

**REQUEST FOR AN ASSURANCE OF CONFIDENTIALITY FOR  
THE NATIONAL HIV PREVENTION PROGRAM MONITORING AND EVALUATION (NHM&E) FOR  
HIV/AIDS PREVENTION PROGRAM DATA**

**Program Evaluation Branch  
Division of HIV/AIDS Prevention  
National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention  
Revised 2010**

**A. PURPOSE OF THE PROJECT**

The National HIV Prevention Program Monitoring and Evaluation (NHM&E) data are used by the Centers for Disease Control and Prevention (CDC), National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention's Division of HIV/AIDS Prevention (DHAP) to evaluate its funded prevention programs. The NHM&E data will be used for monitoring the delivery of prevention services to clients, implementing and improving HIV prevention programs, and reporting the required program performance indicators. Additionally, NHM&E data will enable CDC to provide valuable feedback to these programs and better account for the use of HIV prevention resources. The request for an Assurance of Confidentiality (AOC) is made to ensure that NHM&E data are safeguarded against unauthorized disclosure of sensitive information collected by the health departments and community based organizations. The Assurance of Confidentiality is granted to provide protection to clients from whom sensitive information is being collected, and to HIV prevention program service providers funded directly or indirectly by DHAP. This AOC applies to all CDC staff and contractors at both on-site and off-site locations.

The President's Management Agenda (PMA) requires all federally funded grantees to report key program performance indicators as a method for demonstrating accountability. The grantees and CDC will use performance indicators to show that the programs they implement or support are efficient and effective in achieving their stated process and outcome goals. NHM&E variables are the data source for most domains of program indicators and will improve CDC's ability to monitor progress in addressing the epidemic, based on quantitative measurements that are consistent across health department jurisdictions and CBOs, and enable the agency to identify prevention needs and target assistance where it is most needed.

**B. NHM&E DATA COLLECTION AND SUBMISSION METHODS**

Agencies funded by CDC to conduct HIV prevention programs collect demographic, behavioral risk, and service utilization data, and may (but are not required to) collect individually identifiable data<sup>1</sup> on persons participating in these programs. For NHM&E data management purposes, each individual client record will be identified by a randomly generated unique key that is linked to a particular agency and state. All funded health jurisdictions and CBOs, under any and all CDC HIV prevention program funding announcements, are required to submit required NHM&E data to CDC via the Secure Data Network (SDN). In addition, data currently identified as optional may be required of grantees that receive additional funding for various special studies or projects, as appropriate. However, no client identifying data will be reported to CDC.

---

<sup>1</sup> The term "Individually identifiable data" is defined by CDC/ATSDR Policy on Releasing and Sharing Data as "data or information which can be used to establish individual identity, either directly, using items such as name, address, unique identifying number, or indirectly by linking data about a case-individual with other information that uniquely identifies them."

Agencies must submit their data electronically in a CDC-defined format or using the CDC-supplied HIV Prevention Program Evaluation and Monitoring System (PEMS) or other CDC supplied systems. PEMS is an optional, electronic, secure, browser-based software application designed to provide the necessary mechanism for collecting and reporting standardized, sensitive HIV prevention data. PEMS resides on the CDC network and supports the persistent encryption of specific data variables identified as sensitive by CDC (see the Security Summary for NHM&E for the list of variables that are encrypted) using the 3DES algorithm. This algorithm, also known as Triple DES, employs a 168-bit encryption key and is compliant with the federal security requirements for cryptographic modules [Federal Information Processing System (FIPS) 140-2]. Thus, some information remains encrypted within the database, visible **only** to the agency that entered it. The system encrypts specified individually identifiable variables and includes an encryption indicator for each of these variables. In addition, on-line help warns users of data variables that will not be encrypted to avoid inadvertent release of sensitive data. Data stored on PEMS servers may be accessible to CDC employees or contractors who are authorized to serve as system administrators or maintain the integrity of software and hardware used to operate PEMS. They **will not**, however, be able to view the encrypted individually identifiable variables. Only health departments or CBOs that input client data will be able to access decrypted information.

Data submitted to CDC will not contain the designated individually identifiable variables (e.g., client names or locating information) but will include select client demographic characteristics (gender, race, ethnicity, year of birth, and HIV status) in addition to intervention and behavioral characteristics.

Although data submitted to CDC will not include client names, there remains a possibility that persons may be indirectly identified as being HIV-infected or as having specific behavioral risks for contracting or transmitting HIV. This may pose a threat to confidentiality if unauthorized persons obtain access to this information. All CDC personnel<sup>2</sup> with access to NHM&E data will be required to adhere to a strict security and confidentiality protocol, participate in annual security and confidentiality training, and sign a 308(d) *Nondisclosure Agreement* and an NHM&E data *Rules of Behavior* agreement.

Clearly, NHM&E involves the collection of highly sensitive data, much of it concerning socially stigmatizing conditions or behaviors. The cooperation of health departments, CBOs, and clients will be very difficult to obtain if concerns about privacy and confidentiality are not addressed. The request for an Assurance of Confidentiality represents an attempt to safeguard data collected in HIV prevention programmatic activities. The Assurance of Confidentiality will be provided on request from the state health department or community based organization. Please see the Security Summary for National HIV Prevention Program Monitoring and Evaluation (NHM&E), which further details the procedures in place to avoid potential security violations.

### C. JUSTIFICATION

1. Extent to which the Assurance of Confidentiality is important to protection of the individual or institution.

For purposes of program monitoring and evaluation, personal and confidential information will be collected by the health department or CBO working with the individual. Program data accessible by or submitted to CDC will not contain individually identifiable data (e.g., client names or locating information), but will include client demographics and exposure characteristics (age, year of birth, gender, race, pregnancy status, HIV status, risk behaviors, etc.). In the cases where health departments or CBOs use centralized PEMS (CPEMS), designated individually identifiable data will remain encrypted within the database, visible **only** to the agency that entered it.

---

<sup>2</sup> CDC personnel include CDC employees, fellows, visiting scientists and others, e.g., contractors.

Since NHM&E tracks individuals who participate in HIV prevention intervention programs conducted by health departments and CBOs and information about HIV test results and descriptive client demographics, a potential risk exists for the indirect identification of an individual participant. As a result, clients are vulnerable to various social harms including discrimination. This discrimination may result from being presumed to be at “high risk” for HIV through sexual behavior or injection drug use, disclosure of sexual assault, disclosure of participant’s initial or subsequent HIV/AIDS status, disclosure of partners’ HIV/AIDS status, and disclosure of illicit drug use. Should these data ever be disclosed, participants may suffer discrimination in securing insurance or future medical treatment, personal discrimination based upon HIV status and presumed risk behavior, job discrimination, and even potential drug-related criminal prosecution.

PEMS software has been designed so that participating health departments, CBOs, and clients will be assigned a randomly generated unique key for use during data collection and in the NHM&E database. Data linking the NHM&E-assigned client key and client names or locating information will be available only to the reporting health department or CBO, not to CDC. XPEMS jurisdictions, which utilize their own or other systems rather than PEMS should generate a client key that fits the PEMS format and include it in their data submission to CDC.

