Privacy and Confidentiality Unit:

Assurance of Confidentiality (AoC) Application

Cover Page

Project name:	**"THE NATIONAL HIV PREVENTION PROGRAM MONITORING AND EVALUATION (NHM&E) DATA" (FORMERLY "THE PROGRAM EVALUATION AND MONITORING SYSTEM (PEMS)")**

Contact information

Principle investigator:	**Carolyn Wright**
National Center:	**National Center for HIV, Viral Hepatitis, STD, and TB Prevention**
Division:	**Division of HIV Prevention**
Address:	Click here to enter text.
Phone:	Click here to enter text.
Email:	Click here to enter text.

Table of Contents

Attachments

List all attachments associated with your project or application (Please note some attachments will vary based on the project):
Attachment A: Non-Disclosure Agreement Attachment B: Contrator's Pledge of Agreement

Attachment C: Safeguards for Individuals and Establishments against Invasions of Privacy
Attachment D: Research Determination (attach actual document
Attachment E: Agreement To Abide By Restrictions On Release Of National HIV Prevention Program Monitoring and Evaluation Data
Attachment F: Request for Data from NCHHSTP/DHP/Translation and Evaluation Branch (TEB) by Persons Who Are Not CDC FTEs or Contractors
Attachment G: Privacy Impact Assessment

Current AoC Conditional Approval Period 9/2022 – 9/2027

A) Purpose of Project

Describe the programmatic purpose(s) of the project including the type of data to be collected and the uses of the information collected. This section is a summary of the project and should be approximately two pages.

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, Viral Hepatitis, STD, and TB Prevention's (NCHHSTP) Division of HIV Prevention (DHP) to evaluate its funded HIV prevention programs. The NHM&E data are used for monitoring the delivery of prevention services to individuals, implementing and improving HIV prevention programs, and reporting the required program performance indicators. Additionally, NHM&E data enables 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 (CBOs). The AOC is granted to provide protection to individuals from whom sensitive information is being collected, and to HIV prevention program service providers funded directly or indirectly by DHP. This AOC applies to all CDC staff and contractors at both on-site and off-site locations.

National HIV prevention goals are intended to address three areas: 1) reducing the number of people who become infected with HIV, 2) increasing access to care and improving health outcomes for people with HIV, and 3) reducing HIV-related health disparities. Steps are outlined for federal agencies to support the national HIV prevention goals and specific measurable outcomes tied to these steps. CDC-funded HIV prevention recipients 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 linked to the national HIV prevention goals, the goals of the Ending the HIV Epidemic in the U.S. (EHE) initiative, and the related DHP Strategic Plan. NHM&E data are the source for most domains of HIV prevention program indicators and will improve CDC's ability to monitor progress in addressing the HIV epidemic, based on quantitative measurements that are consistent across health department jurisdictions and CBOs, and enable the agency to identify HIV prevention needs; develop, evaluate, and implement effective prevention strategies; enhance program accountability; and target assistance where it is most needed.

Agencies funded by CDC to conduct HIV prevention programs collect NHM&E data including demographic, priority population, behavioral risk, PrEP awareness and use, and service utilization data (HIV testing, Partner

Services, and other program data). Agencies may (but are not required to) collect individually identifiable data[1] on persons participating in these programs. For NHM&E data management purposes, each individual record will be identified by a unique key that is linked to a particular agency and state. All funded health jurisdictions and CBOs under CDC HIV prevention program Notices of Funding Opportunity (NOFOs) must submit required NHM&E data to CDC through an approved CDC Data System. CDC is currently using EvaluationWeb® or EvalWeb for NHM&E data. EvalWeb is a secure, browser-based software application designed to provide the necessary mechanism for collecting and reporting standardized, sensitive NHM&E data to CDC.

Data Access

EvalWeb resides outside the CDC network and is hosted by Luther Consulting, LLC. Users access EvalWeb via the Secure Access Management System (SAMS) portal. On a schedule determined by CDC, each of the CDC-funded health departments and CBOs send their data, either by key entry or uploading a file, directly to EvalWeb which processes the data and makes specific elements available to authorized agencies or individuals.

