CDBG-DR/MIT

Personally Identifiable Information, Confidentiality, and Non-disclosure Policy

DEPARTMENT OF HOUSING

GOVERNMENT OF PUERTO RICO

April 7, 2025

V.3

This page was intentionally left blank.

PUERTO RICO DEPARTMENT OF HOUSING

CDBG-DR/MIT PROGRAMS

PERSONALLY IDENTIFIABLE INFORMATION, CONFIDENTIALITY, AND NONDISCLOSURE POLICY

VERSION CONTROL

VERSION NUMBER	DATE REVISED	DESCRIPTION OF REVISIONS
1	**March 6, 2020**	**Original Version**
2	**September 17, 2020**	**Additions in various sections of the document to add information gathered from HUD OIG Report: HUD PII Records Protection and Management, 2019-OE-0002a from June 25, 2020, and other HUD references. These appear highlighted in grey color.**
3	**April 7, 2025**	**Edits throughout the document to incorporate references to the CDBG-MIT Program, reorganize content, update definitions in accordance with the Code of Federal Regulations, and integrate the Cybersecurity Act of the Commonwealth of Puerto Rico, Act No. 40-2024. Additionally, revisions have been made to procedures and regulations. All changes are highlighted in gray.**

Table of Contents

1 Introduction

The Puerto Rico Department of Housing (**PRDOH**), as grantee, is committed to the responsible management of the Community Development Block Grant - Disaster Recovery (**CDBG-DR**) and Community Development Block Grant – Mitigation (**CDBG-MIT**) funds. As part of this commitment, PRDOH prioritizes the protection of individual stakeholders' privacy. Through the administration of CDBG-DR/MIT programs, program personnel may encounter or have access to Personal Identifying Information (**PII**). To safeguard this information, appropriate measures must be implemented to ensure that documents containing PII are properly managed, securely stored, and protected against unauthorized access and inappropriate use.

2 Scope

The Personally Identifiable Information, Confidentiality, and Nondisclosure Policy (**PII Policy**) applies to PRDOH CDGB-DR/MIT Programs employees, staff, providers, vendors, suppliers, contractors, subcontractors, consultants, partners, applicants and subrecipients. This policy assures PII remains secure and is used in the appropriate manner for which it was intended.

3 Purpose

The purpose of this policy is to safeguard the right to confidentiality and ensure the protection of confidential and/or sensitive information throughout the process of PRDOH and CDBG-DR/MIT Program. By emphasizing strict adherence to confidentiality measures, this policy fosters trust and credibility within the PRDOH CDBG-DR/MIT Programs. Additionally, it serves to protect the PII information of participants, employees, subrecipients, and contractors from potential breach.

4 Definitions

Applicant: A person who has requested assistance from one of the CDBG-DR/MIT Programs.

Breach: For the purposes of this policy, the term is used to include the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users

and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.[1]

Confidentiality: Preserving authorized restrictions on access and disclosure, including protecting personal privacy and proprietary information.[2]

Contractor: A provider or supplier, as applicable, that produces goods and services for the public government agencies by means of a contract, subcontract, purchase order, agreement or other similar arrangement.

FEMA: Refers to the Federal Emergency Management Agency.

HUD: Refers to the United States Department of Housing and Urban Development.

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.

Nondisclosure: The act of not making something known.

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. Some PII is available in public sources such as telephone books, websites, and university listings. The definition of PII is not attached to any single category of information or technology. Instead, it requires a case-by-case assessment of the specific risk that an individual can be identified. Non PII can become PII whenever additional information is made publicly available, in any medium and from any source, that could be used to identify an individual when combined with other available information.[3]

PRDOH: Refers to the Puerto Rico Department of Housing.

Protected Personally Identifiable Information (Protected PII): For the purposes of this policy, Protected PII refers to PII that, when presented alongside Sensitive PII, requires

---

[1] OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, May 22, 2007, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/omb/memoranda/fy2007/m07-16.pdf.
[2] 44 U.S.C. § 3552.
[3] 2 C.F.R. § 200.1.

enhanced safeguards to protect an individual's privacy and prevent unauthorized access or disclosure.[4]

Sensitive Personally Identifiable Information (Sensitive PII): The personally identifiable information that when lost, compromised, or disclosed without authorization could substantially harm an individual. Examples of Sensitive PII include social security or driver's license numbers, medical records, and financial account numbers.[5] Sensitive PII can encompass standalone information or information paired with another identifier.

Subrecipient: An entity that receives a subaward from a pass-through entity to carry out part of a federal ward. The term does not include a beneficiary or participant.

5 Personally Identifiable Information

To implement the CDBG-DR/MIT Programs, PRDOH must to collect, maintain, use, retrieve and disseminate information related to individuals applying for assistance. Due to the nature of the programs, Applicant's records may include sensitive date such as 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 PII.

PII includes any 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. Due to the nature of personal information, the definition of PII is intentionally broad and not confined to specifics categories of information or technology.

