeguards to control access to data submitted to CDC.
g) The CDC agrees that NHM&E data shared within CDC will be used for the CDC's public health mission.
h) The CDC agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of security as data are used.

1.2.3 Data Sharing

a) The CDC agrees to be responsible for implementing and updating policies and procedures for the publication and redistribution of NHM&E data.
b) The CDC agrees to ensure secure electronic transmission of NHM&E data to CDC when your agency submits data to CDC data systems.
c) The CDC will require that all NHM&E data submitted to CDC are transmitted through a secure data network.
d) The CDC requires that NHM&E data submitted to CDC through the secure data network are encrypted.
e) The CDC will require the non-CDC Data System Administrators to acknowledge a potential authorized user's need to hold a security certificate, and the necessary user rights/levels of this certificate.
f) The CDC has implemented web intrusion detection software for use by CDC data systems.
g) The CDC agrees to take measures through policies and procedures, as necessary, in addition to those mentioned in this document, to maintain high levels of security when data are shared within CDC.

1.2.4 Data Retention and Disposal

a) The CDC agrees to maintain and update NHM&E data retention and disposal policies and procedures.
b) The CDC will comply with federal statutes on data retention and disposal.
c) The CDC agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of security when data are retained and disposed.

1.2.5 Policy and Procedures

a) The CDC agrees to be responsible for establishing, updating, publishing, implementing, and making available policies on NHM&E data and system security.
b) The CDC agrees to document procedures and train CDC staff, contractors, and guest workers on the procedures pertaining to NHM&E data and system security.
c) The CDC agrees to be responsible for communicating policy and procedures to those expected to abide by them at the CDC.
d) The CDC agrees to be responsible for ensuring that a sanction policy is in place to hold individuals responsible for their actions.
e) The CDC agrees to take measures through policies and procedures as necessary, in addition to those mentioned in this document, to maintain high levels of NHM&E data and system security.

1.2.6 Agreements

a) The CDC agrees to be responsible for implementing NHM&E data and system agreements (i.e., non-disclosure agreements, confidentiality agreements, etc.) to be signed by CDC staff who work with CDC data system application, database, and data analysis and security.
b) The CDC agrees to comply with this MOU signed by your agency and the CDC.
c) The CDC agrees to seek reasonable consultation and input while preparing and updating this MOU.
d) The CDC agrees to follow recommended procedures while updating and amending this MOU or handling disputes related to this MOU.

1.2.7 System Security

a) The CDC will be responsible for implementing control measures to mitigate risks to CDC data systems.
b) The CDC agrees to conduct routine security self-assessments.
c) The CDC agrees to ensure that any individual with access to NHM&E data has the routine CDC Security Awareness training, and that this is documented and monitored.
d) The CDC has written full authorization for the operation of the CDC data systems.
e) The CDC agrees to be responsible for CDC data system security, both application and database security after submission of data to CDC.
f) The CDC agrees that a detailed security plan for CDC data systems has been documented.
g) The CDC requires that non-CDC data systems are accessed using identification and authentication such as security certificates, non-CDC data system user identification and passwords.

2.0 Training of Non-CDC Data Systems Users

2.1 External Agency

a) Your agency will be responsible for effectively training agency staff annually on the use of non-CDC data systems and the NHM&E data variables.
b) Your agency will be responsible for annually training agency staff on policies and procedures pertinent to NHM&E data security and client privacy.
c) Your agency will be responsible for providing annual security and privacy awareness training to agency staff.

2.2 The CDC

a) The CDC will be responsible for effectively training its staff, contractors, and guest workers annually on the use of CDC data systems.
b) CDC will also provide training on CDC data systems to external users, when possible.
c) The CDC will be responsible for training its staff on policies and procedures pertinent to CDC data system security and client privacy.
d) The CDC will be responsible for providing annual security and privacy awareness training to its staff.

3.0 System Maintenance

a) The CDC will not be responsible for non-CDC data system maintenance.
b) Your agency will be responsible for the maintenance of the infrastructure upon which non-CDC data systems reside. Your agency will also be responsible for the implementation of updates necessary to transfer NHM&E data to CDC, as determined by future modifications of the NHM&E variable requirements.