Prior to gaining access to EvalWeb, individuals must successfully authenticate their credentials through a process overseen by the CDC. All users must complete Electronic Authentication (E-Authentication) Assurance Level 3 identity proofing requirements. Once a user has successfully completed identity proofing, the completed authorization is transmitted to Luther Consulting via the Secure Access Management System (SAMS). Luther Consulting, LLC will only authorize accounts for individuals who have completed the identity proofing process, who have been recommended by their appropriate jurisdiction, and have been authorized by the CDC program official. A user's access level is assigned based on their organizational role within the recipient jurisdiction. Once users have been granted access, they are required to use second-factor authentication to login by using a SAMS Grid Card or Mobile Soft Token. Both items are issued by SAMS and are unique to an individual. Therefore, users are strictly prohibited from sharing their unique credentials with anyone. Users are also required to read and sign the rules of behavior for EvaluationWeb on an annual basis to ensure they adhere to the requirements for use of the system. As a matter of protocol, SAMS will automatically time out after 30 minutes of inactivity once a user has logged in to EvalWeb. In addition, if a user's EvaluationWeb account shows no activity for an extended period of time (typically 120 days), the account is made inactive and the user must contact the Luther Consulting help desk to re-establish their account.

Luther Consulting, LLC performs, and provides to CDC, monthly host and web application vulnerability scans and corrects any medium, high, or critical vulnerabilities identified in the prescribed timeframe required by CDC. Additional vulnerability scans are provided when a change request is submitted to CDC's Office of the Chief Information Officer (OCIO).

Luther Consulting, LLC maintains configuration management of the EvaluationWeb system by adhering to the System Baseline Configuration (SBC) established by CDC for all system servers. Changes to the system are managed by using the CDC OCIO Information System Change Management (ISCM) Standard Operating Procedures (SOPs), which require all changes to be reviewed and approved by the OCIO prior to implementation into the production environment.

Additionally, the EvaluationWeb system prohibits the use of Secure Socket Layer (SSL) 2 & 3, as required by NIST, and uses Transport Layer Security (TLS) 1.2 as required by CDC to encrypt the browser to browser connection between EvaluationWeb and the Jurisdictions when they upload or key enter data to the system. Additional encryption used by the EvaluationWeb system includes database encryption at the column level using Microsoft SQL Server Enterprise in FIPS Compliant mode, ASA 5515x with Firepower firewalls, and RSA (2048bit PGP or GNUPGP method encryption). All encryption used by the EvaluationWeb system meets Federal

---

1The term "Individually identifiable data" is defined by the 2001 CDC/ATSDR Policy on Releasing and Sharing Data as "data or information which can be used to establish an individual identity, either "directly", using items such as name, address, and unique identifying number, or "indirectly" by linking data about a case-individual with other information that uniquely identifies them."

Information Processing Standards (FIPS) 140-2 requirements and are certified by NIST. The FIPS 199 Security Categorization for the system is moderate for each security objective: Confidentiality, Integrity, and Availability.

B) Justification of Need

Describe why it is important to protect the individual or institution with an Assurance of Confidentiality.

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., individuals' names or locating information), but will include select demographics and personal characteristics (gender, race, year of birth, pregnancy status, and HIV status) in addition to intervention and behavioral characteristics. In the cases where health departments or CBOs use EvalWeb, designated individually identifiable data will remain encrypted within the database, visible ***only*** to the agency that entered it.

Since NHM&E tracks client level data from individuals who participate in HIV prevention intervention programs conducted by health departments and CBOs and information about HIV test results and descriptive demographics, a potential risk exists for the indirect identification of an individual participant. As a result, individuals 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 an individual's initial or subsequent HIV status, disclosure of their partners' HIV 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.

EvalWeb software has been designed so that participating health departments, CBOs, and individuals will be assigned a unique identifier for use during data collection and in the NHM&E database. To identify specific records in EvalWeb, agencies will have the option of independently generating a unique ID or having EvalWeb software generate one for them. Data linking the EvalWeb NHM&E-assigned record identifier and individual's name or locating information will be available only to the reporting health department or CBO, not to CDC.

