

---

ATTACHMENT VI

---

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

---

The purpose of this Memorandum of Understanding is to serve as a written understanding between the Centers for Disease Control and Prevention and the directly funded organizations that use the Centralized Program Evaluation and Monitoring System (CPEMS) or other CDC-licensed or owned systems. It provides a framework for cooperation between Centers for Disease Control and Prevention and the directly funded organizations to maintain security and confidentiality, training, access, technical assistance, and responsibilities related to application or other CDC software.

**CDC Licensed or Owned Data Systems**

The CPEMS deployment model is a centrally hosted version of the CPEMS software, and all the data entered are stored in databases at CDC. The system entails a web server, an application server, and a database server. CDC may also license or utilize other CDC-owned systems for management, collection, or submission of data from CDC-funded HIV prevention programs.

---

**1.0 CDC Data Systems Confidentiality and Security**

---

**1.1 External Agency**

Your agency agrees to be responsible for protecting National HIV Prevention Program Monitoring and Evaluation (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 the Centralized Program Evaluation and Monitoring System (CPEMS) or other CDC-licensed or owned system. Security encompasses data confidentiality, integrity and availability. Client privacy is a right protected by the law.

**1.1.1 Data Collection**

- a) Your agency agrees to adequately protect paper records collected at your agency.
- b) Your agency agrees to adequately protect electronic data collected by your agency.
- c) 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.
- d) Your agency agrees to follow current HIV testing consent and counseling statutes applicable during data collection.
- e) If your agency collects the needed NHM&E data with identifiers, only de-identified data will be submitted to CDC through CDC Data Systems.

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.

- f) 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 data entered into CDC Data Systems at your agency are entered under levels of security commensurate with the security described in the Security Summary for CDC Data Systems Users, ensuring that client confidentiality is maintained.
- b) Your agency agrees to ensure that NHM&E data entered directly or indirectly into Data Systems are input only by staff authorized by your agency.
- c) Your agency agrees to ensure that data integrity is maintained and NHM&E data entered in CDC Data Systems are not altered for misrepresentation or falsification purposes.
- d) Your agency agrees to ensure that if NHM&E data are entered indirectly into CDC Data Systems, such as, into a hand held device, the data on the hand held device are protected from security breaches and data are kept confidential.
- e) Your agency agrees that data entry will occur in a confidential environment, safeguarding against unauthorized disclosure of client information.
- f) Your agency agrees that users of 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 to be responsible for ensuring that paper records and NHM&E electronic data at your agency are stored in a physically secure location where access is limited to authorized personnel.
- b) 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.
- c) Your agency's NHM&E data will be stored in a data repository at the CDC. (See Section 1.2 for CDC responsibilities).
- d) Your agency agrees to make data backups based on a locally recommended (OIT) schedule and to securely store these backups.
- e) Your agency agrees to establish, test, implement, and frequently revise a local data recovery plan.
- f) 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 data.

### **1.1.4 Data Use**

- a) Your agency agrees to ensure that 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 data.
- c) Your agency agrees to use data in a manner that adequately protects client privacy.
- d) Your agency agrees to use data in a manner that is in accordance with federal and state statutes.
- e) Where appropriate, your agency agrees to use data in accordance with the Institutional Review Board (IRB) of your location and get 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 data use.
- g) Your agency agrees to be responsible for implementing and updating policies and procedures for the use of 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 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 data.
- j) Your agency agrees that users of CDC Data Systems will require identification and authentication to access the system for use of data stored in CDC Data Systems.
- 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 to be responsible for implementing policies and procedures for publication and redistribution of data.
- b) Your agency agrees to adequately protect data transported within your agency or to external agencies.
- c) Your agency agrees to comply with all current policies and procedures that are necessary for the submission of NHM&E data electronically via the CDC Secure Data Network (SDN).
- d) Your agency agrees to ensure that all SDN certificates are authorized and current.
- e) Your agency agrees to be responsible for implementing and updating policies and procedures for publication and redistribution of data and ensuring that client confidentiality will be maintained during this process.
- f) Your agency agrees to acknowledge parties supporting publications while engaging in publications that depend on NHM&E data.
- g) Your agency agrees to adequately protect data transmitted electronically within the agency, or to external agencies when data are not being transmitted through CDC Data Systems.

