



PERSONALLY IDENTIFIABLE INFORMATION (PII) PROTECTION POLICIES MANUAL FOR CDBG STATE PROGRAM

AMENDMENTS TO THE MANUAL

This Manual is subject to amendments, in accordance with changes to federal, state, and Puerto Rico Department of Housing (PRDOH) internal regulatory framework. The amendments to the manual will be published by PRDOH and will be registered in the following table.

MANUAL'S VERSION NUMBER	DATE	BRIEF DESCRIPTION OF THE AMENDMENT
Version 1	May 1,2023	Original version.

CONTENTS

AMENDMENTS TO THE MANUAL.....	1
TITLE.....	1
INTRODUCTION	1
LEGAL BASIS.....	1
PURPOSE	2
APPLICABILITY	3
DEFINITIONS	3
PERSONALLY IDENTIFIABLE INFORMATION (PII)	5
TYPES OF PII.....	6
PUBLIC PII.....	6
SENSITIVE AND PROTECTED PII	6
NON-PII	8
PROCEDURES FOR INTAKE AND PROCESSING OF APPLICANT PROVIDED DOCUMENTATION	9
WRITTEN CONSENT AND COMMUNICATION DESIGNEE	10
PHYSICAL SECURITY OF PII	11
VERBAL SECURITY	13
ELECTRONIC TRANSMISSION OF PII	13
METHODS OF SAFE TRANSMISSION OF PII	14
PASSWORD MANAGEMENT.....	15
ACCEPTABLE METHODS FOR DISPOSAL OF CDBG STATE PROGRAM PII.....	16
PII SECURITY PRACTICES OF STATE CDBG PROGRAM CONTRACTORS AND SUBRECIPIENTS	17

CDBG STATE PROGRAM PII TRAINING.....	18
COMPROMISES OF PII SECURITY	18

TITLE

This Manual shall be known as the "Personally Identifiable Information (PII) Protection Policies Manual for CDBG State Program".

INTRODUCTION

This Manual outlines the methods to collect, document, and properly dispose of applicant hard copy paperwork that contains PII as well establishing acceptable uses and methods of transmission of PII data. Basic components of this policy are to establish proper protocols to:

- Ensure proper handling of hard copy documentation and files.
- Secure hard copy PII in applicant files or documents that are being actively reviewed or worked.
- Establish parameters related to the use of applicant data transmitted and maintained in electronic media.
- Outline potential disciplinary actions for violations of PRDOH's PII policy.
- Establish protocols should a breach of data occur during the administration of PRDOH's Community Development Block Grant (CDBG) State Program.

LEGAL BASIS

This Manual is adopted in accordance with the following laws and regulations:

1. Privacy Act of 1974, as amended (5 U.S.C. § 552a);

2. E-Government Act of 2002 (Pub. L. 107-347, 44 U.S.C. § 101);
3. Implementation of Privacy Act of 1974, as revised (40 CFR Part 16);
4. Federal Acquisition Regulation (FAR), Protection of Individual Privacy (48 CFR Subpart 24.1);
5. *Uniform Administrative Requirements, Cost Principles, And Audit Requirements for Federal Awards* (2 CFR Part 200),
6. Puerto Rico Department of Housing Organic Act (Act 103-2001, as amended),
7. Open Data Act of the Government of Puerto Rico (Act 122-2019);
8. Policy for Cyber Security, Puerto Rico Innovation & Technology Service (PRITS), 2021; and
9. Standards for Cyber Security, Puerto Rico Innovation & Technology Service (PRITS), 2021.

PURPOSE

This Manual presents the standards and procedures to be followed by the PRDOH's CDBG State Program for the protection of Personal Identifiable Information in the tasks it manages. They are intended as a guide, which seeks to comply with federal, state, and PRDOH's internal regulations, including the Privacy Act of 1974, the E-Government Act of 2002, 2 CFR 200.303(e), and policy and guidance issued by the President and Office of Management and Budget (OMB).