To identify an individual client and his/her data as reported by the provider and submitted through PEMS, one would need to have access to two separately stored data sources: 1) the CDC database containing data submitted by grantees that link the organization’s ID with a PEMS software randomly-generated client key and 2) the grantee data base that links the randomly generated unique client key to his/her name. Although such an event is unlikely to occur, it is theoretically possible. A possible scenario may be: if a legal entity were to subpoena a record, he/she could obtain data regarding the prevention program provider, and he/she would know which provider to approach for information on the client. It cannot be assumed that client records would not be subject to release. The only way to definitively assure confidentiality of client records is to protect the data submitted to CDC with the identity of the prevention program provider and the PEMS application code that encrypts the data designated as “individually identifying.” For prevention program providers to be able to assure confidentiality to their clients and for CDC to assure confidentiality to prevention program providers, client data submitted to CDC and the identification of establishments associated with those data need to be protected against compulsory legal disclosure.

Therefore, we are requesting that the Assurance of Confidentiality be granted to provide protection both to clients on whom sensitive information is being collected and to providers treating the clients and the entities for which they work. These providers may suffer personal or professional discrimination from perceived or potential disclosure of client data and loss of credibility with clients because of presumed data leakage. Because identifying a client would almost certainly require access to provider information linking the client data to a named person, the best way to provide confidentiality to the clients is to protect the data that contain provider and other information submitted to CDC.

Efforts by legislatures, courts, or government agencies to obtain access to records of persons reporting HIV infection, AIDS, illicit drug use, or other high risk behaviors for non-public health purposes (e.g. for civil, criminal, or administrative purposes) have been discouraged or thwarted because of the Assurance of Confidentiality policy. In addition, because of public interest in the epidemic, frequent requests by the public, the media, and others occur, and, because of existing Assurances of Confidentiality and other protections for data, CDC has been able to inform such parties that we cannot release data that could potentially identify, directly or indirectly, any person on whom CDC maintains a record.

Additionally, CDC/DHAP is establishing rules and procedures for the release of aggregate prevention program data. Data for public use will be anonymized before release and cell sizes will be sufficiently large to prevent identification of individuals. The release of data for public use or to particular parties will not occur until data quality (i.e., test for completeness, validity, reliability and reproducibility) is thoroughly scrutinized and evaluated.

Proactive measures have been taken by CDC to ensure client confidentiality and information security, but the potentially damaging personal and identifying information collected requires that clients be given full assurance that the information they disclose will remain confidential.

2. Extent to which the individual or establishment will not furnish or permit access to data being requested unless an Assurance of Confidentiality is given.

Concerns about confidentiality, including mistrust of the government, are likely to exist in the population eligible for CDC-funded HIV prevention interventions. Disclosure of sensitive information regarding HIV status, drug use, or sexual behavior may result in social or legal repercussions. Individuals who fear that information collected through HIV prevention programs is not protected from disclosures may be reluctant to seek HIV testing and related health services or to reveal sensitive information because of the potential for discrimination.

HIV prevention program providers may be reluctant to risk losing credibility with clients if data are disclosed, and they may not want to be placed in the position of reporting illegal activity (e.g., drug use) to an outside source. Questions have arisen concerning clients' protection from possible disclosures of information through channels authorized by the Freedom of Information Act. Therefore, many health departments and CBOs are reportedly reluctant to report sensitive information about clients unless the information can be protected from disclosure for non-medical purposes by an Assurance of Confidentiality.

The data collected using the NHM&E variables have been determined not to be research data, but data used to evaluate and monitor CDC grantees (health departments and CBOs) funded for a variety of HIV prevention interventions under various program announcements. A major component of the funding requirement is that the funded agencies collect and report intervention data and information about clients served by these interventions. This requirement not only aids the funded agencies to evaluate and monitor their programs, but also provides CDC with information to promote accountability and stewardship of government funds. Successful program evaluation will require funded agencies to collect very sensitive data from their clients to ensure that implemented programs are reducing client risk for HIV, promoting health service utilization, and implementing appropriate and scientifically sound interventions. The success of the evaluation activities hinges primarily on the goodwill of funded agencies and their clients. The likelihood of receiving reports and honest answers on sensitive topics would significantly improve if clients and their health care providers are assured of the confidentiality of their responses. Thus data collected under an Assurance of Confidentiality would be more complete, valid, and reliable. This Assurance of Confidentiality is necessary to effectively monitor and evaluate these federally-funded HIV prevention programs.

3. Extent to which the information cannot be obtained with the same degree of reliability from sources that do not require an Assurance of Confidentiality.

The ability of CDC to effectively assist funded agencies to monitor and evaluate their HIV prevention programs would be greatly hampered if clients and the funded agencies did not report the appropriate and accurate NHM&E data due to concerns that provision of sensitive information could lead to potential litigation or disclosure of such information through subpoena. There is also the possibility of a reporting bias being introduced into the data if some clients or agencies choose not to report due to concerns about confidentiality. These clients and funded agencies are the only sources of information for evaluating the federally funded HIV prevention programs that can ensure that programs are being implemented soundly and effectively. It is vital that data from these sources be collected under an Assurance of Confidentiality.

4. Extent to which the information is essential to the success of the particular statistical or epidemiological project and is not duplicative of other information gathering activities of the Department.

Collection of these data is critical to CDC's core mission and objectives, for reporting indicators to meet the requirements of the President's Management Agenda and to assess the implementation of activities to meet DHAP's strategic goals and objectives. The NHM&E data variables provide a comprehensive yet parsimonious standardized set of program data useful to evaluate, monitor, and improve individual HIV prevention programs and services provided by CDC-funded health departments and CBOs. NHM&E data also enable CDC to identify best practices and to assist grantees in redesigning HIV prevention strategies that do not accomplish stated goals, such as the reduction of high-risk behaviors in targeted populations.

CDC has taken several steps to avoid duplication of effort. We conducted literature searches to identify data collections already conducted or in progress that might substitute for the data collected in the NHM&E project. Representatives from other Public Health Service data collection projects (Health Resources and Services Administration (HRSA)-Ryan White project and the Substance Abuse and Mental Health Service Administration (SAMHSA)) were contacted to discuss types and methods of data collection. Data variables and collection tools were shared with these projects to enlist recommendations and best practice ideas and assess common data elements.

Within CDC, data elements from several previously used HIV prevention data collection systems were identified and assessed. These include the following systems: Evaluation and Analysis System (ERAS), the Community-based Organizations Systems (CBOS), HIV Counseling and Testing System (CTS), and STD/Management Information System (MIS). To reduce duplication, the NHM&E dataset combines these four datasets into one. With the exception of the STD/MIS system, the other systems (ERAS, CBOS, and CTS) are replaced by the standardized, routinely reported NHM&E data and PEMS and other software. The data collected on STD/MIS have been recently modified to match NHM&E data for those items related to HIV partner services. Most STD/MIS data are not reported to CDC, except for morbidity data, which are reported through the NETSS system (refer to OMB No. 0920-0497, Evaluating CDC Funded Health Department HIV Prevention Programs, Partner Counseling and Referral Services). Only NHM&E partner services data collected in STD/MIS are reported to CDC as part of the NHM&E data collection.