To identify an individual and his/her data as reported by the provider and submitted through EvalWeb, one would need to have access to two separately stored data sources: 1) the CDC database containing data submitted by recipients that link the organization's ID with a EvalWeb software generated individual's identifier and 2) the recipient database that links the unique individual identifier 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 individual. It cannot be assumed that individuals' records would not be subject to release. The only way to definitively assure confidentiality of individuals' records is to protect the data submitted to CDC with the identity of the prevention program provider and the EvalWeb 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 individuals on whom sensitive information is being collected and to providers treating the individuals and the entities for which they work. These providers may suffer personal or professional discrimination from perceived or

potential disclosure of an individual's data and loss of credibility with individuals because of presumed data leakage. Because identifying an individual would almost certainly require access to provider information linking the individual data to a named person, the best way to provide confidentiality to the individuals 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 HIV epidemic, frequent requests by the public, the media, and others occur, and because of existing Assurances of Confidentiality and other protections of 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/DHP is establishing rules and procedures for the release of aggregate NHM&E 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 individuals of confidentiality and information security, but the potentially damaging personal and identifying information collected requires that individuals be given full assurance that the information they disclose will remain confidential.

Describe why the individual or institution will not furnish or permit access to the information unless an Assurance of Confidentiality is issued.

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 individuals 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 individuals' 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 individuals 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 recipients (health departments and CBOs) funded for a variety of HIV prevention services under various program announcements (Appendix B). A major component of the funding requirement is that the funded agencies collect and report intervention data and information about individuals served by these interventions. This requirement not only helps 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 individual risk for HIV, promoting health service utilization, and implementing appropriate and scientifically sound interventions, thus achieving the goals of EHE. 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 individuals 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.

Describe whether or not the information could be obtained with the same degree of reliability from sources that do not require an assurance.

The ability of CDC to effectively assist funded agencies to monitor and evaluate their HIV prevention programs would be greatly hampered if individuals and the funded agencies did not report 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 individuals or agencies choose not to report due to concerns about confidentiality. These individuals 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.

Describe how 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 of Health and Human Services.

Collection of these data is critical to CDC's core mission and objectives for understanding and reporting outcome measures related to the national HIV prevention goals and to assess the implementation of activities to meet the national HIV prevention goals, EHE, and DHP'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 recipients in redesigning HIV prevention strategies that do not accomplish stated goals, such as the reduction of high-risk behaviors in targeted populations. This data collection is essential to CDC and is not known to duplicate any other similarly designed systems.

Describe how the issuance of the Assurance of Confidentiality might restrain CDC from carrying out any of its responsibilities.

The granting of Section 308(d) Assurance of Confidentiality for NHM&E data will not restrict CDC from carrying out any of its responsibilities. The assurance statement, while protecting the privacy rights of HIV prevention program individuals 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 a 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 Translation and Evaluation Branch. Such non-CDC employees will be required to sign a special 308(d) confidentiality pledge (Attachment E) and undergo formal security and confidentiality training prior to accessing data and annually thereafter. 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 the release of data without restrictions. Restrictions will be imposed to insure that confidential information is not disclosed. Some data may be further restricted using statistical methods for disclosure protection (e.g., suppression of cell sizes, perturbation methods such as random and controlled rounding, recoding). 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

Describe the advantages of assuring confidentiality and how they outweigh the disadvantages.

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 recipients, 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 indicators in support of national HIV prevention goals, EHE, and the DHP Strategic Plan. The ability to protect privacy and confidentiality of individuals' information reported 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 data project an Assurance of Confidentiality. Therefore, the advantages of this Assurance easily outweigh the disadvantages.

C) Confidentiality Assurance Statement

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

A National HIV Prevention Program Monitoring and Evaluation (NHM&E) data collection process is being implemented by the Translation and Evaluation Branch (TEB), Division of HIV Prevention (DHP), 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 consists of data on agency and individuals' characteristics, program plans, and service delivery. This information is collected by CDC-funded health department jurisdictions and community based organizations (CBOs) in the course of providing HIV prevention services.

The NHM&E data collection process is conducted by CDC-funded health departments and community based organizations and their partner agencies that submit information to CDC after removing an individual's identifying information such as an individual's name, address, phone number, day and month of birth, and other identifying or locating information.[1] 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. Individuals' records maintained by CDC are identified by a unique key that is linked to a particular agency and state. 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 individuals 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 individuals 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 individuals.

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

---

2 The term "Individually identifiable data" is defined by 2011 CDC/ATSDR Policy on Releasing and Sharing Data as "data or information which can be used to establish an individual identity, either "directly", using items such as name, address, and unique identifying number, or "indirectly" by linking data about a case-individual with other information that uniquely identifies them."

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 health care providers treating the individuals 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, county, or local government.