These policies have the objective of protecting the right to confidentiality and the protection of confidential and/or sensitive information throughout PRDOH's CDBG State Program. Furthermore, it has the purpose to ensure the confidentiality and integrity of PII provided in a hard copy format and/or electronically stored or transmitted. It will also help to safeguard CDBG State Program participants, employees, subrecipients, and contractors confidential or sensitive information from any potential breach.

APPLICABILITY

This Manual will apply to all activities subsidized in whole or in part with CDBG State funds administered by the PRDOH. Likewise, it will apply to all persons that perform tasks related to PRDOH's CDBG State Program including employees, staff, providers, vendors, suppliers, contractors, subcontractors, consultants, partners, applicants, and subrecipients.

Similarly, municipalities that receive allocations of CDBG State funds as subrecipients through PRDOH, must have their written policies and procedures on PII protection in compliance with the federal, state, and local regulations.

DEFINITIONS

For purposes of this Manual, the terms below will have the following definitions:

1. Applicant - A person who has requested assistance from subrecipients of the PRDOH's State CDBG Program.
2. Department or PRDOH - Puerto Rico Department of Housing.

3. Breach - Occurs when personally identifiable information is viewed, leaked, or accessed by anyone who is not the individual or someone authorized to have access to this information, as part of their official duties.
4. Confidential and/or sensitive information - Refers to information about an individual or pertaining to a business that the person or business would not want to be disclosed to unauthorized parties.
5. Confidentiality - The protection of personal and/or sensitive information.
6. Contractor - A private company that produces goods and services for the public government agencies by means of a contract, subcontract, purchase order, agreement, or other similar arrangement.
7. Non-Personally Identifiable Information (Non PII) - Information that is not sufficient to distinguish or trace the identity of the person to whom such information belongs.
8. Nondisclosure - The act of not making something known.
9. Personally Identifiable Information (PII) - Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual (2 CFR 200.79). Information which can be used to distinguish or trace an individual's identity (e.g., their name, social security number, biometric records) by itself, or when combined with other personal or identifying information which is linked or linkable to a specific individual, (e.g., date and place of birth, mother's maiden name).
10. Protected PII - Means an individual's first name or first initial and last name *in combination with* any one or more types of information, including, but not limited to, Social Security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical or financial records, and

educational transcripts. Protected PII does not include information that is required by law to be disclosed (2 CFR 200.82).

11. Public PII - Personally identifiable information that is available in public sources such as telephone books, public web sites, and university listings (2 CFR 200.79).

12. Secretary - Secretary of Puerto Rico Department of Housing.

13. Sensitive PII - The personally identifiable information that when lost, compromised, or disclosed without authorization could substantially harm an individual. Sensitive PII can encompass standalone information or information paired with another identifier.

14. Subrecipient - A municipality receiving funds from PRDOH's CDBG State Program. It is further defined at 2 C.F.R. § 200.93, as a non-Federal entity that receives a subaward from a passthrough entity to carry out part of a federal program.

15. System of Records - Group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

PERSONALLY IDENTIFIABLE INFORMATION (PII)

In order to implement the CDBG State Program, PRDOH needs to collect, maintain, use, retrieve, and disseminate information related to those individuals who apply for assistance. Due to the nature of the program, Applicant's records may contain income information, insurance information, bank account numbers, passwords, Personal Identification Numbers (PIN), housing inspection reports, and annotations of various types of assistance.

Some, if not most of the information on the Applicant's records is considered personally identifiable information.

PII refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual, e.g., their full name, social security number (including only the last-4 digits), biometric data, policy numbers, award amounts, income, and bank account information.

TYPES OF PII

PUBLIC PII

Public PII is information that is available in public sources such as telephone books, public websites, and university listings. It includes, for example, first and last name, address, work telephone number, email address, home telephone number, and general educational credentials.

SENSITIVE AND PROTECTED PII

Protected PII means an individual's first name or first initial and last name in combination with any one or more of types of information, including, but not limited to, social security number, passport number, credit card numbers, clearances, bank numbers, biometrics, date and place of birth, mother's maiden name, criminal, medical and financial records, educational transcripts. This does not include PII that is required by law to be disclosed (2 CFR 200.82).

In determining what PII is sensitive, the context in which the PII is used must be considered. For example, a list of people subscribing to a PRDOH newsletter is not sensitive PII; a list of people receiving treatment for substance abuse is sensitive PII.