In addition to systems at CDC, other federal systems were reviewed. Specifically, consultations were held with the Health Resources and Services Administration (HRSA) and the Substance Abuse and Mental Health Services Administration (SAMHSA) to identify and match similar data elements to avoid duplication. Given that HRSA and SAMHSA do not collect detailed HIV prevention program data, very few similarities were identified. The only overlap detected was in the collection of HIV testing data, and SAMHSA determined that they would use the NHM&E HIV testing data variables and HIV testing data collection form to collect data from their grantees.

Finally, workshops were held with federally funded HIV prevention grantees and national partners (e.g., National Association of State and Territorial AIDS Directors [NASTAD]) to discuss issues surrounding the sensitive nature of the data to be collected and the many nuances surrounding the proposed data collection methods and strategies.

This is a data collection essential to CDC and does not duplicate any other similarly designed systems.

5. Extent to which an Assurance of Confidentiality would restrain CDC from carrying out any of its responsibilities.

The granting of Section 308(d) Assurance of Confidentiality for PEMS data will not restrict CDC from carrying out any of its responsibilities. The assurance statement, while protecting the privacy rights of HIV prevention program clients and the agencies that collect and submit the data, will enable CDC to collect the data necessary to evaluate and monitor the federally funded HIV prevention programs and

promote appropriate stewardship of public funds. Any CDC personnel with potential access to HIV prevention program client level data or to encryption technology will be required to adhere to strict security and confidentiality protocol and will be required to sign a *308(d) Nondisclosure Agreement* and an *NHM&E Rules of Behavior* agreement.

Occasionally, guest researchers, visiting fellows, and other non-CDC employees may have access to the NHM&E database. Such an arrangement will be time-limited, and will take place under the direct supervision of the Chief of the Program Evaluation Branch. Such non-CDC employees will be required to sign a special 308(d) confidentiality pledge (Attachment G) and undergo formal security and confidentiality training. The training emphasizes that protections in place to hold NHM&E data confidential will last until the person or establishment gives consent for release.

The only known restraint on CDC is on release of data without restrictions. Restrictions will be imposed to insure that confidential information is not disclosed. In addition, some data may be further restricted through the use of statistical methods for disclosure protection (e.g., suppression of cell sizes, random perturbations, recoding, top- or bottom-coding). Such procedures are already done with HIV surveillance data, for example, because small cell size in a small population can allow identification of individuals through induction. Data will be released in the aggregate with appropriate protections to avoid disclosing confidential information. Thus CDC will fulfill its obligation as a good steward of the data while assuring that important information about HIV prevention is available to the public and public health community for public health purposes. Therefore, the 308(d) Assurance of Confidentiality is not considered problematic.

6. Extent to which the advantages of assuring confidentiality outweigh the disadvantages of doing so.

We have identified no disadvantages to CDC receiving an Assurance of Confidentiality for collection of NHM&E data. The Assurance of Confidentiality will increase the accuracy and completeness of reporting by the grantees, thereby enhancing the reliability and validity of the data collected. These HIV prevention data will support the following: (1) management of program operations and service delivery, (2) monitoring and analysis for ongoing program implementation and improvement, and (3) program evaluation to determine the outcome or benefit of services and agency performance on key service indicators. The ability to protect privacy and confidentiality of client information reported through NHM&E to CDC is essential to maintain the credibility CDC has established with the public health community and private organizations. This credibility will assure continued cooperation for implementation of program evaluation and special projects in the future.

No major disadvantages are foreseen by providing the NHM&E project an Assurance of Confidentiality. Therefore, the advantages of this Assurance easily outweigh the disadvantages.

## ATTACHMENT A

### CDC ASSURANCE OF CONFIDENTIALITY

#### ASSURANCE OF CONFIDENTIALITY FOR THE NATIONAL HIV PREVENTION PROGRAM MONITORING AND EVALUATION (NHM&E) HIV PREVENTION PROGRAM DATA

A National HIV Prevention Program Monitoring and Evaluation (NHM&E) data collection process is being implemented by the Program Evaluation Branch (PEB), Division of HIV/AIDS Prevention (DHAP) a component of the Centers for Disease Control and Prevention (CDC), an agency of the United States Department of Health and Human Services. The HIV prevention information requested by CDC through NHM&E consists of data on agency and client characteristics, program plans, and service delivery. This information is collected by CDC-funded health department jurisdictions and community-based organizations in the course of providing HIV prevention services.

The NHM&E data collection process is conducted by CDC-funded health department jurisdictions, community-based organizations and their grantees that submit information to CDC after removing client identifying information such as client name, address, phone, day and month of birth, and other identifying or locating information<sup>3</sup>. Personal characteristics (gender, race, ethnicity, year of birth, pregnancy status, and HIV status), risk behaviors, service utilization and lifestyle information about the individual, and the computer-generated client code will be part of the CDC database. Client records maintained by CDC are identified by a randomly generated computer code linked to a specific health department and agency. The data are used for the management of program operations and service delivery, program monitoring and analysis to support ongoing program improvement, program evaluation to determine the outcome or benefit of services and agency performance on key program indicators, and statistical summaries. The data may also be used for focused evaluation studies.

Information collected by CDC under Section 306 of the Public Health Service (PHS) Act (42 USC 242k) as part of the NHM&E data collection process that would permit direct or indirect identification of individual clients on whom a record collected during the course of HIV prevention services or the identification of two categories of establishments furnishing the information -- the health care providers treating the clients and the entities for which they work -- is collected with the guarantee that it will be held in confidence, will be used only for the purposes stated in this Assurance, and will not otherwise be disclosed or released without the consent of the individual or establishments in accordance with Section 308 (d) of the Public Health Service Act (42 U.S.C. 242m(d)). This protection lasts forever, even after death of the clients.

HIV prevention information reported to CDC will be used (without identifiers) primarily for statistical and analytic summaries for (1) management of program operations and service delivery, (2) monitoring ongoing program implementation and improvement; and (3) program evaluation to determine the outcome or benefit of services and agency performance on key service indicators in which no individual on whom a record is maintained can be identified (directly or indirectly). In addition, data will be used for special evaluations of agency performance, the outcomes or benefits of services, community planning, and characteristics of populations at increased risk for infection or transmission of HIV. When necessary for conducting quality assurance of HIV prevention information or in the interest of public health and disease prevention, CDC may confirm information submitted; in such instances only the minimum amount of information necessary will be disclosed.

No CDC HIV prevention information that could be used to identify any individual on whom a record is maintained, directly or indirectly, or that could identify the establishments furnishing the information --the

---

<sup>3</sup> Individually identifiable data is defined by CDC/ATSDR Policy on Releasing and Sharing Data as "data or information which can be used to establish individual identity, either directly, using items such as name, address, unique identifying number, or indirectly by linking data about a case-individual with other information that uniquely identifies them."

health care providers treating the clients and the entities for which they work-- will be made available to anyone for non-public health purposes. In particular, such information will not be disclosed to the public; to family members; to parties involved in civil, criminal, or administrative litigation, or for commercial purposes, to agencies of the federal, state, or local government.

