

Appendix V

PIDS Data Security Plan

This document describes the security features that are employed by the PRAMS Integrated Data Collection System (PIDS). PIDS is a web based centralized system housed at the CDC mid-tier datacenter (MTDC). MTDC is a highly secure facility that houses numerous CDC systems that contain sensitive data such as personally identifiable information (PII).

Security for Mail and Phone Surveys Operations

1. User Access Security

PIDS access is controlled by the Secure Access Management System (SAMS). A user must first be authenticated by SAMS before given access to PIDS. SAMS is a CDC supplied application that is built using best-of-breed COTS security technologies including CA SiteMinder and Identity Manager, and Entrust Identity Guard. SAMS has the highest possible security rating; High / High/ High.

Once a user has been passed the identity proofing process, they will be invited to become a PIDS user. SAMS validates that only the appropriate users have access to the system. This includes username/password authentication to enter the PIDS portal. PIDS uses role based access, allowing states to access ONLY their data. SAMS is also the mechanism used to securely transfer files between States and the CDC. See **Chapter 6 (Data Management)** for a more detailed explanation.

2. Data Security using Encryption

PII data will be transmitted, and loaded into PIDS, from states to CDC through the https protocol. This means that the contents of the transmission between state and CDC are encrypted and rendered meaningless until the transmission is decrypted once received at the CDC. Once the transmission is decrypted at the CDC, data is parsed and loaded into PIDS and fields that are flagged as PII are encrypted and then stored in the database. All PIDS data will be stored and accessed in accordance with industry standard procedures. PIDS employs Blowfish encryption to secure PII fields in the database.

The most stringent security will be imposed on PII data maintained in PIDS. Data stored in PIDS will be accessible to PIDS users based on roles assigned for system access.

PIDS has three distinct user roles for state staff. All users have access to some aspect of respondent PII:

1. Data Manager/Analyst - full access to all data stored in PIDS including PII data; this role is applicable to state administrators, state contract staff, and Contracted PIDS administrators (providing technical support to PIDS).
2. Phone Interviewers – access to the phone module including PII that appears in the CATI header while conducting phone calls.
3. Mail Data Entry Staff- access to data entry module and verification workbench; including limited access to a few PII fields that appear on the data entry screen.

Other users with access to PIDS include contract PIDS developers and CDC staff. Developers have access to PII. CDC staff members do not have access to PII data.

- Please note that it is not permissible to upload or input any SSN into PIDS.
- Question Response data is accessible to all PIDS users. PII data is not included in question response data. Data elements collected include case id (key variable for identifying each record in PIDS) and question response values provided by PRAMS participants.

3. Physical Security

PIDS is located at the CDC MTDC. The MTDC is a highly secure facility using industry standard security for a data center.

Security for Self-Report Web Surveys Operations

1. User Access Security

Mailed letters to mothers will offer the choice of completing the survey on paper or online. The letters provide a unique passcode for each mother and a web address for accessing and completing the survey. The web address is common across all states, but once the mother enters her unique passcode, the server redirects to the state welcome page. Once a mother is granted access to the system, her name and birth year are shown. She has the opportunity to confirm or correct the information that is shown. She also has the option to provide an email address and/or phone number.

2. Data Security using Encryption

Data will be transmitted from moms completing the survey to CDC through the https protocol. This means that the contents of the transmission between mom and CDC are encrypted and rendered meaningless until the transmission is decrypted once received

at the CDC. Once the transmission is decrypted at the CDC, data is parsed and loaded into PIDS and fields that are flagged as PII are encrypted and then stored in the database. All PIDS data will be stored and accessed in accordance with industry standard procedures. PIDS employs Blowfish encryption to secure PII fields in the database.

3. Physical Security

PIDS is located at the CDC MTDC. The MTDC is a highly secure facility using industry standard security for a data center.