---

[4] Previously, Protected PII under 2 C.F.R. Part 200 was defined as an individual's first name or initial and last name, when combined with sensitive information such as Social Security numbers, passport numbers, financial records, medical records, or biometric data. This definition acknowledged that combining such elements heightened the risk of harm if disclosed. Under the revised 2 C.F.R. 200.1, Protected PII is now defined as "PII except for PII that must be disclosed by law." However, to ensure clarity, this policy defines Protected PII as PII that, when presented alongside Sensitive PII, requires enhanced protection.

[5] HUD, Protecting PII Capacity Building Guidance on Protecting Privacy Information, April 2015, https://files.hudexchange.info/resources/documents/Housing-Counseling-Protecting-PII-Capacity-Building-Guidance-Protecting-Privacy-Information.pdf.

Given the broad scope of the definition of PII, context plays a critical role in determining the appropriate level of protective measures to be applied. However, when handling PII, it is prudent to adopt a cautious approach to ensure the highest level of protection.

5.1 Sensitive PII and Protected PII

Sensitive Personally Identifiable Information (**Sensitive PII**) refers to information that, if lost, compromised, or disclosed without authorization could substantially harm to an individual. Due to the heightened risk associated with its unauthorized access or exposure, Sensitive PII requires enhanced handling protocols and security measures.

Certain types of PII are inherently sensitive as standalone data elements, such as a Social Security number (**SSN**), driver's license, or state identification number. Additionally, other data elements—such as citizenship or immigration status, medical information, ethnic or religious affiliation, sexual orientation, or lifestyle details—become Sensitive PII when associated with an individual's identity, whether directly or indirectly inferred. When PII is combined with Sensitive PII, it must also be safeguarded accordingly, leading to its classification as Protected Personally Identifiable Information (**Protected PII**).

For the purposes of this policy, all safeguards and protective measures shall be applied comprehensively to both standalone Sensitive and Protected PII. This approach ensures a consistent and thorough level of protection, acknowledging the heightened risks associated with linked data. By enforcing these stringent safeguards, the policy aims to uphold the confidentiality, integrity, and security of such information.

5.2 Access and Management of Sensitive and Protected PII

According to the 2 C.F.R. §200.303(e), as part of internal control when managing Federal awards funds, all PRDOH staff, subrecipients, and contractors must "[t]ake reasonable measures to safeguard protected personally identifiable information and other information the Federal awarding agency or pass-through entity designated as sensitive or the non-Federal entity considers sensitive consistent with applicable Federal, state, local, and tribal laws regarding privacy and obligations of confidentiality".

In the implementation, management, and execution of CDBG-DR/MIT Programs, PRDOH personnel, subrecipients, contractors, and partner agencies will collect, use, process, store, disseminate, and access a significant amount of applicants' personal information. All individuals granted access to confidential applicant information are responsible for safeguarding passwords, equipment, case files, and communication channels.

To ensure compliance with these requirements, PRDOH has implemented safeguards, protective measures, and best practices to protect Sensitive and Protected PII obtained through the implementation, management, and execution of the CDBG-DR/MIT Programs.

5.2.1 Confidentiality and Non-disclosure

The right to privacy and control over Applicant's personal information is embedded in the Constitution of the Commonwealth of Puerto Rico.[6] As part of this constitutional protection, it is the State's responsibility to safeguard an individual's dignity, intimacy, and personal integrity.

Individuals authorized to access confidential applicant information must be instructed on the right to privacy and protection of personal information embedded in Art. 173 of the Puerto Rico Penal Code of 2012, 33 LPRA § 5239 *et seq*., which states that any person that disseminates, publishes, reveals, or gives away to a third party, data, communications, or images referred to in Art. 171[7] and Art. 172[8] of the Code, or who offers or requests such distribution or access, shall be subject to a fixed term of imprisonment of three (3) years. If the convicted person is a legal entity, they shall be subject to a fine of up to ten thousand dollars ($10,000).

---

[6] P.R. CONST. Art. II, § 8.

[7] Art. 171, 33 LPRA § 5237, refers to violations of personal communications; when somebody, without authorization and with the purpose of gaining knowledge for themselves or for others, takes any means of communication, or intercepts them, will be sanctioned. If the person is in possession of these documents as part of their work functions, they will not be considered as authorized to use the information for any other purpose other than strictly that of the mean for which it was intended to.

[8] Article 172, 33 LPRA § 5238, refers to changing or using personal data in files; any person who, without authorization, takes possession, utilizes, modifies or alters, in perjury of the information holder or a third party, information which is personal, filed in electronic or physical means, will be sanctioned.

PRDOH CDBG-DR/MIT subrecipients, contractors and subcontractors must abide by the confidentiality and non-disclosure clause in their contracts or subrecipient agreements. Additionally, employees of PRDOH, subrecipients, and contractors should only access confidential or sensitive information relevant to their assigned program, unless their position requires access to data across multiple programs.