Information obtained during NHM&E data collection process will be kept confidential. Only authorized employees of the Program Evaluation Branch, Prevention Program Branch, and the Quantitative Sciences and Data Management Branch within the Division of HIV/AIDS Prevention, their contractors, guest evaluators, fellows, visiting scientists, research interns, graduate students and those researchers with a defined public health purpose will have access to the NHM&E data. Information that could indirectly identify clients will not be shared with researchers outside of DHAP except for very rare occasions. These rare occasions may occur if a guest researcher, expert consultant, or other non-employee is invited to work on-site using the database. Such an arrangement will be time-limited, and will take place under the direct supervision of the Chief, Program Evaluation Branch. Additionally, authorized individuals are required to handle the information in accordance with procedures outlined in the *NHM&E Certification and Accreditation Authority to Operate*, the *NHM&E Rules of Behavior*, the *Confidentiality Security Statement for National HIV Prevention Program Monitoring and Evaluation (NHM&E) Data*, the *Nondisclosure Agreement*, the *Agreement to Abide by Restrictions on Release of NHM&E HIV Prevention Program Data Collected and Maintained by the Program Evaluation Branch*, and *Safeguards for Individuals and Establishments Against Invasions of Privacy*.

ATTACHMENT B

THE NATIONAL HIV PREVENTION PROGRAM MONITORING AND EVALUATION FOR HIV/AIDS  
PREVENTION PROGRAMS  
THE CENTERS FOR DISEASE CONTROL AND PREVENTION

CDC NON-RESEARCH DETERMINATION

The project "National HIV Prevention Program Monitoring and Evaluation (NHM&E)" formerly called "Program Evaluation and Monitoring System (PEMS)" has been determined to not be research and an IRB review is not required. See attached letter from Robert Janssen, MD, Director, Division of HIV/AIDS Prevention, National Center for HIV/AIDS, Viral Hepatitis, STD, and TB Prevention.



DEPARTMENT OF HEALTH & HUMAN SERVICES

Public Health Service

Centers for Disease Control  
and Prevention (CDC)  
Atlanta GA 30333

March 8, 2004

**Subject:** Human Subjects and the Program Evaluation and Monitoring System

Dear Colleagues:

In 2003, CDC began the development of a comprehensive Program Evaluation and Monitoring System (PEMS) to improve HIV/AIDS prevention programs, provide enhanced reporting capabilities, and support compliance with federal funding requirements. The purpose of PEMS is to document specific activities being carried out by health departments and community-based organizations funded by CDC under program announcements 04012, 04064, 03003, and 01163. Data collected through PEMS will not be testing new hypotheses or proving the effectiveness of existing or new HIV prevention services. Rather, PEMS will provide a standardized, confidential data collection system to monitor activities funded as part of CDC's HIV prevention program and to track the implementation of the Advancing HIV Prevention initiative by CDC grantees. Since the design and intent of the data collection are not to develop or contribute to generalizable knowledge, but to improve individual HIV prevention programs and services provided by CDC-funded health departments and CBOs, CDC has determined that PEMS is not research and IRB review is not required.

The CDC Associate Director for Science website provides the agency's guidelines for defining research and nonresearch in the public health arena at <http://www.cdc.gov/od/ads/opspoll1.htm>.

Sincerely,

A handwritten signature in black ink that reads "Robert S. Janssen".

Robert S. Janssen, M.D.  
Director, Divisions of HIV/AIDS Prevention

CC: Janet Cleveland, M.S., Deputy Director, DHAP-IRS  
Mac McCraw, B.A., Chief, DHAP-IRS/PPB  
Ida Onorato, M.D., Deputy Director, DHAP-SE  
Julie M. Scofield, Executive Director, NASTAD  
Carlos M. Smiley, Lead Grants Specialist, OD/OCCO/PGO  
Samuel Taveras, M.Ed., Acting Chief, DHAP-IRS/CBB  
Craig W. Thomas, Ph.D., Project Officer, DHAP-IRS/PERB  
Linda Wright-De Agüero, Ph.D., M.P.H., Chief, DHAP-IRS/PERB  
Project Officers, DHAP-IRS/PPB

## ATTACHMENT C

### CONFIDENTIALITY SECURITY STATEMENT FOR NATIONAL HIV PREVENTION PROGRAM MONITORING AND EVALUATION (NHM&E) DATA

The Program Evaluation Branch (PEB), in the Division of HIV/AIDS Prevention (DHAP), National Center for HIV/AIDS, Viral Hepatitis, STD and TB Prevention NCHHSTP has applied for a 308(d) Assurance of Confidentiality protection for data collected through program evaluation activities related to the “**National HIV Prevention Program Monitoring And Evaluation (NHM&E)**” data collection (including counseling and testing information, HIV risk behaviors, client demographics, and intervention characteristics) and conducted under cooperative agreements with local/state/territorial health departments, and community-based organizations (CBOs). Because of this Assurance of Confidentiality, documents and files that contain client-level information are considered confidential materials and are safeguarded to the greatest extent possible. The confidentiality of NHM&E program data collected at the local, state, and organizational levels is protected under state/territorial law, rule, or regulation. Although client names, addresses, phone numbers, or other directly identifying information will not be reported to CDC by health departments or CBOs, NHM&E data are highly sensitive and may have the potential to indirectly identify individuals to whom services are provided. Therefore these NHM&E client level data, the identity of the agency furnishing the information, and the PEMS application or other software that encrypts the client identifying information are required to have 308(d) protection. The security requirement is rated as moderate, according to FIPS Pub 199 and NIST (SP) 800-60, which defines “moderate” as “The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.”

It is the professional, ethical, and legal responsibility of each permanent CDC employee, their contractors, guest researchers, fellows and other non CDC researchers who may be granted access to NHM&E data to protect the confidentiality of all HIV prevention information reported to CDC. This document describes the procedures and practices that DHAP/PEB intends to use to protect the confidentiality of data collected as part of NHM&E.

Portions of the data analysis and programming work that support this project are performed under contract. Therefore, we have included reference to contractors in the Assurance of Confidentiality Statement and this Confidentiality Security Statement. Contractors working with NHM&E data will sign a contractor confidentiality pledge after they complete the required confidentiality and data security training.

Authorized staff of the CDC, contract staff, and other personnel granted access to NHM&E data are required to maintain and protect, at all times, the confidentiality of records that may come into their presence and under their control. In particular, they may not discuss, reveal, present, or confirm to external parties information on, or characteristics of, individuals, or small numbers of cases, in any manner that could directly or indirectly identify any individual on whom a record is maintained by an HIV prevention program or identify the agencies that collect and submit the data. To assure that they are aware of this responsibility and the penalties for failing to comply, each CDC staff member, contract staff, and other staff granted access to program evaluation records or related files, will be required to read and sign a *Nondisclosure Agreement* (CDC 0.979) or the appropriate 308(d) pledge. These documents basically assure that all information in NHM&E records and related files will be kept confidential and will be used only for public health epidemiologic, monitoring, evaluation, or statistical purposes. When the Assurance of Confidentiality is obtained, staff working on NHM&E program and data activities will be required to attend a training session at which the confidentiality procedures for the program activities will be discussed in greater detail by the CDC Confidentiality Officer, a representative of the Office of General Counsel, and the Chief of the Program Evaluation Branch or their designees. Signed agreements will be obtained at this time from each staff person who is authorized to access NHM&E records. Thereafter, security and confidentiality training shall be conducted annually, and participation in such training shall be mandatory for all persons granted access to NHM&E data and related files. PEB staff and their contractors shall be required to sign confidentiality agreements on an annual basis after completing security and confidentiality trainings. It shall be the responsibility of the Technical Steward (PEMS Data

Security Steward) and the PEB Data Security Steward to provide for interim training and obtain signed authorizations from employees and contractors who are granted access to NHM&E data prior to the next annual confidentiality training session.