- h) Your agency agrees that data submitted to the CDC will be used for CDC's public health mission.
- i) 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 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 agrees to fully comply with all 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 data security and client privacy at your agency. These policies should be informed by federal and state statutes, regulations, and case law regarding the protection of HIV data.
- b) Your agency agrees to document procedures and annually train staff on the procedures pertaining to 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 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 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 memorandum of understanding signed by your agency and the CDC.
- c) Your agency agrees to develop and implement any necessary 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**

The CDC agrees to be responsible for protecting NHM&E data and system security as defined in the Assurance of Confidentiality (AOC) and CDC Data Systems Security Summary. 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 with access limited to authorized personnel.
- b) The CDC agrees to store data collected by your agency in a central secure data repository at the CDC.
- c) The CDC agrees that data stored in the central data repository will be accessible to only a select few individuals (e.g. database administrator, CDC IT staff) at the CDC.
- d) The CDC agrees that safeguards to protect data stored in CDC Data Systems have been implemented.
- e) The CDC has agreed to implement encryption technology to ensure that sensitive client-identifying data, as defined in the Security Summary, 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 in CDC Data Systems.

### **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 the data submitted to CDC.
- b) The CDC agrees to use data in a manner that is in accordance with federal statutes.
- c) The CDC will use 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 use of NHM&E data at the federal level.
- e) The CDC has implemented data and system access safeguards to control access to data submitted to CDC.
- f) The CDC agrees that data shared within CDC will be used for the CDC's public health mission.
- g) 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 will house two separate databases for data in CDC Data Systems. The transactional database, will house all the data that the grantee enters into CDC Data Systems (with identifiers, if applicable.) The submission database will house the data that are actually submitted to CDC as part of the data reporting requirements. The submission database will contain data stripped of any client identifying information.
- b) The CDC agrees to be responsible for implementing and updating policies and procedures for publication and redistribution of data.
- c) The CDC agrees to ensure secure electronic transmission of NHM&E data to CDC when your agency submits data in CDC Data Systems.
- d) The CDC will require that all data submitted to CDC is transmitted through the CDC Secure Data Network (SDN).
- e) The CDC will require the CPEMS Systems Administrators to acknowledge a potential authorized user's need to hold an SDN digital certificate, and the necessary rights/levels of this certificate.
- f) The CDC requires that NHM&E data submitted to CDC through the SDN are encrypted.
- g) The CDC/SDN has implemented web intrusion detection software for use by CDC Data Systems.
- h) 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 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 staff on the procedures pertaining to 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 data and system security.

### **1.2.6 Agreements**

- a) The CDC agrees to be responsible for implementing data and system agreements (i.e. non-disclosure agreements, confidentiality agreements, etc) to be signed by CDC staff who work with CDC Data Systems application, database, analysis and security.
- b) The CDC agrees to comply with this Memorandum of Understanding (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, 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 this is documented and monitored.
- d) The CDC has written full authorization for the operation of CDC Data Systems.
- e) The CDC agrees to be responsible for CDC Data Systems security, both application and database security before and after submission of data to CDC.
- f) The CDC agrees that CDC Data Systems has undergone system security certification and accreditation and this has been documented.
- g) The CDC agrees that a detailed security plan has been documented.
- h) The CDC has implemented mechanisms in CDC Data Systems to track system activities.
- i) The CDC has implemented a service system to support CDC Data System users.
- j) The CDC requires that CDC Data Systems are accessed using identification and authentication such as digital certificates, CDC Data System user identification, and passwords.

---

## **2.0 Training of CDC Data Systems Users**

---

### **2.1 External Agency**

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

---

## **3.0 CDC Data Systems Maintenance**

---

- a) The CDC will be responsible for the maintenance of the infrastructure upon which CPEMS and other CDC-owned systems reside. CDC is not responsible for infrastructure maintenance of CDC-licensed systems.

---

## **4.0 Access to CDC Data Systems**

---

### **4.1 External Agency**

- a) Authorized staff from your agency will access CDC Data Systems through a digital certificate or through other required security procedures, such as password protection or eAuthentication procedures.
- b) Your agency agrees to ensure that digital 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.
- c) Your agency agrees to document and maintain a list of local authorized users with SDN digital certificates and to promptly inform CDC when a user's certificate or password is no longer necessary or if there are any changes to the permission rights granted by CDC.
- d) Your agency agrees to ensure that a process is in place to request, establish, issue, document current account holders, and close user accounts.
- e) Your agency agrees to maintain an approved up-to-date listing of authorized users and their access levels.
- f) Your agency will ensure that written policies are readily accessible to any staff with access to NHM&E data.
- g) Your agency agrees to ensure that user identifications and passwords are managed accordingly, hence ensuring proper identification and authentication of users.
- h) Suspected or actual breaches of confidentiality must be reported to your System Administrator, who will determine the nature and extent of the breach and, if necessary, immediately report it to the CDC Data Systems Security Coordinator via the NHM&E Service Center (1-888-736-7311) or assigned Program Prevention Branch (PPB) Project Officer. If the breach was local, the System Administrator will investigate to determine the cause, and develop