All PRDOH and subrecipient employees, contractors, partner agencies, and other program personnel with access to confidential or sensitive information must sign a Confidentiality and Non-Disclosure Agreement. This agreement is part of the employee file along with an acknowledgment of receipt of this Policy.

Exceptions to the limitation on access to confidential or sensitive information applies when such access is required by monitoring or oversight agencies and their personnel, whether federal or local. However, personnel involved in monitoring or oversight who are granted access to files, documents, computers, and other devices containing Sensitive and Protected PII must adhere to the same stringent security and confidentiality standards as CDBG-DR/MIT Programs personnel. Any disclosed information must be strictly limited to the specific program or area under review. Access to such information must be closely supervised, and electronic access must include uniquely tailored roles and privileges, ensuring that all accessed data is tracked and recorded.

5.2.1.1 Cybersecurity Act of the Commonwealth of Puerto Rico

The Cybersecurity Act of the Commonwealth of Puerto Rico, Act No. 40-2024, 3 LPRA § 10121, establishes the public policy for the protection of government information and infrastructure, ensuring its confidentiality, integrity, and availability throughout its lifecycle—storage, transmission, and processing.

The Act applies to PRDOH, its employees, subrecipients, contractors, and any natural or legal person conducting business or entering into contracts with the government. PRDOH is committed to complying with the minimum cybersecurity standards and principles established by the Act, which include, but are not limited to:

- Establish control mechanisms to block inappropriate internet traffic and implement a security policy that restricts access to websites containing

malware, spyware, ransomware, phishing threats, and other identified threats, unless access is required for official duties;

- Establish multi-layered security controls to reinforce confidentiality, integrity, and authorization of information;
- Develop appropriate use policies for equipment and information systems and implement administrative and technical controls to regulate access to both internal and external networks;
- Adopt administrative controls requiring encryption based on National Institute of Standards and Technology (**NIST**) recommendations to enhance data confidentiality and integrity during storage and transmission. Establish technical mechanisms to enforce established policies;
- Ensure that remote connections to the government network are only through a Virtual Private Network (**VPN**) or any other private network program contracted exclusively by the government for official use when work-related tasks are necessary;
- Any software or application developed or used by PRDOH or its contracted providers to serve citizens or facilitate internal operations must comply with minimum security standards;
- Establish a data classification mechanism based on its criticality to the government and citizens. Following this classification, Multifactor Authentication (**MFA**) shall be implemented for all users;
- Contracts with service providers must include measures to protect sensitive assets and require compliance with the Federal Information Security Management Act of 2002 (**FISMA**), 44 U.S.C. § 3541, *et seq*;
- Contracted information and communications technology service providers shall share information and notify the Puerto Rico Innovation and Technology Service (**PRITS**) and PRDOH within no more than forty-eight (48) hours upon discovering a cybersecurity incident or a potential incident that could compromise government data, software products, firmware, or confidential services of the government or any natural or legal person.
- Government Information Technology (**IT**) systems must only be used for authorized purposes, with role-based access;

- Information processing facilities and assets must be housed in secure, unmarked areas, protected with an appropriate security perimeter and controls to prevent unauthorized access and damage. Additionally, they must be equipped with a backup power generator to prevent failures in the event of electrical service issues, as part of a contingency protocol;
- Confidential information, including PII, shall not be exposed or unprotected under any circumstances. It must be encrypted in all states (i.e., in transit and at rest);
- Establish and maintain a cybersecurity education program for personnel and service providers;
- Develop and integrate data backup and recovery plans to ensure operational continuity, considering both locally maintained systems and cloud-based systems managed by suppliers or third parties;
- Compliance with any additional cybersecurity standards published by the Puerto Rico Innovation and Technology Service (**PRITS**).

5.2.2 Termination and Information Access

The off-boarding process must involve the Human Resources division, Operations, IT, and any other relevant area to which the employee has access to files, drives, applications, or any other information handling method.

During this process, the relevant areas will work together to identify the information, disks, or applications the employee had access to, in order to deactivate all assigned credentials and access privileges. It is the responsibility of the employee's supervisor or department head to notify the IT area and formally request the removal of all access rights. Additionally, if the device assigned to the employee or their mobile phone contains applications that synchronize data from emails, contacts, calendars, and/or remote storage drives, all of these shall be reviewed and deactivated immediately.

The off-boarding process must ensure the following actions are taken:

- Reinforce the importance of maintaining confidentiality;
- Retrieve any remaining information in the employee's possession;

- Recover all off-site devices belonging to PRDOH, such as tablets and laptops; and
- Collect keys, ID badges, and any other access device.

5.2.3 Written Consent and Communication Designee

The use of information will be limited to ensuring compliance with program requirements, HUD and federal 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 PRDOH CDGB-DR/MIT Programs participant, employee, or contractor. The Consent form must disclose the details to be shared and be signed and dated by the affected party.