Attachment D, the CDC Employee Nondisclosure Agreement, and Attachment E, the Contractor's Pledge of 308(d) confidentiality entitled "Safeguards for Individuals and Establishments against Invasions of Privacy" are the Nondisclosure Agreements that will be signed by all federal personnel and federal contractors, respectively, accessing NHM&E data. The originals will be retained by PEB, DHAP for five years, with copies kept at the Office of the Chief Science Officer (OCSO)

Attachment F is the "Agreement to Abide by Restrictions on Release of NHM&E HIV Prevention Program Data Collected and Maintained by the Program Evaluation Branch, Division of HIV/AIDS Prevention," which must be signed by all PEB staff and their contractors who are granted access to records, files and databases containing information from NHM&E. Attachment G "308(d) Assurance of Confidentiality Pledge for Non-CDC Employees." Must be signed by all non CDC employees who are granted access to records, files, and databases containing information from NHM&E.

CDC personnel include CDC employees, fellows, visiting scientists and others, e.g., contractors. Individuals who are not CDC personnel may request access to PEB data. These individuals would request and receive permission to have the (non-individually identified) data (Attachment J--Request for Access to Data by Outside Individuals to Program Evaluation Branch Databases) and sign Attachments I (Pledge of 308(d) Confidentiality for Individuals having access to CDC data) and K (Agreement to Abide by Restrictions on Release of HNM&E HIV Prevention Program Data Collected and Maintained by the Program Evaluation Branch, Division of HIV/AIDS Prevention).

#### **Restrictions on Use of Information and Safeguarding Measures:**

- Information collected in the course of conducting NHM&E activities will be used only for monitoring, evaluation, epidemiologic or statistical purposes related to public health and shall not otherwise be divulged or made known in any manner that could result in the direct or indirect identification of any individual on whom a record is maintained or the establishment furnishing the information.
- CDC personnel and their contractors are responsible for protecting all confidential records containing information that could potentially identify, directly or indirectly, any person on whom a record is maintained, from direct observation, from theft, or from accidental loss or misplacement due to carelessness. All reasonable precautions will be taken to protect confidential program monitoring and evaluation data.
- All contractor personnel will receive project-specific training in security and confidentiality procedures, in addition to the training and background investigations they must undergo prior to being hired by the contractor. All contractors and their records must be maintained in a physically secure environment with appropriate oversight by the technical monitor.
- In the event that NHM&E data confidentiality is breached, (e.g., a grantee fails to remove personal identifiers of individuals, their family members or sexual or drug-using partners before forwarding electronic data to DHAP, or incorrectly enters such identifying data into unencrypted notes fields, lost or misplaced data storage media), a process is in place for reporting and mitigation of any deficiencies that allowed the breach to occur. Upon discovery of the breach, DHAP PEB staff will immediately review and record a description of the breach and notify the CDC Computer Security Incident Response Team (1-866-655-2245) and the PEB Data Security Steward (1-404-718-8636) within one hour of discovery. The PEB Data Security Steward along with the NCHHSTP Information Systems Security Officer (ISSO) will evaluate the suspected breach situations and determine whether a breach in NHM&E data confidentiality or security has occurred. If any confidential or sensitive data were breached, the PEB Data Security Steward and the NCHHSTP Information Systems Security Officer (ISSO) will take responsibility of notifying

responsible local or external staff, PEMS IT, ISSO, OCISO, and, if necessary, the Department of Health and Human Services. After receiving guidance from PEB's Data Security Steward and the NCHHSTP Information Systems Security Officer (ISSO, PEB staff will immediately delete the file from the secure data network (SDN), emails, or hard copies, and document the type of identifiers found, the date and time the file was deleted from the SDN server or emails, actions taken to resolve the issue, and report any finding to the appropriate PEB team leader and PEB Data Security Steward. The project area will be notified orally and the conversation documented. An email notification that details the breach, impact, action steps required, and recommended trainings/readings will also be sent to the project. The entire process of breach notification should be complete within one hour of determination that a breach has occurred.

- Except as needed for operational purposes, photocopies of confidential records are not to be made or transmitted via fax or email. If photocopies or faxes are necessary, they should have no identifying information and care should be taken that all copies and originals are recovered from the copy/fax machines and work areas. Correspondence containing sensitive information, e.g., regarding reports of HIV test results, shall be maintained in a locked file cabinet. All confidential paper records will be destroyed by shredding the documents as soon as operational requirements permit.
- E-mail, memoranda, reports, publications, slides, and presentations that contain data collected through HIV program monitoring or evaluation activities shall not contain data or information that could directly or indirectly identify any person on whom a record is maintained by CDC. In particular, specific geographic identifying information is highly sensitive material. It shall be the responsibility of each CDC staff member and their contractors who are granted access to sensitive NHM&E information to safeguard such data. Only the minimum information necessary to conduct the CDC staff member's or contractor's specific job-related duties shall be accessed. Telephone conversations with local/state/territorial health department or CBO personnel that include discussions of sensitive information shall be conducted discreetly, preferably in private walled offices.

#### **Enhanced Protection of Computerized Files:**

All data will be protected in confidential computer files. The following safeguards are implemented to protect NHM&E files so that the accuracy and the confidentiality of the data can be maintained:

- Computer files containing programs, documents, or confidential data will be stored in computer systems that are protected from accidental alteration and unauthorized access. Computer files will be protected by password systems, access controls which can be audited, virus detection procedures, encryption, and routine backup procedures. XPEMS is an external solution for grantees who prefer not to, or who are unable to support the technology required to migrate to other NHM&E solutions such as PEMS. XPEMS users collect information requested by the CDC, process the data locally, convert the data into a format that complies with the NHM&E application, and transfer the requested data, either directly or indirectly through a CDC-licensed system, using the CDC Secure Data Network (SDN). The SDN serves as a secure medium of communication to transport data sent via XPEMS and scanning servers. HIV prevention data collected and stored at state and local health departments using XPEMS or CDC recommended scanning or other systems are required as part of their cooperative agreement award, to certify through a memorandum of understanding, that they comply with security recommendations PEMS and SDN software ensure that sensitive data are encrypted and securely transmitted to CDC.
- Some agencies may use a centralized web-based solution for data collection consisting of a web server, application server, and a database server that resides on the CDC network (this is referred to as PEMS). These data may contain names or other personally identifying information on individuals participating in CDC-funded HIV prevention program activities. If an agency is a PEMS user, PEMS supports the persistent encryption of specific data variables using the 3DES algorithm. This algorithm is also known as Triple DES, employs a 168-bit encryption key and is

compliant with the federal security requirements for cryptographic modules (Federal Information Processing System [FIPS] 140-2). Thus, some information remains encrypted within the database, visible **only** to the agency that entered it. Although data collection forms and software that CDC provides to NHM&E cooperative agreement recipients for reporting on CDC-sponsored HIV prevention program projects or activities may enable the collection of personal identifiers at the local, state, territorial or CBO level, these identifiers are not transmitted to DHAP.