and implement process improvements to correct. Sanctions for violations of confidentiality protocols should be established in writing, as part of the agency policies and should be consistently enforced.

- i) 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 digital certificates.
- b) The CDC will, with the assistance of the state's CPEMS System's Administrator, verify the identity of the digital certificate requestor.
- 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 to only 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 CDC Data Systems Privacy**

---

#### **5.1 External Agency**

- 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 data are collected in a manner that ensures client privacy and meets current 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.

#### **5.2 The CDC**

- a) The CDC agrees to abide by the privacy rules and regulations applicable to data in CDC Data Systems.

---

### **6.0 CDC Data Systems Technical Assistance**

---

#### **6.1 External Agency**

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

## **6.2 The CDC**

- a) The CDC agrees to provide technical assistance through the Customer Service and 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:
  - o CDC Data Systems software questions
  - o CDC Data Systems IT related programmatic questions
  - o CDC Data Systems network questions
  - o CPEMS digital certificates questions
  - o CDC Data Systems import/export and data extraction questions
  - o CDC Data Systems submission/ transfer questions

---

## **7.0 CDC Data Systems Users Roles and Responsibilities**

---

### **7.1 External Agency**

- a) Your agency will select a CDC Data System Administrator who will define and document the roles and responsibilities of the CDC Data Systems users, and how they are aligned with CDC Data Systems access levels. The CDC DATA System Administrator will also be responsible for verifying CDC Data Systems users need to access data and 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 CDC Data Systems and their respective roles and responsibilities.
- c) Your agency agrees to obtain signatures 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 CDC Data System Administrator will notify CDC if there are any changes or replacements to staff who require access/termination to the Secure Data Network (SDN).
- e) Your agency 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 digital certificates or password and other security measures to users of CDC Data Systems.
- b) The CDC will designate information technology staff.
- c) The CDC will designate a CPEMS Super System Administrator.

---

## **8.0 CDC Data Systems Infrastructure**

---

### **8.1 The CDC**

- a) The CDC agrees that CDC Data Systems are being made accessible to your agency for collection and reporting of HIV prevention data.

- b) The CDC asserts that CDC Data Systems will be secure web based applications.

---

## 9.0 Rules of Behavior

---

### 9.1 External Agency

- a) Your agency agrees that all users at your agency and the agencies you fund will read and comply with the Security Summary.
- b) Your agency agrees to have all your users of CDC Data Systems read, understand, and sign a Rules of Behavior for CDC Data Systems Agency Users.
- c) Your agency agrees to have your System Administrator of CDC Data Systems read, understand, and sign a Rules of Behavior for CDC Data Systems Agency System Administrators.
- d) Your agency agrees to put in place and have every user of every agency you fund sign a Rules of Behavior for CDC Data Systems Agency Users.
- e) Your agency agrees to put in place and have every System Administrator of every agency you fund read, understand, and sign a Rules of Behavior for CDC Data Systems Agency System Administrators.
- f) Your agency agrees that each staff member with authorized access to CDC Data Systems will sign the Rules of Behavior for CDC Data Systems Agency Users and Rules of Behavior for CPEMS Agency System Administrators (where the agency utilizes PEMS) every two years.
- g) Your agency agrees to keep the Rules of Behavior for CDC Data Systems Agency Users and Rules of Behavior for CPEMS Agency System Administrators (where appropriate) on file for five years.

### 9.2 The CDC

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

---

## 10.0 Monitoring

---

### 10.1 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 needed 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 Memorandum of Understanding.
- 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 SDN and 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  
CDC Data Systems**

---

Agreed to and accepted by the NCHHSTP Business Steward:



---

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

Date: October, 09<sup>th</sup> , 2010

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

---

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

Name of directly funded agency \_\_\_\_\_

Date: \_\_\_\_\_

Telephone Number: \_\_\_\_\_