As well as context, the association of two or more non-sensitive PII elements may result in sensitive PII. For instance, the name of an individual would be sensitive when grouped with place and date of birth and/or mother's maiden name, but each of these elements would not be sensitive independent of one another. Therefore files/data may be sensitive as a whole, but individual data points or documents may not be considered sensitive. This means the file/data must be handled as sensitive PII.

For determining which PII may be electronically transmitted, the following types of PII are considered sensitive when they are associated with an individual. Secure methods must be employed in transmitting this data when associated with an individual:

- Place of birth;
- Date of birth;
- Full Name, Mother's maiden name;
- Biometric information and personal characteristics including photographic images, fingerprints, handwriting, retina scan, voice signature, and facial geometry;

- Medical information, except brief references to absences from work;
- Personal financial information (account numbers, award amounts, income);
- Credit card or purchase card account numbers;
- Passport numbers, driver's license number and tax payer ID;
- Potentially sensitive CDBG State Program information related to grant or loan awards (applicant identification number, grant/loan amounts, among others);
- Criminal history;
- Any information that may stigmatize or adversely affect an individual; and
- SSN or the last 4 digits of a SSN alone.

NON-PII

The following additional types of PII may be transmitted electronically without protection because they are not considered sufficiently sensitive to require protection.

- Work phone numbers;
- Work addresses;
- Work e-mail addresses;
- Documents that do not include an SSN or where the SSN is removed or other applicant sensitive information (CDBG Program applicant identification number or award amounts); and

- General background information about individuals found in their application for assistance.

The determination that certain PII is non-sensitive does not mean it is publicly releasable. The determination to publicly release any information can only be made by the official authorized to make such determinations.

PROCEDURES FOR INTAKE AND PROCESSING OF APPLICANT PROVIDED DOCUMENTATION

PRDOH's CDBG State Program, in conjunction with contractors and sub-recipients, will ensure that all PII discussed with and received by program applicants will be protected and retained as necessary. During intake of these documents, case managers must ensure that only required PII be retained by the CDBG Program. During intake sessions, only required program documents shall be scanned/filed into PRDOH or the subrecipients' system of record with original documentation returned to the applicant during the intake meeting. In the event hard copies of the documents are retained for review and use of the Program, hard copy documents must be appropriately stored or filed in a secure location until they can be shredded or returned to the applicant. A secure location means that they are locked in the case manager's desk or stored in a locked file cabinet when not in use. In addition, PRDOH requires that all mail or written correspondence to the applicant must be uploaded into the system of record and/or hard copy file within 24 hours of any notification by regular mail. In addition, all case managers granted access to

PII must acknowledge and follow PRDOH's policies regarding the physical, verbal, and electronic security of PII as outlined below.

WRITTEN CONSENT AND COMMUNICATION DESIGNEE

Applicant information is subject to the Federal Privacy Act of 1974, thus, “[p]ersonal information may be used only by authorized persons in the conduct of official business”. The use of information will be limited to ensuring compliance with CDBG State Program regulations; reducing errors and mitigating fraud and abuse; and the disclosure of this information will only be to those for whom the Applicant has provided written consent to do so. Consent should be obtained from the involved parties when disclosing confidential or sensitive information concerning a CDBG State Program participant, employee, or contractor. The Consent form discloses the details to be shared and be signed and dated by the affected party. Certain federal programs provide for Applicants to designate a third party to obtain information on their Program application. This third party is known as a Communication Designee. They may obtain information from and provide information to the Program on behalf of the Applicant; they may not, however, sign any document or enter into any agreement unless they have been vested with a Power of Attorney.

PRDOH, subrecipients and contractor employees and staff should only have access to confidential or sensitive information from their own program. Program Guidelines include dispositions that ensure the confidentiality of

program applicants as well as the protection and safeguarding of files. An exception to the limitation of access to confidential or sensitive information contemplates the need to provide access to monitoring or oversight agencies or bodies, and their personnel, whether they be federal, state or local. Monitoring and oversight activities are very important roles in helping PRDOH with the proper implementation of CDBG State Program and its funds. Notwithstanding this exception, monitoring or oversight personnel who are granted access to files, documents, computers, and other devices, containing PII must employ the same level of caution any PRDOH staff, subrecipient or contractor should employ. Information disclosed shall be limited to the precise program or area being monitored or overseen, access must be supervised, and any electronic access shall have uniquely tailored roles and privileges that allow for tracking and keeping records of accessed information.