4.0 Access to Non-CDC Data Systems

4.1 External Agency

a) Authorized staff from your agency will access non-CDC data systems through security procedures such as password protection or e-authentication procedures.
b) Your agency agrees to define, document, implement, and frequently update ROBs, policies, and procedures for non-CDC data system access.
c) Your agency agrees to ensure that security certificates and other security measures are used to access applications used to submit data from non-CDC data systems to CDC.
d) Your agency agrees to ensure that security certificates and other security measures are used appropriately and that users apply for a new digital certificate or renew their certificates and other security measures each year.

e) Your agency agrees to document and maintain a list of local authorized users with security certificates and to promptly inform CDC when a user's certificate is no longer necessary or if there are any changes to a user's permission rights granted by CDC.
f) Your agency agrees to ensure that a process is in place to request, establish, issue, document current account holders, and close non-CDC data system user accounts.
g) Your agency agrees to maintain an approved up-to-date listing of authorized non-CDC data system users and their access levels.
h) Your agency will ensure that written policies are readily accessible to any staff with access to NHM&E data.
i) Your agency agrees to ensure that user identifications and passwords are managed accordingly, hence ensuring proper identification and authentication of users.
j) All suspected or actual breaches of confidentiality or security of NHM&E records or data involving personally identifiable information (PII) such as names, addresses, identification numbers, dates (except year), etc., should be reported to the CDC Information Systems Security Officer (phone 404.639.1806; e-mail:rxv2@cdc.gov) and the CDC Division of HIV/AIDS Prevention (DHAP) Program Evaluation Branch (PEB) Data Security Steward (phone: 404-718-8636; e-mail: swr2@cdc.gov) **within one hour of discovery**. All other (non-PII) suspected or actual breaches of confidentiality or security (e.g., possible virus attacks, hackers, password divulgence, lost or misplaced storage media without PII, failure to follow secure storage policies, etc.) should be immediately reported to your 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 DHAP PEB Data Security Steward. In consultation with appropriate legal counsel, the Agency System Administrator should determine whether a breach warrants reporting to law enforcement agencies. Sanctions for violations of confidentiality protocols should be established in writing, as part of the agency policies, and should be consistently enforced.
k) Your agency agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of system security during system access.

4.2 The CDC

a) The CDC will have a certificate authority for security certificates.
b) The CDC will, with the assistance of the state's non-CDC Data System Administrator, verify the identity of all digital certificate requestors.
c) The CDC will ensure that written policies are readily accessible to any staff having access to NHM&E data.
d) The CDC has implemented mechanisms to control access to CDC data systems only to authorized users through identification and authentication.

e) The CDC agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of system security when the system is accessed.

5.0 Non-CDC Data Systems Privacy

a) Your agency agrees to be responsible for adequately protecting client privacy at your agency. Client privacy is a right protected by law.
b) Your agency agrees to be responsible for ensuring that NHM&E data are collected in a manner that ensures client privacy and meets current state HIV testing consent and confidentiality laws.
c) Your agency agrees to be responsible for annually training its staff on privacy issues.
d) Your agency agrees to be responsible for complying with all relevant federal and state statutes on privacy (e.g., HIPAA, if applicable.)
e) Your agency agrees to take measures as necessary, in addition to those mentioned in this document, to maintain high levels of privacy.

6.0 Non-CDC Data Systems Technical Assistance

6.1 External Agency

a) Your agency agrees to provide technical assistance to your non-CDC data system users and the non-CDC data system users of your directly funded organizations.

6.2 The CDC

a) The CDC agrees to provide technical assistance for CDC data systems through the NHM&E Service Center.
b) The CDC will provide details to your agency on how to obtain technical assistance on CDC data systems (e-mail or phone).
c) The CDC will support the following types of issues:
    - CDC data system software questions
    - CDC data systems IT related programmatic questions
    - CDC data systems network questions
    - Security certificate questions
    - CDC data systems import/export and data extraction questions
    - Data file submission or transfer questions

7.0 Non-CDC Data Systems Users Roles and Responsibilities

7.1 External Agency

a) Your agency will select a non-CDC Data System Administrator who will define and document the roles and responsibilities of the non-CDC data system users, and how they are aligned with non-CDC data system access levels.