Information obtained during the NHM&E data collection process will be kept confidential. Only authorized employees of the Division of HIV Prevention and their contractors, guest evaluators, fellows, visiting scientists, research interns, graduate students, and researchers with a defined public health purpose will have access to the NHM&E data. Information that could indirectly identify individuals will not be shared with researchers outside of DHP 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, Translation and Evaluation Branch. Additionally, authorized individuals are required to handle the information in accordance with procedures outlined in the *NHM&E Rules of Behavior*, the *Confidentiality Security Statement for National HIV Prevention Program Monitoring and Evaluation (NHM&E) Data*, the *Nondisclosure Agreement for Federal Personnel*, the *Agreement to Abide by Restrictions on Release of National HIV Prevention Program Monitoring and Evaluation Data Collected and Maintained by the Translation and Evaluation Branch*, Division of HIV Prevention, and *Safeguards for Individuals and Establishments Against Invasions of Privacy*.

D) Confidentiality Security Statement

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

The Translation and Evaluation Branch (TEB), in the Division of HIV Prevention (DHP), National Center for HIV, 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 HIV testing and partner services information, HIV priority populations, and an individual's demographics and intervention characteristics) and conducted under cooperative agreements with local/state/county/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, county, and organizational levels are protected under state/territorial law, rule, or regulation. Although individuals' 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 EvalWeb application or other software that encrypts the individually 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 DHP/TEB uses to protect the confidentiality of data collected.

Portions of the data analysis and programming work that support this project are conducted 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 Agreemen*t (CDC 0.979) or the appropriate 308(d) pledge. These documents 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 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 Translation and 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. TEB 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 NCHHSTP Technical Steward (NCHHSTP Data Security Steward) and the TEB Data Security Steward to provide 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 Nondisclosure Agreement for Federal Personnel, 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 TEB, Office of the Branch Chief for five years.

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

CDC personnel include CDC employees, fellows, visiting scientists and others, e.g., contractors. Individuals who are not CDC personnel may request access to data. These individuals would request and receive permission to have the (non-individually identified) data (Attachment H--Request for Data from NCHHSTP/DHP/TEB by Persons who are not CDC FTEs or Contractors) and sign Attachment G (308(d) Assurance of Confidentiality Pledge for Non-CDC Personnel) and Attachment F (Agreement to Abide by Restrictions on Release of National HIV Prevention Program Monitoring and Evaluation Data Collected and Maintained by the Translation and Evaluation Branch, Division of HIV Prevention).

Enhanced Measures to Ensure Security and Confidentiality

CDC DHP TEB Policies and Responsibilities

- CDC DHP TEB has developed and adopted written policies and procedures on data security that are reviewed annually and revised when needed. The policies are reviewed by all staff authorized to access confidential NHM&E data. They include: CDC/ATSDR Policy on Releasing and Sharing Data, Rules of Behavior for CDC Staff and Contractors, Nondisclosure Agreement for Federal Personnel, Contractors Pledge for 308(d) Confidentiality, and several policies, standards, procedures and guidelines from the CDC's Office of Chief Information Officer (OCIO).

- The data security policies mentioned above define roles and NHM&E data access levels for all CDC staff and contractors authorized to access confidential NHM&E data, and the procedures for accessing these data securely.

- 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.

- In the event that NHM&E data confidentiality is breached, (e.g., a recipient fails to remove personal identifiers of individuals, their family members, or sexual or drug-using partners before forwarding electronic data to DHP, or incorrectly enters such identifying data into unencrypted notes fields, and 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, DHP TEB 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 TEB Data Security Steward within one hour of discovery of the incident. The TEB 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 TEB Data Security Steward and the NCHHSTP ISSO will take responsibility of notifying responsible local or external staff, EvalWeb staff, ISSO, OCIO, and, if necessary, the Department of Health and Human Services. After receiving guidance from TEB's Data Security Steward and the NCHHSTP ISSO, TEB staff will immediately delete the file from the secure data network, emails, or hard copies, and document the type of identifiers found, the date and time the file was deleted from the server or emails, actions taken to resolve the issue, and report any finding to the appropriate TEB team leader and TEB Data Security Steward. The project area will be notified verbally and the conversation will be documented. An email notification that details the breach, impact, action steps required, and recommended trainings/documents will also be sent to the project area. The entire process of breach notification should be complete within one hour of determination that a breach has occurred.

Data Collection and Use

- Information collected in the course of conducting NHM&E activities will be used only for the original clearly stated purposes, i.e., 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. Only the minimum information needed to conduct specific approved NHM&E activities and achieve a public health goal will be collected and used. No personally identifiable information will be collected by CDC staff and contractors while conducting NHM&E activities.