PRDOH and Subrecipients employees, contractors, partner agencies, staff, and other personnel with access to confidential or sensitive information must complete a Confidentiality and Non-disclosure agreement. This agreement is part of the employee, contractor, partner agency, staff, or personnel file, along with an acknowledgement of receipt of this Policy. This agreement, in summary, establishes that neither party nor any of its employees shall divulge or release data or information developed or obtained from the contractual relationship.

Physical security applies to all paper documents or files, as well as CDs, floppy disks, USB drives, tapes, and backups containing PII. PRDOH requires the following for all items that should be physically secured:

- Access to documents containing PII is limited based on a legitimate business need for the information and document. Only CDBG State Program designated personnel shall have access to PII. Sensitive documents shall not be left out when CDBG State Program personnel is away from their desk.
- CDBG State Program employees must log off their computers and lock their desks and file cabinets at the end of the day.
- Access to PII shall be limited or not granted for any CDBG State Program personnel with an actual or perceived conflict of interest.
- Documents containing PII must be shredded when no longer required for the CDBG State Program purpose for which they were collected.
- Documents containing PII should be stored in locked drawers or program file cabinets unless the office space itself is considered a controlled space with no access permitted to non-designated personnel.
- Access control to office spaces containing documents with keyed or electronic locks will be used if locked file cabinets are not in use. Access control may be used in conjunction with locked file cabinets.

- Files are only to be removed from locked cabinets when in use. Locked fireproof file cabinets must be used for all collateral files or documents (e.g., grant or loan agreements, covenants, among others).
- Keys to secure spaces are controlled and logged/assigned.
- Combinations given out to employees are logged.
- Management is to review changing locks and combinations upon staff changes.
- CDBG State Program employees should notify management staff immediately if they see an unfamiliar person that receives and stores applicant PII.

VERBAL SECURITY

CDBG State Program employees, contractors, and subrecipients granted access to PII must exercise precautions when discussing PII.

- PII should not be shared with coworkers unless it is required for them to complete their job duties.
- Limit information when leaving voicemail to name of facility and return phone number.
- No PII should be discussed in public places.

ELECTRONIC TRANSMISSION OF PII

Examples of electronic transmission of PII, include, but are not limited to:

- E-mail, text, and instant messages;

- Document(s) attached to an e-mail message;
- File Transfer Protocol (FTP);
- General Web Services;
- File Sharing Services; and
- Electronic Data Interchange (EDI).

METHODS OF SAFE TRANSMISSION OF PII

Although the transmission of PII is strongly discouraged by PRDOH, there may be instances when this type of information must be shared among CDBG State Program staff. If this situation arises during the administration of the CDBG State Program, there are several methods considered acceptable when transmitting PII:

- Installing encryption software on a select number of desktops and designating those computers for the transmission of sensitive PII.
- Using encryption software to encrypt the sensitive PII before sending it electronically, e.g., as an e-mail attachment. The password key should be forwarded to the recipient in a separate e-mail from the attached file or mailed.
- Using an application designed to protect the transmission of sensitive PII, e.g., Web-based applications that use TLS1.0, secure file share, or secure file transfer applications such as Secure Shell File Transport Protocol (SFTP).

- Sending documents with sensitive PII by facsimile is permissible if the sender alerts the designated recipient that sensitive PII is being sent. The recipient must then verify by phone or e-mail that the information has been received.
- Transfer of information via secure web applications.
- Transfer of information via VPN.
- FTP in conjunction with encryption unless secure/encrypted FTP protocols have been put into place.

In addition to the above listed protocols, anti-virus and anti-spyware programs on individual computers and on servers on the CDBG State Program network should be regularly run by PRDOH.