The non-CDC Data System Administrator will also be responsible for verifying non-CDC data system users who need to access NHM&E data and the access levels necessary when requested by CDC employees.

b) Your agency agrees to be responsible for ensuring that roles and responsibilities are documented, including a current list of individuals with access to non-CDC data systems and their respective roles and responsibilities.
c) Your agency agrees to obtain signatures that confirm agreement with current security measures from all current employees and contractors and all new employees and contractors who replace or assume the duties of current signatories to security documents.
d) Your agency non-CDC Data System Administrator will notify CDC if there are any changes or replacements to staff that require access to or termination from the secure data network.
e) Your agency non-CDC Data System Administrator will annually document certification that all components of the MOU regarding your agency are met.

7.2 The CDC

a) The CDC will designate CDC staff to assign security certificates or passwords and other security measures to users of CDC data systems.
b) The CDC will designate information security staff for CDC data systems.

8.0 Rules of Behavior

8.1 External Agency

a) Your agency agrees that all non-CDC data system users at your agency and the agencies you fund will read and comply with the Rules of Behavior (ROB) outlined for users and system administrators.
b) Your agency agrees to require all your users of non-CDC data systems read, understand, sign, and agree to abide by the ROB for Non-CDC Data System Agency Users.
c) Your agency agrees to have your System Administrator of non-CDC data systems read, understand, sign, and agree to abide by the ROB for Non-CDC Data System Agency System Administrators.
d) Your agency agrees to put in place and require every user of every agency you fund to sign an ROB for Non-CDC Data System Agency Users.
e) Your agency agrees to put in place and have every system administrator of every agency you fund read, understand, sign, and agree to abide by the ROB for Non-CDC Data System Agency System Administrators.
f) Your agency agrees that each staff member with authorized access to non-CDC data systems will sign either the ROB for Non-CDC Data System Agency Users (for users) or the ROB for Non-CDC Data System Agency System Administrators (for administrators) every two years.

g) Your agency agrees to keep the ROB for Non-CDC Data System Agency Users and ROB for Non-CDC Data System Agency System Administrators (where appropriate) on file for five years.

8.2 The CDC

a) The CDC will provide your agency with rules of behavior describing what is and is not permitted, defining and describing:
   - Ethical conduct
   - Authentication management
   - Information management and document handling
   - System access and usage
   - Incident reporting
   - Training and awareness

b) The CDC will keep the MOUs with our directly funded agencies on file for five years, but all the documents should be affirmed annually.

9.0 Monitoring

9.1 External Agency

a) Your agency agrees to periodically (at least annually) assess its data security measures and compliance to all required standards, regulation, and data security guidelines.
b) Your agency agrees to periodically assess the data security measures and compliance to all required standards, regulation, and data security guidelines for its partners and sub-contracting agencies.

9.2 The CDC

a) The CDC realizes how critical it is to protect client privacy and data security, and will periodically assess whether your agency is implementing necessary controls to safeguard the security of NHM&E data and client privacy.
b) The CDC will assess whether CDC directly funded agencies are meeting the terms of this MOU.
c) CDC will monitor timely completion and submission of signed MOUs.
d) The CDC will provide technical assistance if non-compliance is observed.
e) The CDC, through regular security operations with the Office of the Chief Information Security Officer (OCISO), will determine when sanctions are necessary, including but not limited to inability to use CDC data systems.

Memorandum of Understanding (MOU) between
the Centers for Disease Control and Prevention (CDC)
and Directly Funded Agency(ies) for use of the Non-CDC Data Systems

Agreed to and accepted by the NCHHSTP Business Steward:

Dale Stratford

Dale Stratford, PhD, Chief, Program Evaluation Branch, DHAP

Date: July 1st, 2011

I certify that I have read the Non-CDC Data Systems Memorandum of Understanding (including the Rules of Behavior document). On behalf of my agency, I hereby acknowledge the intent to comply with the terms and procedures stated in this document.

_____

Name of Non-CDC data system covered by this agreement

_____

Name and title of the authorizing representative of the directly funded agency

Name of directly funded agency: _____

Date: _____

Telephone Number: _____