- The NHM&E data submitted to CDC will contain only PEMS-generated or XPEMS-generated unique client codes. However, because these are 308(d) protected data, they will be transmitted to CDC in a secure and confidential manner. Electronic data are transmitted via a secure socket layer (SSL) or via the SDN connection with the PEMS web server and application server at CDC. In the case of PEMS or other CDC system, all data transmissions are automatically encrypted by the software that generates the transfer files after deleting any personally identifying information. In addition, a select number of NHM&E variables collected by health departments or community-based organizations (CBOs) that relate to personally identifying information (such as reported age, agency client codes, last name, first name) are encrypted within the PEMS database and visible only to the agency that entered the information.
- The DHAP local area network (LAN) and mainframe computers maintained by CDC's Information Technology Services Office (ITSO) comply with Federal policies, statutes, regulations, and other directives for the collection, maintenance, use, and dissemination of data, including the Department of Health and Human Services Automated Information Systems Security Program and the Computer Security Act of 1987 (Public Law 100-235). Additionally, the LAN is in compliance with CDC's ITSO Automated Data Processing (ADP) Security Policy. The DHAP LAN currently operates under Windows. Security features implemented include user ID and password protection, mandatory password changes, limited logins, user rights/file attribute restrictions, and virus protection.
- For users of PEMS, data will be entered through a web browser into PEMS by staff at state and local health departments and CBOs, and transmitted via SSL to the PEMS application and databases supported by CDC-Information Technology Services Office (ITSO). Grantees using their own locally-developed software systems will convert the data into a format that complies with the PEMS application and transfer the data, directly or indirectly through a CDC-system, via SDN. The data will then be uploaded from the PEMS database into the DHAP Local Area Network (LAN). Access to the files, only upon express written approval by the NHM&E Business Steward, will be granted to DHAP employees, or contractors, and any ITSO or other CDC employees or contractors who service or maintain the systems or components necessary to support the management of NHM&E program and data files. The list of authorized users will be maintained by the NHM&E Technical and Business Stewards and the LAN administrator. This list of users will be reviewed on at least an annual basis to delete individuals no longer needing access.
- Backup copies of LAN data will be made by the LAN tape backup system; data on ITSO databases is backed up by the ITSO backup system. Backup services for both sets of data are provided under a separate CDC-wide contract. Contractor facilities and staff are subject to the same Federal policies, statutes, regulations, and other directives, as well as to departmental and CDC security policies, which apply to CDC ITSO and LAN computers and staff. Access to LAN backup tapes is restricted to three DHAP staff: the LAN administrator, the Network administrator, and the computer help-desk coordinator). Access to the CDC ITSO backup tapes is restricted to authorized personnel. Contractors are prohibited from any access to backup tapes without written permission from the Business or Technical Stewards.

#### **Dissemination of Data from HIV Prevention Program Activities**

State and local health departments and CBOs receive confirmation of their transmittals of data to CDC.

CDC staff is responsible for timely dissemination of aggregate data at the national level, consistent with the data release policies of the *CDC/ATSDR Policy on Releasing and Sharing Data*. Data will generally be reported only in aggregate form as summary statistics, including suppression of cell sizes and geographic identifiers; such summary statistics cannot be used to indirectly identify an individual or the establishment furnishing the data. In addition, some data may be further restricted through the use of statistical methods for disclosure protection (e.g., random perturbations, recoding, top- or bottom-coding). Modes of disseminating data include reports, articles in the *MMWR*, publications, and public use slide sets. DHAP PEB staff may provide data in response to special requests from Congress, the Department of HHS, other government agencies, and other programs within CDC on a priority basis with the approval of the Director, DHAP, the PEB Branch Chief or the PEMS Business or Technical Stewards. These data will only be provided in summary tables and analyses that do not allow for the direct or indirect identification of clients or establishments providing the requested intervention information.

#### **Records Disposition for the National Archives and Records Administration**

Records that are determined to be permanently valuable are sent to the National Archives and Records Administration (NARA). Transfers of such records and files will be done in accordance with the May 1996 agreement stating that CDC will transfer to NARA all permanent data sets in accordance with approved schedules contained in part IV of the CDC Records Control Schedule B-321, with the exception of identifying information collected under an Assurance of Confidentiality agreement as specified under the Public Health Service Act, Sections 301(d) and 308(d).

**ATTACHMENT D**

**NONDISCLOSURE AGREEMENT FOR FEDERAL PERSONNEL**

*(308(d) Assurance of Confidentiality for CDC/DHAP Employees)*

The success of CDC's operations depends upon the voluntary cooperation of States, of establishments, and of individuals who provide the information required by CDC programs under an assurance that such information will be kept confidential and be used only for monitoring, evaluation, epidemiological or statistical purposes.

When confidentiality is authorized, CDC operates under the restrictions of Section 308(d) of the Public Health Service Act, which provides in summary that no information obtained in the course of its activities may be used for any purpose other than the purpose for which it was supplied, and that such information may not be published or released in a manner in which the establishment or person supplying the information or described in it is identifiable unless such establishment or person has consented.

"I am aware that unauthorized disclosure of confidential information is punishable under Title 18, Section 1905 of the U.S. Code, which reads:

'Whoever, being an officer or employee of the United States or of any department or agency thereof, publishes, divulges, discloses, or makes known in any manner or to any extent not authorized by law any information coming to him in the course of his employment or official duties or by reason of any examination or investigation made by, or return, report or record made to or filed with, such department or agency or officer or employee thereof, which information concerns or relates to the trade secrets, processes, operations, style of work, or apparatus, or to the identity, confidential statistical data, amount or source of any income, profits, losses, or expenditures of any person, firm, partnership, corporation, or association; or permits any income return or copy thereof or any book containing any abstract or particulars thereof to be seen or examined by any person except as provided by law; shall be fined \$1,000, or imprisoned not more than one year, or both; and shall be removed from office or employment.'

"I understand that unauthorized disclosure of confidential information is also punishable under the Privacy Act of 1974, 5 U.S.C. Section 552a (i) (1), which reads:

'Any officer or employee of any agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established there under, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.'

**My signature below indicates that I have read, understood, and agreed to comply with the above statements.**

\_\_\_\_\_  
Type or Print Name

\_\_\_\_\_  
Date

\_\_\_\_\_  
Signature

\_\_\_\_\_  
Center/Institute/Office (type or print)

## ATTACHMENT E

### **Contractor's Pledge of 308(d) Confidentiality Safeguards for Individuals and Establishments Against Invasions of Privacy**

In accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m), the contractor and employees of the contractor are required to assure confidentiality and to undertake safeguards for individuals and establishments to assure that confidentiality is maintained.