Physical Security

- 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, theft, or accidental loss or misplacement due to carelessness. All reasonable precautions will be taken to protect confidential program monitoring and evaluation data. Such precautions include but are not limited to: limiting access to secure areas that contain confidential NHM&E data to authorized persons, establishing procedures to control access to secure areas by non-authorized persons, ensuring that CDC staff and contractors working with NHM&E data at offsite locations return the documents to a secure area by close of business.

- 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., reports of HIV test results, shall be maintained in a locked file cabinet. All confidential paper records will be destroyed by shredding the documents using crosscutting shredders before disposal as soon as operational requirements permit.

- All confidential records accessed or held by contractors must be maintained in a physically secure environment with appropriate oversight by a technical monitor.

- 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 individual 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 person 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 person's or contractor's specific job-related duties shall be accessed. Telephone conversations with local/state/county/territorial health department or CBO personnel that include discussions of sensitive information shall be conducted discreetly, preferably in secure offices.

Electronic Data Security and Enhanced Protection of Computerized Files

All electronic data will be protected in confidential computer files. These data will not be stored in private computer systems and non-CDC electronic environments. 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 NHM&E data will be stored in computer systems that are protected from accidental alteration and unauthorized access. Official CDC computers and electronic environments (currently CITGO, VPN) used to access confidential NHM&E data will be protected by protective software, password systems, access controls which can be audited, virus detection procedures, encryption that meets federal standards, and routine backup procedures. CDC-funded HIV prevention programs that collect and store data at state, county, and local health departments for direct transmission to CDC are required, as part of their cooperative agreement award, to submit annually a Certification of Compliance statement signed by an overall responsible party (ORP) to certify, that they comply with CDC security recommendations. The secure browser session using Transport Layer Security (TLS) between CDC and Luther Consulting, LLC serves as a secure medium of communication to transport data sent directly to CDC. The TLS software ensures that sensitive data are encrypted and securely transmitted to CDC.

- All DHP-funded agencies are required to use a secure, browser-based software application, for collecting and reporting standardized, sensitive HIV prevention data. Currently TEB uses EvaluationWeb (EvalWeb) which resides outside the CDC network and is hosted by Luther Consulting, LLC. The data collected or reported to EvalWeb may contain personally identifying information on individuals participating in CDC-funded HIV prevention program activities.
  EvaluationWeb system prohibits the use of Secure Socket Layer (SSL) 2 & 3, as required by NIST, and uses Transport Layer Security (TLS) 1.2 as required by CDC to encrypt the browser to browser connection between EvaluationWeb and the Jurisdictions when they upload or key enter data to the system. Additional encryption used by the EvaluationWeb system includes database encryption at the column level using Microsoft SQL Server Enterprise in FIPS Compliant mode, ASA 5515x with Firepower firewalls, and RSA (2048bit PGP or GNUPGP method encryption). All encryption used by the EvaluationWeb system meets Federal Information Processing Standards (FIPS) 140-2 requirements and are certified by NIST.

Encryption of data at rest ensures that only authorized individuals will have access to view the data in the database. 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, county, territorial, or CBO level, these identifiers are not transmitted to DHP.

- The NHM&E data submitted to CDC via EvalWeb will contain only unique client codes and no personally identifiable information. However, because these are 308(d) protected data, they will be transmitted to CDC in an approved secure and confidential manner. Electronic data transmitted by CDC staff and contractors are done so via a TLS. In the case of EvalWeb, all data transmissions are automatically encrypted by the software that generates the transfer files. In the case of EvalWeb, all data transmissions are automatically encrypted by the software that generates the transfer files. In addition, a select number of NHM&E variables collected by health departments or CBOs that relate to personally identifying information (e.g., age, agency client codes, last name, first name) are encrypted within the EvalWeb database and visible only to the agency that entered the information.

  The DHP Local Area Network (LAN) is maintained by CDC's Information Technology Services Office (ITSO) and complies 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 DHP 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. In addition, the use of a Personal Identity Verification (PIV) card (also called a Smart Card) is required to access network systems. Standardized Smart Cards enhance security, reduce identity fraud, and protect the personal privacy of those issued government identification badges. In order to comply with Homeland Security Presidential Directive 12 (HSPD-12) a valid Smart Card or PIV Card is required.