Certain CDBG-DR/MIT 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. The Communication Designee serves as a point of contact for the Applicant and is not a Power of Attorney. They are authorized to receive and provide information to the Program on behalf of the applicant; however, they are not permitted to sign any documents or enter into agreements unless they have been granted Power of Attorney.

5.2.4 PII Collection

The collection of Sensitive and Protected PII should be strictly limited to what is necessary for the effective implementation and management of the CDBG-DR/MIT Programs and should not be collected or maintained without the proper authorization. When the PII is used to determine an Applicant's rights, benefits or privileges such information must be collected directly from the individual, whenever possible.

Puerto Rican law regulates the protection and collection of Social Security numbers by government entities, including agencies, branches, municipalities, public corporations, and their contractors, within established parameters authorized by federal law.

Act No. 187-2006, as amended, 18 LPRA § 926(f), known as the Parameters of the Use of Social Security Number of Entities that Provide Services to the Government Act, mandates that private entities contracting with the government must ensure that citizens' Social Security numbers are not transmitted, displayed, or disclosed in publicly accessible or visible documents to unauthorized individuals.

The Prohibition of the Use of Social Security Number in the Employee's Identification Device or in Any Document of General or Routine Circulation Act, Act No. 207-2006, 29 LPRA § 621a, prohibits employers—whether private or public corporations of the Commonwealth of Puerto Rico—from displaying an employee's Social Security number on identification cards or in any publicly visible location or widely circulated document. Employees may waive these protections voluntarily and in writing; but such a waiver cannot be imposed as a condition of employment.[9] If a document containing a worker's Social Security Number must be made public for a purpose that does not require it, the number shall be redacted—partially or completely—to ensure it is illegible.

The Public Policy for the Use of the Social Security Number as Identification Verification and the Protection of its Confidentiality Act, Act No. 243-2006, as amended, 29 LPRA § 621(b), authorizes government entities— including agencies, departments, instrumentalities of the Commonwealth, the Executive, Legislative, and Judicial Branches, municipalities, public corporations, and their contractors— to collect Social Security numbers for official transactions. These numbers may be used to verify identity, cross-reference internal records, and facilitate information exchange. However, any entity requesting a citizen's Social Security number must disclose the legal authority for the request, the intended purpose, and whether providing the number is mandatory or voluntary.

[9] Exemptions to Act No. 27-2006 apply when the use of a Social Security number is legally required, authorized, or regulated by federal laws or regulations. The Act also does not apply when the number is used for identity verification, tax contributions, contracting, or payroll purposes, provided the employer implements appropriate security measures to protect its confidentiality.

5.2.5 Information Sharing Access Agreements

As part of disaster recovery and mitigation efforts, PRDOH works along with federal and local agencies, partners, and subrecipients to share information, which includes Sensitive and Protected PII. In order to establish clear directives, PRDOH has data and information sharing agreements, also known as, Information Sharing Access Agreements (**ISAA**). These ISAA establish the parties' responsibilities in protecting, handling and sharing PII.

As part of said efforts, PRDOH engaged in an ISAA with the Federal Emergency Management Agency (**FEMA**). Through an amendment to the original ISAA[10], FEMA allowed PRDOH to share PII with its contractors. This agreement, as well as other information sharing agreements may suffer from amendments from time to time, as well as time extensions for its validity. According to the DHS/FEMA 008 – Disaster Recovery Assistance Files System of Records[11], this system allows the Department of Homeland Security (**DHS**) and FEMA to collect and maintain records on applicants for its Disaster Assistance programs that provide financial and other tangible assistance to survivors of Presidentially-declared disasters.

These ISAA should include, at a minimum, the following clauses:

- PII should be shared and transmitted in a safe manner that minimizes the probability of a breach.
- Login credentials clauses (username and passwords).
- User instructions, manuals and proper handling and protections of PII.
- Login credentials must not be shared among unauthorized staff or CDBG-DR/MIT employees.
- Parties shall ensure the accuracy of the information.
- PII should only be used to administer Program objectives.

---

[10] The original Information Sharing Access Agreement between the Department of Homeland Security Federal Emergency Management Agency and Puerto Rico Department of Housing for Hurricane Irma, FEMA-4336-DR, and Hurricane María, FEMA-4339-DR was signed on November 2017. The second amendment to this agreement was signed on May 2019.

[11] DHS/FEMA 008 – Disaster Recovery Assistance Files System of Records, 78 FR 25283 (Apr. 30, 2013). Document can be accessed at: 2013-10173.pdf (govinfo.gov)

- Those who handle or have access to PII shall be instructed of the confidential nature and legal consequences that may arise for mishandling the information.
- Technical, physical, and administrative safeguards to secure PII.
- Compliance with requirements and regulations contained in 2 C.F.R. part 200.
- Ensure cloud-based systems to meet or exceed the baseline privacy and security controls applicable to the Federal Government Systems.
- These systems should be constantly monitored to ensure they run in their latest updated version.
- Limit access to PII to personnel who administer assistance.
- Prohibit PII disclosure to third parties without written consent.
- Ensure personnel with access to PII shall complete privacy and security trainings and understands PII protection.
- Notice of Security Incident – to be notified **immediately** in case of actual data security incident.
- Extension of clauses and its enforcement to any contractors to access to PII.

