Privacy Act Checklist
OMB control # 0920-0696
National HIV Prevention Program Monitoring and Evaluation Data

Does the data collection involve collecting sensitive or personally identifiable information?

Some of the client-level data to be collected are sensitive. HIV can be transmitted from person to person through sexual contact and the sharing of HIV contaminated needles and syringes. These modes of transmission necessitate the collection of sensitive data regarding sexual behavior and drug use. Because collection of these data will be used to provide improved HIV prevention services to high-risk populations, to enhance HIV prevention programs at the local level, and to reduce high-risk behaviors in persons most likely to acquire or transmit HIV, specific information about client demographics and client behavior and needs is essential to designing appropriate interventions and programs and to monitoring and evaluating these programs.
This data collection also includes race and ethnicity questions, which may also be viewed as sensitive by some respondents, for use in data analysis (e.g., designing and evaluating programs, as discussed above).

The CDC Privacy Review Officer and the NCHHSTP IT Security Information System Security Officer (ISSO), have assessed this data collection for applicability of 5 U.S.C. § 552a, and determined that the Privacy Act does not apply to the overall information collection. A privacy impact assessment was completed (see **Attachment 5**).

Describe how personal information will be maintained and who will have access to it.

All HDs and CBOs funded under CDC HIV prevention program Notice of Funding Opportunity announcements submit National HIV Monitoring and Evaluation (NHM&E) data to CDC through an approved CDC data system. CDC is currently using EvaluationWeb® and REDCap for NHM&E data but will transition to One CDC Data Platform (1-CDP), an internal CDC data system, in 2027.
EvaluationWeb® is a secure, browser-based software application designed to provide the necessary mechanism for collecting and reporting standardized, sensitive NHM&E data. EvaluationWeb® resides outside the CDC network and is managed by Luther Consulting, LLC. Twice per year, each of the participating HDs and CBOs send their data, either by key entry or uploading a file, directly to EvaluationWeb® which processes the data and makes specific elements available to authorized agencies or individuals.

Prior to gaining access to EvaluationWeb®, individuals must successfully authenticate their credentials through a process overseen by CDC and Luther Consulting, LLC. Luther Consulting, LLC enforces required access controls. All users of EvaluationWeb® must complete Electronic Authentication (e-authentication) Assurance Level 3 identity proofing requirements established by CDC. Once a user has completed e-authentication, they are issued a SAMS grid card and 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 successfully completed the identity proofing process, who have been recommended by their appropriate jurisdiction, and have been authorized by the CDC program official. Users are assigned access levels based on their organizational role in the recipient jurisdiction. Once users have been granted access, they can access the system via the SAMS login portal using their SAMS issued grid card. The grid card provides a combination of letters and numbers that are unique to the user. Users are not permitted to share their SAMS issued grid card with anyone. Each user must have their own SAMS grid card. Users must also 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.

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 Office of the Chief Information Security Officer (OCISO) Information System Change Management (ISCM) Standard Operating Procedures (SOP), which requires that all changes must be approved by OCISO prior to implementation into the production environment. EvaluationWeb® is hosted by Amazon Web Services (AWS) in US-East 1 which is rated FedRamp Moderate and inherits all security controls up to the application layer from AWS. The system uses AWS Loadbalancer which uses Transport Layer Security (TLS) 1.3 and accepts TLS 1.2 as required by CDC to encrypt the browser-to-browser connections. Encryption used by the EvaluationWeb® system includes column level SQL encryption (Microsoft CryptoAPI (CNG) FIPS 140-2 CertID# 2936) and uses the AWS Web Application Firewall to block outside counties and malicious traffic. All encryption used by the EvaluationWeb® system meets Federal Information Processing Standards (FIPS) 140-2 requirements as certified by the National Institute of Standards and Technology (NIST).

The EvaluationWeb® system has passed the full Security Assessment and Authorization Process and has an authority to operate (ATO) until August 16, 2027 (**Attachment 7A**). This means that our security measures meet the requirements of the NIST 800-53, HHS, and CDC.