- For users of EvalWeb, data will be entered through a web browser into EvalWeb by authorized and previously authenticated staff at state, county, and local health departments and CBOs, and transmitted via SSL to the EvalWeb application and databases supported by Luther Consulting, LLC. Access to the files, only upon express written approval by the NHM&E Business Steward, will be granted to DHP 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 E-Authentication Coordinator. This list of users will be reviewed on at least an annual basis to delete individuals no longer needing access.

- Backup services for NHM&E data are performed by Luther Consulting, LLC. 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 authorized computers and staff. Access to the backup data is restricted to authorized personnel.

- The use of personal or company owned equipment and electronic environment to directly access, manage, transfer, store, or download confidential CDC NHM&E data is strictly prohibited. In situations where staff at offsite locations and those without official CDC equipment need to access and manage confidential CDC NHM&E data, this should be done through approved CDC applications such as CITGO or the use of official portable CDC media and devices. CITGO is a Web-based application that CDC employees and contractors can utilize to securely access applications and data remotely.

Dissemination of Data from HIV Prevention Program Activities

- State, county, and local health departments and CBOs receive confirmation of their transmittals of data to EvalWeb. CDC staff are 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. NHM&E information will be released only for purposes related to public health, and sharing of such information will be limited to those with a justified public health need consistent with the original purpose for which NHM&E data were collected. DHP TEB staff may provide data in response to special requests from Congress, the Department of Health and Human Services, other government agencies, and other programs within CDC on a priority basis with the approval of the Director, DHP; the TEB Branch Chief; or the TEB 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 individuals 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 datasets 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).

Reference

1. Centers for Disease Control and Prevention. Data Security and Confidentiality Guidelines for HIV, Viral Hepatitis, Sexually Transmitted Disease, and Tuberculosis Programs: Standards to Facilitate Sharing and Use of Surveillance Data for Public Health Action. Atlanta (GA): U.S. Department of Health and Human Services, Centers for Disease Control and Prevention; 2011. Accessed on 12/15/2011 from: http://www.cdc.gov/nchhstp/programintegration/docs/PCSIDataSecurityGuidelines.pdf.

E) Regulatory Determinations

Non-Research Determination
This activity was reviewed by CDC and was conducted consistent with applicable federal law and CDC policy. See e.g., 45 C.F.R. part 46.102(l)(2), 21 C.F.R. part 56; 42 U.S.C. §241(d); 5 U.S.C. §552a; 44 U.S.C. §3501 et seq. It has been determined that the project is non-research. Please see attachment D.

PRA Determination
The activity was reviewed by CDC and it has been determined that the Paperwork Reduction Act (PRA) applies to this project. *OMB control number is 0920-0696.*
.

Privacy Act Applicability
The activity was reviewed by CDC and it has been determined that the Privacy Act does not apply to this project. *Please provide Privacy Act determination supporting documentation as an attachment.* Please see attachment G.

Attachments

List all attachments associated with your project or application (Please note some attachments will vary based on the project):
Attachment A: Non-Disclosure Agreement Attachment B: Contrator's Pledge of Agreement Attachment C: Safeguards for Individuals and Establishments against Invasions of Privacy Attachment D: Research Determination (attach actual document) Attachment E: Agreement To Abide By Restrictions On Release Of National HIV Prevention Program Monitoring and Evaluation Data Attachment F: Request for Data from NCHHSTP/DHP/Translation and Evaluation Branch (TEB) by Persons Who Are Not CDC FTEs or Contractors Attachment G: Privacy Impact Assessment

ATTACHMENT A

NONDISCLOSURE AGREEMENT FOR DATA COVERED BY AN ASSURANCE OF CONFIDENTIALITY

(*For use with CDC/DHAP employees involved in activities with information covered by a Section 308(d) Assurance of Confidentiality*)

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

When confidentiality is authorized, CDC operates under the restrictions of Section 308(d) of the Public Health Service Act (42 U.S.C. §242m(d)), 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. As a CDC employee granted access to information covered by Section 308(d), I understand and acknowledge that I am bound to comply with the restrictions provided to the information under Section 308(d).

I am aware that unauthorized disclosure of information covered by Section 308(d) of the Public Health Service Act may subject me to disciplinary action.

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

> '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 not more than $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, Subsection 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 thereunder, 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.'