It is essential to note that this data is protected under the Privacy Act of 1974, 5 U.S.C. § 552a, *et seq*. While the Privacy Act does not apply to Puerto Rico or its agencies, PRDOH, as a grantee of HUD, must comply with its requirements for managing and protecting data received from federal sources. As such, PRDOH is responsible for managing access to this data and must:

- Request the data only when necessary, based on specific program requirements outlined in the approved Action Plan;
- Limit access to Authorized Users who must adhere to the data use requirements specified in the ISAA, acknowledge their responsibilities under the Privacy Act and FISMA, and be informed of the civil and criminal penalties for noncompliance;
- Ensure Authorized Users receive training to uphold proper information security and privacy protections in accordance with the ISAA, the Privacy Act, and FISMA.
- Conduct breach and risk assessments to determine if HUD notification or remediation actions for affected individuals are required;

- Encrypt and securely store applicant PII, whether in physical or electronic form, in a manner that prevents unauthorized access or use.

Furthermore, PRDOH will retain FEMA data received only for the necessary processing period, typically until grant closeout. Any FEMA data obtained but not used must be deleted after application processing is complete.[12]

5.2.6 Methods of Transmission

At times, it may be necessary transmitting PII to authorized individuals, agencies, or Program staff. However, such transmissions should occur only when absolutely essential, with strict precautions to ensure data security. All CDBG-DR/MIT Programs providers, vendors, suppliers, contractors, subcontractors, consultants, partners, and subrecipients must redact or omit any non-essential confidential information or PII from invoices and documentation sent via email. If transmitting Sensitive PII or Protected PII is necessary, it must be sent through secure web applications or encrypted before being emailed.

Measures should be taken if the information is faxed; the fax number should be confirmed; the intended recipient will be waiting for the fax and no unauthorized person will intercept it. Sender shall ensure that none of the transmission is stored in memory on the fax machine, that the fax is located in a controlled area, and all paper waste is disposed of properly. When faxing Sensitive and Protected PII, only controlled fax machines shall be used, not central receiving centers.[13]

Sensitive and Protected PII in physical documents must not be left unattended on desks, printers, or in any areas accessible to unauthorized personnel. Additionally, personnel must ensure that their computers are never left unattended in a manner that could allow unauthorized access to such information.

Other measures should be taken as specified in this Policy to treat the information as confidential and to protect the transmission of PII:

---

[12] HUD, Overview of Computer Matching Agreements and Data Sharing Agreements for CDBG-DR and CDBG-MIT Grantees, https://www.hud.gov/sites/dfiles/CPD/documents/CDBG-DR/CMA-and-DSA-Overview-for-Grantees.pdf.
[13] See https://www.hud.gov/sites/documents/OHC_PII081214.PDF.

- Discussions of Sensitive and Protected PII over the phone should be done only after confirming the person is authorized to do so and is informed that the discussion will include such type of information.
- Sensitive and Protected PII shall not be included in voice messages on any communications mean.
- Sensitive and Protected PII should not be discussed in public or shared spaces where unauthorized persons can overhear.
- Meetings where Sensitive and Protected PII will be discussed should be held in secure spaces. Minutes on these notes should be treated as confidential when they contain such PII.[14] Additionally, records of the date, time, place, subject, chairperson, and attendees shall be maintained.[15]
- Records containing individual's Sensitive PII shall not be removed from facilities where the information is authorized to be stored and used, unless approval is first obtained from a supervisor.[16]
- Interoffice or translucent envelopes shall not be used to mail Sensitive and Protected PII. Instead, sealable opaque envelopes should be used.
- When using the U.S. Postal Service to deliver Sensitive and Protected PII, documents shall be double-wrapped (using two envelopes, one inside the other) and mark only the inside envelope as confidential with the statement - *To Be Opened by Addressee Only)*.

5.2.7 Public Access to Records

As required by federal and state laws, public information contained, stored, or generated in government entities must be available for public inspection, upon request. As provided in 24 C.F.R. § 570.508, PRDOH must provide citizens with reasonable access to records regarding the past use of CDBG funds, in accordance with applicable State and local laws regarding privacy and confidentiality. For more information on records accessibility by the public and the complete public information request process, refer to the Record Keeping, Management, and Accessibility Policy,

---

[14] HUD, Protecting PII Capacity Building Guidance on Protecting Privacy Information, April 2015, https://www.hud.gov/sites/documents/OHC_PII042815.PDF.
[15] See https://www.hud.gov/sites/documents/OHC_PII081214.PDF.
[16] Id.

available in English and Spanish at https://recuperacion.pr.gov/en/resources/policies/general-policies/ and https://recuperacion.pr.gov/en/resources/policies/general-policies/.