Aggregate and qualitative data are collected through the REDCap system. REDCap is a secure web application designed to manage online data collection for research and/or operations. REDCap has both system-level and user-level security. To grant access to external users, a CDC program official must request access through the CDC REDCap User Access Request tool, prompting users to be e-authenticated through the SAMS federal information technology system. Users will then be added to the REDCap system which can be accessed through authenticated, password-protected logins. The project host must add each individual user to the project and can assign a data access group to each user. The data access group will allow users to only access and enter data assigned to their health department group.

About half the HDs maintain their own electronic data collection systems and upload data from their systems into EvaluationWeb®. The other HDs and all directly funded CBO recipients key-enter data directly into EvaluationWeb®.

1-CDP is an internal CDC data system. Once users have been granted access, they can access the system via the SAMS login portal using their SAMS issued grid card as previously described. All 1-CDP users will complete Electronic Authentication Assurance Level 3 identity proofing requirements. Access to the 1-CDP system will be given by CDC.

1-CDP is classified as a High FIPS 199 system, with High/High/High assurance levels directed for Confidentiality, Integrity, and Availability. Most of 1-CDP's controls are fully inherited from the Palantir Federal Cloud System – High and AWS GovCloud FedRAMP accreditation packages. 1-CDP adheres to FedRAMP High Rev. 5 security controls with Digital Identity Levels (DIL) of IAL3/FAL3/AAL3. 1-CDP uses TLS 1.2 throughout for Data-in-Transit encryption. AWS Key Management Service (KMS) Hardware Security Module is utilized to encrypt all data stored in AWS at the file level. Encryption keys are managed and auto rotated via policy with AWS KMS. All encryption used by 1-CDP meets Federal Information Processing Standards (FIPS) 140-3.

The 1-CDP system has passed the full Security Assessment and Authorization Process and has authority to operate (ATO) until August 16, 2026 (**Attachment 7B**). This means that the system's security measures meet the requirements of the NIST 800-53, HHS, and CDC.

Information about agencies and programs is required as part of the Notice of Funding Opportunity announcement. Information about clients is collected by the agencies as part of their routine data collection, and clients are informed of any consent required by the agency or state regulations. Program data accessible by CDC will not contain client names but will include "sensitive" information such as client demographics (e.g., age, sex, race, HIV status) and behavior. Information in identifiable form, such as name, address, and birthdate may be collected by the HD or CBO working with the individual for purposes of local program activity such as providing case management, but no individually identifiable information will be submitted to CDC.

Whether data is uploaded to EvaluationWeb® using CDC-specified formats or directly entered, no individually identifiable information is submitted to CDC. For NHM&E data management purposes, each individual record will be identified by a unique key that is linked to an agency and state. This key is maintained in EvaluationWeb®, but the client key can only be re-linked to identifiers at the local level. NHM&E data submitted into 1-CDP will only be identified by a unique key that is linked to a funded agency and state. No personally identifiable information will be entered into 1-CDP; neither CDC nor recipient programs will be able to link data to individuals.

How long will sensitive or personal information be maintained? This information is crucial. If sensitive information is maintained for even one day, the Privacy Act will apply and we will have to provide language in the clearance package.

The CDC Privacy Review Officer and the NCHHSTP IT Security Information System Security Officer (ISSO), have assessed this data collection for applicability of 5 U.S.C. § 552a, and determined that the Privacy Act does not apply to the overall information collection (**Attachment 5A and 5B**).

Will the collected information be covered by the appropriate CDC Assurance of Confidentiality?

Yes. All NHM&E data are covered by a CDC Assurance of Confidentiality specific to NHM&E data under the Public Health Services Act 308(d), as well as state confidentiality laws (**Attachment 6**).

If identifiable information will be filed and retrieved by the name of the individual:

No personal information will be collected or maintained.