These provisions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by existing statute or Executive order relating to (1) classified information, (2) communications to Congress, (3) the reporting to an Inspector General of a violation of any law, rule, or regulation, or mismanagement, a gross waste of funds, an abuse of authority, or a substantial and specific danger to public health or safety, or (4) any other whistleblower protection. The definitions, requirements, obligations, rights, sanctions, and liabilities created by controlling Executive orders and statutory provisions are incorporated into this agreement and are controlling.

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

_____ _____ _____

Typed/Printed Name Signature Date

_____

National Center/Institute/Office/Branch

ATTACHMENT B

NON-EMPLOYEE 308(d) PLEDGE OF CONFIDENTIALITY

(For use when Non-Employees are provided access to data covered by a 308(d) Assurance of Confidentiality)

I,_____as a non-CDC Employee (e.g., Guest Researcher, Visiting Fellow, Student, Trainee, employee of a federal agency other than CDC, etc.) may be given access to information that is identifiable or potentially identifiable to a person and that is covered by Section 308(d) of the Public Health Service Act (42 U.S.C. §242m(d)), or an Assurance of Confidentiality. As a condition of this access, I am required to comply with the following safeguards for the protection of this covered data.

1. I agree to be bound by the following assurance:

   In accordance with Section 308(d) of the Public Health Service Act (42 U.S.C. §242m(d)), i agree that no information obtained in the course of the activity described in the Assurance of Confidentiality will be used for any purpose other than the purpose for which it was supplied, unless I am informed in writing that such person has consented to its use for such other purposes. Further, I agree that no information obtained in the course of the activity described in the Assurance of Confidentiality will be disclosed in a manner in which the establishment or person supplying the information or described in it is identifiable, unless I am informed in writing that the establishment or person has consented to such disclosure, to anyone other than authorized staff of CDC or staff covered under this 308(d) Assurance.

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

   To preclude observation of confidential information by persons not authorized to have access to the information on the project, I shall maintain all records that I am provided access to that identify establishments or persons covered by this Assurance of Confidentiality or from which establishments or persons covered by this Assurance of Confidentiality could be identified in locked containers or protected computer files when not under immediate supervision by me or another authorized member of the project. The keys or means of access to these containers or files are not to be given to anyone other than those authorized to have access. I further agree to abide by any additional requirements imposed by CDC for safeguarding the identity of establishments or persons covered by this Assurance of Confidentiality.

My signature below indicates that I have carefully read and understand this agreement and the Assurance of Confidentiality, which pertains to the confidential nature of this project. As a(n)

_____ (e.g., visiting scientist, guest researcher, fellow, trainee, employee of a federal agency other than CDC, 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 or persons covered under this Section308(d) Assurance of Confidentiality. I understand that any disclosure in violation of this Confidentiality Pledge may lead to termination of my employment, fellowship, training experience, or scientific collaboration, as well as other penalties.

_____

(Typed/Printed Name)

_____

(Signature)

_____

(Date)

ATTACHMENT C

Agreement of CDC Contractors for Safeguards

Against Invasions of Privacy for Certain Establishments or Persons Covered by an Assurance of Confidentiality

(*For use where Contractors/Subcontracts have access to information covered by a 308(d) Assurance of Confidentiality*)

Access to data covered by an Assurance of Confidentially, titled _____, ("Assurance") as provided by Section 308(d) of the Public Health Service Act (42 U.S.C. §242m(d)), is necessary for certain projects funded through contract task order number(s) _____. Consistent with Section 308(d), the contractor is required to give an assurance of confidentiality and to provide for safeguards to assure that confidentiality of the data covered by the Assurance is maintained.

To provide this assurance and these safeguards in performance of the contract, the contractor shall

1. Be bound by the following assurances:
    a. No information that is identifiable or potentially identifiable to an establishment or person covered by the Assurance and obtained in the course of this activity may be used for any purpose other than the purpose for which it was supplied, unless CDC informs contractor in writing that such establishment or person has consented to its use for such other purposes.
    b. No information that is identifiable or potentially identifiable to an establishment or person covered by the Assurance and obtained in the course of this activity may be disclosed to anyone other than authorized staff of CDC or others noted in the Assurance, unless CDC informs contractor in writing that such establishment or person has consented to its disclosure to such other persons.
    c. No preliminary data from studies or projects that identifies or potentially identifies an establishment or person covered by the Assurance may be disclosed to anyone other than authorized staff of CDC or others noted in the Assurance of Confidentiality statement, unless this information is otherwise in the public domain or CDC has provided written permission for use of this information to be made public. For example, if CDC clears an abstract for a scientific presentation, this constitutes permission for public presentation.
    d. New research study ideas that are not already funded through the above-referenced contract task order may be discussed or presented during calls/meetings as part of normal communications and coordination between CDC and the contractor; should these ideas lead to further activities with information covered by this Assurance, these protections will extend to those activities only if agreed to in writing by CDC.