Act No. 141-2019, Transparency and Expedited Procedure for Public Information Access Act, 3 LPRA § 9911, as amended, establishes the public policy of the Government of Puerto Rico affirming that government-produced information and documentation are presumed to be public and equally accessible to all individuals. Any request for information, or a decision to deny its disclosure, must be justified in writing, citing the legal grounds for the refusal within **ten (10) business days**.

However, the right to access public information is subject to specific limitations. The Government of Puerto Rico Open Data Act, Act No. 122-2019, 3 LPRA § 9891, establishes the framework for the effective management of government data. Under Section 4, 3 LPRA § 9894, government entities may invoke claims of confidentiality or privilege to protect and withhold certain data, provided such claims meet one or more of the following criteria:

(a) The information is protected by law;
(b) The data is covered by evidentiary privileges available to citizens;
(c) Disclosure would infringe on the fundamental rights of third parties;
(d) The information reveals the identity of a confidential informant; or
(e) The information is classified as "official information" under Rule 514 of the Puerto Rico Rules of Evidence.

Accordingly, when responding to Requests for Information (**RFI**), any Sensitive and Protected PII must be redacted. In cases where any of the aforementioned exemptions apply, such as when the requested information is legally protected, falls under evidentiary privileges, or its disclosure could infringe on the fundamental rights of third parties, the request must be denied. Additionally, any denial of access to information must be accompanied by a written justification specifying the legal grounds for the refusal.

5.2.8 Disposing of PII

Records containing PII should not be kept longer than required. Once the recordkeeping time frames are met, these records should be destroyed. An appropriate disposure of Sensitive and Protected PII is accomplished by **permanently** disposing of electronic records and/or hard copy records.[17]

PRDOH requires CDBG-DR/MIT personnel, contractors, and subrecipients to properly dispose Sensitive and Protected PII in accordance with recordkeeping timelines, so that they cannot be read or reconstructed. Acceptable methods of disposal include paper shredding, burning or pulverizing, and physical destruction of media or permanent removal of PII data from storage devices. Disposal of computers and portable storage devices must include the use of software that securely erases data and hard drives in a way that files are no longer recoverable.

6 PII Breach

The Office of Management and Budget (**OMB**) defines an incident as "an occurrence that (1) actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information or an information system; or (2) constitutes a violation or imminent threat of violation of law, security policies, security procedures, or acceptable use policies".[18] It also defines a breach as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar term referring to situations where persons other than authorized users and for an other than authorized purpose have access or potential access to personally identifiable information, whether physical or electronic.[19]

Examples of incidents that may lead to breaches of PII are:

- Loss, damage, theft, or improper disposal of files, documents, equipment that contain PII;

---

[17] Id.
[18] OMB Memorandum No. 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 3, 2017, https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-12_0.pdf.
[19] *Id.*

- Accidentally or purposely sending files, documents, reports that contain PII to a person without authorization to view, handle or manage this information;
- Sending files or documents that contain PII without the proper protection (encryption);
- Allowing unauthorized people to use a computer that contains files and documents with PII;
- Discussing PII in a public area; and
- Any security break-in scenario that could compromise PII (computer virus, phishing, etc.).

6.1 Preventing a PII Breach

To ensure the protection of PII and compliance with this Policy, all employees, contractors, and subrecipients of the CDBG-DR/MIT Program who have access to PII or systems used to collect, manage, transmit, or dispose of PII must receive adequate training. This training shall equip them with the necessary knowledge to handle and protect PII effectively, as well as to identify and respond to security incidents.

Trainings shall emphasize the principles and requirements outlined in this Policy and any related guiding documents, including but not limited to:

- The importance of protecting an individual's confidentiality;
- Identifying information that requires protection;
- Safeguarding data and files;
- Proper storage of information;
- Preventing improper or unintentional data sharing; and
- Responding to potential security threats.

6.2 Reporting a PII Breach

All CDBG-DR/MIT Programs employees are required to immediately report any suspected or confirmed PII incident, breach, or potential threat, regardless of the medium or form, to their supervisor. Employees must report the incident without delay and should not wait for confirmation that a breach has occurred before notifying their supervisor. The supervisor, in turn, must escalate the incident to the CDBG-DR/MIT Program Office of Policy Development, Risk Management, and Compliance (**PDRMC**).

Additionally, IT service providers, as well as any other vendor, supplier, contractor, subcontractor, consultant, partner, or subrecipient who manage CDBG-DR/MIT Programs data, must report any cybersecurity breach, incidents or potential threats to the PRDOH CDBG-DR/MIT Program Office of Policy Development, Risk Management and Compliance and to the Subrecipient Management Unit.

The incident report, along with the description of the incident, should encompass the who, what, when and how:

Who	Who was responsible for the incident? Who is harmed by the incident?
What	What is the information compromised? What is the impact of that information being compromised?
When	When did the incident occur? When was it detected? When was it reported?
How	How was the information accessed? How was the incident detected?