To provide these safeguards in performance of the contract, the contractor and the contractor's employees shall:

1. Be bound by the following confidentiality assurance:

#### **Assurance of Confidentiality**

In accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m), the Director, CDC assures all respondents that the confidentiality of their responses to the request for NHM&E information will be maintained by the contractor and CDC and that no information obtained in the course of this activity will be disclosed in a manner in which the individual or establishment supplying the information is identifiable, unless such individual or establishment has consented to such disclosure. The contractor will release no information from the data obtained or used under this contract to any persons except authorized staff of CDC.

2. Maintain the following safeguards to assure that confidentiality is protected by the contractor and the contractor's employees and to provide for the physical security of the records:

- a. After having read the above assurance of confidentiality, each employee of the contractor participating in this project is to sign the following statement of understanding: I have carefully read and understand the CDC assurance which pertains to the confidential nature of all records to be handled in regard to this data collection. As an employee of the contractor I understand that I am prohibited by law from disclosing any such confidential information which has been obtained under the terms of this contract to anyone other than authorized staff of CDC.

- b. To preclude observation of confidential information by persons not employed on the project, the contractor shall maintain all confidential records that identify individuals or establishments or from which individuals or establishments could be identified under lock and key. Specifically at each site where these items are processed or maintained

- All confidential records that could permit identification of individuals or establishments are to be kept in locked containers when not in use by the contractor's employees. The keys or means of access to these containers are to be held by a limited number of the contractor's staff at each site. When confidential records are being used in a room, admittance to the room is to be restricted to employees pledged to confidentiality and employed on this project. If at any time the contractor's employees are absent from the room, it is to be locked.
- If records are maintained in electronic form, the medium on which the files are stored (floppy disk, CD-ROMS, and removable hard drives) must also be kept in locked containers or, if maintained on a computer, access secured by all available means (including keyboard locks, passwords, encryption, etc., and

office locks).

- Personal computers, desktop or laptop, containing confidential records should never be maintained in an open, unsecured space. Only a limited number of authorized staff may have keys or other means of access to such cabinets or rooms.
- When confidential records are in use, whether by themselves or viewed on computer monitors, these must be kept out of the sight of persons not authorized to work with the records.
- Except as needed for operational purposes, copies of confidential records (paper documents, electronic files, or records of other kinds) are not to be made. Any duplicate copies made of confidential records are to be destroyed as soon as operational requirements permit. Approved means of destruction include shredding, burning, and macerating.
- Should reuse of electronic media (hard drives and rewritable compact disks) containing confidential records be contemplated, extreme care should be taken not to dispose of information in such a way that it can be recovered by unauthorized users of the electronic medium involved.

c. The contractor and his professional staff will take steps to ensure that the intent of the pledge of confidentiality is enforced at all times through appropriate qualifications and standards for all personnel working on this project and through adequate training and periodic follow up procedures.

3. Release no information from the data obtained or used under this contract to any person except authorized staff of CDC.
4. By a specified date, which may be no later than the date of completion of the contract, return all project data to CDC or destroy all such data, as specified by the contract.

---

**My signature below indicates that I have read, understood, and agreed to comply with the above statements.**

---

Type or Print Name

---

Date

---

Signature

---

Center/Institute/Office (type or print)

## ATTACHMENT F

### AGREEMENT TO ABIDE BY RESTRICTIONS ON RELEASE OF NATIONAL HIV PREVENTION PROGRAM MONITORING AND EVALUATION DATA COLLECTED AND MAINTAINED BY THE PROGRAM EVALUATION BRANCH, DIVISION OF HIV/AIDS PREVENTION

I, \_\_\_\_\_, understand that NHM&E data collected by CDC and related NHM&E activities and projects under Section 306 of the Public Health Service Act (42 U.S.C. 242k) are protected at the national level by an Assurance of Confidentiality (Section 308(d) of the Public Health Service Act, 42 U.S.C. 242m (d)), which prohibits disclosure of any information that could be used to directly or indirectly identify any individual on whom a record is maintained by CDC. This prohibition has led to the formulation of the following guidelines for release of prevention program data collected on such persons, to which I agree to adhere. These guidelines represent a balance between the potential for inadvertent disclosure and the need for the CDC/DHAP to be responsive to information requests having legitimate public health application.

Therefore, I will not release, to individuals or agencies outside CDC and the local/state/territorial health department or community-based organization (CBO) reporting the data, specific data in any format (e.g., publications, presentations, slides, interviews) without the consent of the appropriate health department or CBO, except as consistent with the format described below. Specifically, in accordance with the principles of the Assurance of Confidentiality for The Program Evaluation and Monitoring System for HIV Prevention Programs authorized under Section 308d of the U.S. Public Health Service Act:

- I am permitted to release national, regional, local/state/territorial health department and CBO tabulations, from the NHM&E database in either narrative or tabular format, if appropriate statistical methods for disclosure protection (e.g., suppression of cell sizes  $\leq 5$ , random perturbations, recoding, top- or bottom-coding) are implemented.
- I am not permitted to release narrative or tabular data based on denominators (e.g., population size or given characteristics) that pose a risk for individual identification regardless of a given numerator size. For certain populations, the members of which are to be found infrequently in a population, large numbers (e.g.,  $\geq 100,000$ ) may be needed to protect confidentiality. Use of denominator rules must be approved in writing by the Chief, Program Evaluation Branch (PEB), Division of HIV/AIDS Prevention (DHAP), or their designee, prior to release of the data.
- I understand that release of data not specifically permitted by this agreement is prohibited unless written permission is first obtained from the PEB Branch Chief, DHAP or her/his designee.
- When publishing local/state/territorial health department or CBO-specific data in accordance with the restrictions outlined above, I will inform the appropriate state and local health departments or CBO in advance of the release of state, local or CBO data, so as to afford them the opportunity to anticipate local queries and prepare their response.
- I will undertake all reasonable efforts to ensure that no individual could be directly or indirectly identified through a single table or combination of tables, including but not limited to, the restrictions on releasing small cell sizes.
- When presenting or publishing data from HIV prevention program-related studies, investigations, or evaluations, I will adhere to the principles and guidelines outlined in this agreement.
- I will obtain prior review and approval of presentations published articles, graphs, maps, tables, and other materials from the PEB Branch Chief, DHAP or her/his designee.
- I will acknowledge in all reports and presentations of this data, the original source of the data (e.g., the health department or CBO initially providing the data) as well as the name of the PEB

Branch in DHAP that is responsible for preparing and aggregating HIV prevention program data for dissemination.

- I agree that no data will be used for reports, presentations or publications until such time as the quality of the data has been evaluated (including, but not limited to, tests for completeness, validity, reliability, and reproducibility) and approved for sharing or release.
- For data designated “provisional” or “preliminary” by PEB, a provisional data disclaimer shall be included in all reports, presentations and publications.
- I will not attempt to merge the NHM&E dataset with any other dataset without the written permission of the Chief, PEB, DHAP or her/his designee.
- I will not further release the data to any other party without prior written approval of the Chief, PEB, DHAP or her/his designee.