PASSWORD MANAGEMENT

The PRDOH also requires that CDBG State Program personnel, contractors and/or subrecipients control access to sensitive information by requiring the use of “strong” passwords (e.g., a mix of letters, numbers, and characters) and multifactorial authentication (MFA). Passwords to enter the PRDOH CDBG State Program system should be frequently changed. In addition, PRDOH requires the following in the execution of CDBG State Program activities:

- Sharing passwords or posting them near CDBG State Program workstations is not permitted.
- Password-activated screen savers must be used to lock employee computers after a period of inactivity.

- Users who don't enter the correct password within a designated number of log-on attempts should be locked out of the CDBG State Program system.

ACCEPTABLE METHODS FOR DISPOSAL OF CDBG STATE PROGRAM PII

PRDOH requires all CDBG State Program staff, contractors, and subrecipients to properly dispose of sensitive information so that it cannot be read or reconstructed. Acceptable disposal methods are:

- Paper - shredding, burning, and/or pulverizing.
- Electronic Media
 - If the media cannot be physically destroyed like a CD or DVD, data wiping software that permanently removes the PII data from the storage device must be used.
 - CDs and DVDs can be shredded or burned.

In order to effectively carry out these procedures the following must occur:

- Document shredders should be made available throughout the workplace, including next to the photocopier.
- Disposal of computers and portable storage devices must include the use of software for securely erasing data and hard drive so that the files are no longer recoverable.

PII SECURITY PRACTICES OF STATE CDBG PROGRAM CONTRACTORS AND SUBRECIPIENTS

All CDBG State Program contracts or grant agreements with PRDOH will require that all contractors and subrecipients adopt and properly administer PRDOH's PII policies and procedures. Failure to effectively carry out these policies or any breach of information may cause PRDOH to terminate the contract or grant agreement. In addition, PRDOH requires that all CDBG State Program contractors and subrecipients maintain files and procedures regarding:

- Reference or background checks conducted prior to onboarding CDBG Program employees who will have access to sensitive data.
- Employee review and acknowledgement of the PRDOH's PII and acceptable use policies.
- Restricting access to CDBG State Program PII to a limited number of personnel.
- Identification of employees with an actual or perceived conflict of interest. Identified employees shall not be granted access to information or PII that is the source of the conflict of interest.
- Zero tolerance policy related to the release of any applicant provided information without written consent of the applicant and/or PRDOH.
- PII Training provided to CDBG Program personnel.
- Procedures in place for ensuring that CDBG Program personnel who leave the project or employment no longer have access to sensitive information

e.g., timely termination of passwords, and collection of keys and identification cards as part of the out-processing routine.

PRDOH will conduct an initial monitoring of all CDBG State Program contractors and subrecipients for compliance with these policies and procedures. In addition, PII security will be regularly monitored by PRDOH.

CDBG STATE PROGRAM PII TRAINING

The PRDOH will conduct PII training for all CDBG State Program personnel and contractor/subrecipient staff as necessary. In addition to PII training, PRDOH requires:

- All CDBG State Program employees, contractors, and subrecipient staff must read this policy and acknowledge understanding of this document.
- All CDBG State Program employees, contractors, and subrecipient staff must read and agree to PRDOH's acceptable use, wireless, and sanctions policies.
- Any suspicious activity shall be immediately reported to PRDOH Secretary's Office.

COMPROMISES OF PII SECURITY

All compromises or potential compromises of PII security shall immediately be reported to the PRDOH Secretary's Office in order to assess the situation and


determine the appropriate action to be taken. In addition, the following steps should be taken:

- Immediate investigation of the security incident and termination of any existing vulnerabilities or threats to personal information.
- Any compromised computer should be immediately disconnected from any CDBG State Program network.
- Suspension of access to physical or electronic information for any personnel suspected of creating a breach of PII security.

The Secretary will be responsible for notifying all appropriate entities, affected applicants, and law enforcement agencies, as applicable. In addition, the Secretary will be responsible for the termination of any contracts or grant agreements as determined necessary.

APPROVAL

This Policy will take effect immediately after its approval. This document supersedes any previously approved version.



William O. Rodríguez Rodríguez
Secretary

May 4, 2023
Fecha