Failure to promptly report an incident may significantly hinder the ability to mitigate the breach, implement remedial measures, and protect PII from potential harm. Records and documentation of the information and actions relevant to the incident must be kept.

6.3 Evaluation of a PII Breach

When evaluating the type and severity of a breach, PRDOH shall consider intent and recipient. When analyzing intent in a PII breach, this refers to whether the information was compromised intentionally, unintentionally or if the intent is unknown. PRDOH will also evaluate if the recipient of disclosed PII is known, unknown, as well as the trustworthiness of that recipient, if it is a known recipient.[20] This evaluation will provide a frame of reference of the risk associated with the potential or confirmed PII breach.

Privacy incidents can be classified as low, moderate or high according to the severity of the incident. Factors that are considered for this evaluation are: the sensitivity of the

[20] *Id.*

PII involved; number of individuals affected; and the harm that may result or has resulted from the incident.

Low-level Impact	An incident involving the unauthorized or unethical disclosure, use, or disposal of a limited amount of Sensitive and Protected PII. The impact is minimal, with only a small number of individuals affected and minor potential harm resulting from the incident.
Moderate-level Impact	An incident involving the unauthorized or unethical disclosure, use, or disposal of Sensitive and Protected PII that could cause a significant adverse effect. This level of incident may impact a substantial number of individuals and result in considerable harm.
High-level Impact	An incident involving the unauthorized or unethical disclosure, use, or disposal of Sensitive and Protected PII that results in a serious adverse effect. This level of impact includes the exposure of a significantly large amount of data and may cause severe harm to individuals.

Despite these classification parameters, each incident will be assessed on a case-by-case basis to ensure a thorough and comprehensive evaluation. This assessment will consider all relevant factors, including the nature and scope of the incident, accessibility and sensitivity of the data involved, the potential or actual harm caused, and whether any mitigation measures were implemented to reduce the risk and impact of the breach.

Additionally, as part of the assessment, PRDOH will determine whether the involvement of the CDBG-DR/MIT IT Department is necessary to fully assess the scope, cause, and potential consequences of the breach. PRDOH will also evaluate whether the severity and scale of the incident warrant formal notification to HUD. All high-impact incidents, due to their significant risk and potential harm, will be reported to HUD.

6.4 Mitigating the Risk of a PII Breach

PRDOH and its vendors, suppliers, contractors, subcontractors, consultants, partners, or subrecipients who manage CDBG-DR/MIT Programs data must be prepared to act promptly when a PII breach occurs in order to reduce the potential harm that the

affected individuals may confront. Once a full evaluation and risk assessment has been performed, the following step is to apply the adequate measures to mitigate the possible harm to individuals that the potential or confirmed PII breach may cause. Because each PII breach is fact specific, the actions required to mitigate potential harm will be on a case-by-case basis. When considering the need to mitigate any damages the following factors should be considered:

- Damage occurred, if any;
- Nature of the damage;
- Amount of gravity of damages;
- Type of data disclosed;
- Reason for the disclosure; and
- If in fact the harm can be mitigated.

Actions of mitigation may include countermeasures, guidance and/or services to address the breach and minimize potential harm:

- **Countermeasures** should be put in place immediately and may include containing the incident, restoring affected systems, and notifying impacted individuals. The selection of appropriate countermeasures must consider both the immediate objective of minimizing harm to affected individuals and the long-term goal of preventing similar incidents in the future.[21] A comprehensive approach to mitigation ensures both an effective response to the immediate breach and the implementation of proactive measures to enhance future PII security.
- **Guidance** should be provided to affected individuals, offering clear instructions on how they can obtain more information about the breach, as well as
- **Services,** such as identity recovery, credit monitoring, fraud alerts, or legal assistance. However, since these services may not always be available or may not fully address the specific risks of a given incident, individuals should be provided with clear information, relevant resources, and guidance on

[21] HUD Privacy Office, HUD Breach Notification Response Plan Rev. 1.0, p. 42, October 10, 2021, https://www.hud.gov/sites/dfiles/OCHCO/documents/3150.1cioh.pdf.

alternative measures they can take to safeguard their data and mitigate potential harm.

6.5 Notification of PII Breach

Affected parties of a PII breach should be notified **forty-five (45) days** after the breach has been detected and impacted individuals have been identified. The notification should provide clear and comprehensive information about the breach, including:

- The date or estimated timeframe of the incident;
- The types of PII involved;
- The countermeasures and/or services implemented to mitigate harm;
- The actions individuals should take to further protect themselves; and
- Guidance with clear instructions on how affected individuals can obtain more information about the breach, including a designated point of contact for further inquiries and their contact details.
- Recommended actions they may take to further protect themselves.