I also agree to the following:

- I will not give my access password or keys to any unauthorized person.
- I will treat all NHM&E data at my worksite confidentially and maintain records that could directly or indirectly identify any individual on whom CDC maintains a record in a locked file cabinet. Sensitive identifying information from special evaluations will only be maintained in a locked file cabinet in a locked room which has restricted access.
- I will keep all hard copies of data runs containing small cells locked in a file cabinet when not in use, shredding them when they are no longer necessary to my analysis.
- I will not produce a “back-up” data file of NHM&E data or related databases maintained by the Program Evaluation Branch DHAP on an unsecured network drive or unapproved storage device.
- I will not remove electronic files, records or databases from the worksite.
- I will not remove hard copies of forms, confidential communications, or any records containing sensitive data and information or the like from the worksite.
- I will access the NHM&E data only through the secure servers storing the data and will not store copies or subsets of the data on a unsecured network drive or other unapproved electronic media.
- I will not remove from the worksite, tabulations or data in any format that could directly or indirectly identify any individual.
- I will maintain confidentiality of records on individuals in all discussions, communications, e-mails, tabulations, presentations, and publications (and the like) by using only the minimum information necessary to describe the individual case.
- I will not release data to the press or media without appropriate clearance procedures and pre-screening of the request by the Office of Communications, NCHHSTP.
- I am responsible for obtaining IRB review of projects when appropriate.

Federal personnel and their contractors, outside of PEB personnel and their contractors, and other staff who request access to PEMS data must also agree to the terms and conditions of the “Confidentiality Security Statement for the National HIV Prevention Program Monitoring and Evaluation Data” and sign the “DHAP/PEB Nondisclosure Agreement” for employees or sign the contractor pledge, “Safeguards for

Individuals and Establishments against Invasions of Privacy” (for contractors). Data requestors should complete the “Request for Access by Federal Personnel and Contractors to Program Evaluation Branch Databases” and clearly and precisely explain the use to which the data will be put and limitations on usage of the data. The requestor’s description of their intended use of the data should provide evidence to PEB, DHAP that there is a legitimate public health purpose that justifies use of the data. The data user should demonstrate their need for restricted-access data and microdata rather than tabular data.

**I have read this document, “Agreement to Abide by Restrictions on Release of NHM&E HIV Prevention Program Data” and I agree to abide by these. Failure to comply with this agreement may result in disciplinary action, including possible termination of employment.**

\_\_\_\_\_  
Name of requestor

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

\_\_\_\_\_  
Signature

\_\_\_\_\_  
CIO, Division, Branch

Approved: \_\_\_\_\_  
Chief, PERB, DHAP, NCHSTP or designee

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

## ATTACHMENT G

### **(308(d) Assurance of Confidentiality Pledge for Non- CDC Personnel)**

I, as a non-CDC Employee (Guest Researcher, Visiting Fellow, Student, Trainee, Employee of a Federal Agency other than CDC, etc.) may be given access to directly or indirectly identifiable data on individuals and institutions that are covered by Section 308(d) of the Public Health Service Act (42 U.S.C. 242m). As a condition of this access, I am required to comply with the following safeguards for individuals and establishments against invasions of privacy.

1. I agree to be bound by the following Assurance of Confidentiality:

In accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. 242m), all participating establishments supplying information or respondents to requests for data are assured by the Director, CDC that this information will be maintained by the individual having authorized access to the data and kept confidential. No information obtained in the course of this activity will be disclosed in a manner in which the individual or establishment supplying the information or described in it is identifiable, unless the individual or establishment has consented to such disclosure, to anyone other than authorized staff of CDC.

After having read the above assurance of confidentiality, each individual having access to potentially identifying data is to sign the following statement of understanding: I have carefully read and understand the CDC assurance which pertains to the confidential nature of all records to be handled in regard to this data collection. I understand that I am prohibited by law from disclosing any such confidential information obtained under the terms of this contract to anyone unless authorized by CDC.

2. I agree to maintain the following safeguards to assure that confidentiality is protected and to provide for the physical security of the records:

- a. To preclude observation of confidential information by unauthorized persons, the individual signing below shall maintain all confidential records that identify individuals or establishments or from which individuals or establishments could be identified under lock and key. Specifically at each site where these items are processed or maintained:

- All confidential records that could permit identification of individuals or establishments are to be kept in locked containers when not in use. The keys or means of access to these containers are to be held by a limited number of individuals. When confidential records are being used in a room, admittance to the room is to be restricted to those pledged to confidentiality. If at any time the individual signing below is absent from the room, it is to be locked.
- If records are maintained in electronic form, the medium on which the files are stored (floppy disk, CD-ROMS, removable hard drives, and their equivalents) must also be kept in locked containers or, if maintained on a computer, access secured by all available means (including keyboard locks, passwords, encryption, etc., and office locks).
- Personal computers, desktop or laptop, containing confidential records should never be maintained in an open, unsecured space. Only a limited number of authorized staff may have keys or other means of access to such cabinets or rooms.
- When confidential records are in use, whether by themselves or viewed on computer monitors, these must be kept out of the sight of persons not authorized to work with the records.
- Except as needed for operational purposes, copies of confidential records (paper

documents, electronic files, or records of other kinds) are not to be made. Any duplicate copies made of confidential records are to be destroyed as soon as operational requirements permit. Approved means of destruction include shredding, burning, and macerating.

- Should reuse of electronic media (hard drives and rewritable compact disks) containing confidential records be contemplated, extreme care should be taken not to dispose of information in such a way that it can be recovered by unauthorized users of the electronic medium involved.

b. The individual signing below will take steps to ensure that the intent of the pledge of confidentiality is enforced at all times through appropriate qualifications and standards for all personnel working having access to the data and through adequate training and periodic follow up procedures.

3. Release no data obtained or used under this contract to any person except that authorized by CDC.

My signature below indicates that I have carefully read understand and agree to comply with this agreement and the statements contained therein and the assurance which pertains to the confidential nature of these records. As a(n) (\_\_\_\_\_) (employee of a Federal agency other than CDC, visiting scientist, guest researcher, fellow, trainee, etc.), I understand that I am prohibited from disclosing any such confidential information that has been obtained under this project to anyone other than authorized staff of CDC forever. I understand that any disclosure in violation of this Confidentiality Pledge will lead to termination of my employment, fellowship or training experience with CDC as well as other penalties.

\_\_\_\_\_  
(Typed/Printed Name)

\_\_\_\_\_  
(Signature and date)

**ATTACHMENT H**

**Request for Data from NCHHSTP/DHAP/Program Evaluation Branch (PEB)  
by Persons Who Are Not CDC FTEs or Contractors**

Note: PEB does not require formal clearance of products resulting from an analysis of national HIV prevention program monitoring and evaluation data unless there is a CDC author on the analysis; however, we would like to see a courtesy copy of any such product.

**Date of Request:**

**Contact Information of Requester (Name, Address, Telephone Number):**

**Domains of Data Requested:**

**Research Question (Purpose of the Investigation) and Justification for Data Request:**

**Database(s) and Variables Requested:**

**Potential Venue for Publication/Presentation:**

**Name of Primary Author:**

**Names of Coauthors:**

**PEB Approval:**

\_\_\_\_\_  
Chief, (PEB), DHAP or designee (signature)      Date

\_\_\_\_\_  
NHM&E Data Technical Steward (signature)      Date

-----  
For PEB Use Only: Retain signed copies of the "Request for data..." "Pledge of 308(d) Confidentiality",  
and the "Agreement to Abide by Restrictions..."