2. Maintain the following safeguards to assure that the confidentiality provided by Section 308(d) and the Assurance is protected by the contractor and to provide for the physical security of the records:

    a. After having read the above Assurance, each employee of the contractor participating in this project is to sign the following pledge of confidentiality:

I have carefully read and understand the CDC assurance, which pertains to the confidential nature of identifiable or potentially identifiable data covered by the Assurance of Confidentiality to be handled in regard to these studies and reviewed as part of activities under task order _____. As an employee of the contractor, I understand that I am prohibited by law from disclosing any such confidential information that identifies or potentially identifies an establishment or person covered by the Assurance of Confidentiality, which has been obtained under the terms of this contract, to anyone other than authorized staff of CDC and that I may use this information only for the purposes for which it was obtained and consistent with the task order.

b. To preclude observation of confidential information that identifies or potentially identifies an establishment or person covered by the Assurance by persons not employed on the project, the contractor shall maintain all confidential records that identify establishments or persons or from which establishments or persons could be identified under lock and key.

Specifically, at each site where these items are processed or maintained, all confidential records that will permit identification of establishments or persons 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 staff at each site. When confidential records that will permit identification of establishments or persons 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.

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

3. Flow down all requirements set forth in this Agreement to all subcontracts and all subcontract employees.

_____

(Typed/printed Name)

_____

(Signature)

_____

(Date)

ATTACHMENT D Research Determination

ATTACHMENT E

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

I, _____, understand that National HIV Prevention Program Monitoring and Evaluation (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 Division of HIV Prevention (DHP) 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/county/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 National HIV Prevention Program Monitoring and Evaluation 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/county/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 ≤ 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., ≥100,000) may be needed to protect confidentiality. Use of denominator rules must be approved in writing by the Chief, Translation and Evaluation Branch (TEB), DHP, 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 TEB Branch Chief, DHP, or their designee.

- When publishing local/county/state/territorial health department or CBO-specific data in accordance with the restrictions outlined above, I will inform the appropriate state, county, and local health departments or CBO in advance of the release of state, county, 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 TEB Branch Chief, DHP, or their designee.

- I will acknowledge in all reports and presentations of these data, the original source of the data (e.g., the health department or CBO initially providing the data) as well as the name of staff in TEB, DHP who 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 TEB, 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, TEB, DHP, or their designee.

- I will not further release the data to any other party without prior written approval of the Chief, TEB, DHP, or their designee.

I also agree to the following:

- I will not give my access password, passphrase, or keys to any unauthorized person.

- I will treat all NHM&E data at my worksite (i.e., telework, remote, TDY, or office) 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 TEB DHP 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 an 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 TEB personnel and their contractors, and other staff who request access to NHM&E 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 "DHP/TEB 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 Translation and 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 TEB, DHP 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 National HIV Prevention Program Monitoring and Evaluation (NHM&E) 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: _____ Date: _____

Chief, TEB, DHP, NCHHSTP or designee

ATTACHMENT F

Request for Data from NCHHSTP/DHP/Translation and Evaluation Branch (TEB)

by Persons Who Are Not CDC FTEs or Contractors

Note: TEB 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 (*descriptions, time frame, and geographic area covered by data):*

Brief Outline of Proposed Analytic Methods:

Timeline for completing data request:

Potential Venue for Publication/Presentation:

Name of Primary Author:

Names of Coauthors:

TEB Approval:

_____ _____

Chief, (TEB), DHP or designee (signature) Date

_____ _____

TEB Data Technical Steward (signature) Date

- -

For TEB Use Only: Retain signed copies of the “Request for Data from NCHHSTP/DHP/Translation and Evaluation Branch (TEB) by Persons who are not CDC FTEs or Contractors,” “Pledge of 308(d) Confidentiality for Non-CDC Personnel,” and “Agreement to Abide by Restrictions on Release of National HIV Prevention Program Monitoring and Evaluation Data Collected and Maintained by the Translation and Evaluation Branch, Division of HIV Prevention.”

ATTACHMENT G Privacy Impact Assessment