Contractors, subcontractors, consultants or subrecipients responsible for issuing breach notifications must certify to PRDOH that the required notifications have been made in accordance with this Policy. This certification should include documentation confirming the date, method, and recipients of the notification, as well as a summary of the information provided. PRDOH reserves the right to request additional details to ensure compliance with notification requirements and to uphold its commitment to transparency and PII protection.

6.5.1 Data Bank Security Breach and Notification to Citizens

The Citizen Information on Data Banks Security Act, Act No. 111-2005, as amended, 10 LPRA § 4051, *et seq.*, states that any entity[22] who owns or has under its custody a data

[22] For purposes of this law, the definition of entity includes agencies and any government instrumentality or organism from any of the three branches of government as well as any corporation or private organization authorized to do business or operate in Puerto Rico. 10 LPRA § 4051(d).

bank that includes personal information[23] of Puerto Rican resident citizens shall notify said citizens of any security breach of their system, when the data banks that suffered the breach contained personal information that wasn't safeguarded by password protected encryption. The notification of this breach will be sent in a clear and conspicuous manner and it must describe the security violation in general terms and the information that was involved. This notification will include a telephone number or website information where people can reach out to for further information or assistance. Written notification will be sent out to all potential affected parties via regular mail or email authenticated following the Electronic Transactions Act of Puerto Rico, Act No. 148-2006, as amended, 10 LPRA § 4081. If the cost of notifying or identifying all affected parties results too onerous, or if the cost exceeds one hundred thousand dollars ($100,000) or the affected parties are over one hundred thousand (100,000), the notification shall be done:

1. By publishing an announcement of the breach at the place of business of the entity, on its webpage (if it has one), and on any informative newsletter or bulletin that it publishes and sends through its mail list (post or electronic); and,
2. By issuing a communication of the breach to the press that shall inform of the situation and provide information on how to communicate with that entity for follow up. If the information where to be relevant to a specific sector (commercial or professional), the communication can be issued through the publication of major circulation oriented towards that sector.[24]

6.6 Requirements for Contractors, Subrecipients, and other Partners

PRDOH requires that all CDBG-DR/MIT Programs partners, subrecipients, consultants, contractors, and their personnel meet or exceed the standards set forth by this Policy, and ensure that the contractors or subrecipients adopt and properly administer this Policy. As such, CDBG-DR/MIT Programs contracts and subrecipient agreements

[23] For purposes of this law, the definition of personal information includes the name or first initial and surname, together with any of the following: Social Security number, driver's license, electoral card or any other official identification number, bank account numbers or any other type of financial information, username and password for information systems access, medical information protected by HIPAA, tax information, and work evaluations. 10 LPRA § 4051(d).
[24] Art. 4, 10 LPRA § 4053.

include provisions to safeguard confidential and sensitive information, prohibiting its use, sale, marketing, or disclosure to third parties without the PRDOH's written consent.

Contractors, subrecipients, and partners must ensure that their PII policies incorporate comprehensive training, effective management practices, and robust breach response protocols. They must also maintain adequate systems with the capability to track and monitor access to Sensitive and Protected PII, ensuring the security of such information. Furthermore, they shall facilitate inspections or investigations to verify compliance with this Policy.

These measures enable PRDOH to respond promptly and effectively to any potential or actual PII breaches. As part of breach response protocols, contractors, subrecipients, and partners shall collaborate with PRDOH by exchanging relevant information to accurately report and manage breaches. Throughout this information exchange, they must adhere to industry best practices for safety and security.

Failure to comply with this Policy may result in disciplinary action by PRDOH and the imposition of sanctions and/or additional conditions by HUD, as outlined in 2 C.F.R. § 200.338.

7 Recommended Best Practices for Safely Handling PII

PRDOH personnel, subrecipients, contractors, subcontractors, and other partners along with their staff must protect information entrusted to them by program applicants. In its management and handling of PII, there are several strategies and activities that should be implemented. This section, which is not an exhaustive list, includes suggested best practices.

7.1 General practices

- Limiting the collection, access, use, and disclosure of personal information to legitimate job functions or reasons allowed by law;
- Safeguarding personal information when in the person's possession;
- Collecting only the PII that is needed for the purposes for which it is collected;
- Keeping accurate records of where PII is stored, used, and maintained in hard copy and electronic files;

- Periodically auditing all Sensitive PII holdings to make sure that all such information can be readily located;[25]
- Following proper disposal methods of documents that contain PII; and
- Immediately reporting suspected or confirmed acts or incidents of privacy violations.

7.2 User ID's and passwords

- User ID's and passwords are for individual use and shall not be shared.
- This information is considered private and confidential and must be treated as such.
- Passwords must be construed as strong passwords containing a minimum of eight (8) characters, with a combination of upper and lowercase letters, numbers and special characters.
- Not to be easily guessed.
- Passwords should be changed at regular intervals as determined by the Information Technology Security Policy.
- Neither should be allowed to be included in automated login process or saved by the browsers.

7.3 Hard Copy and Electronic Files

- PII inventories shall be maintained with identifying lists of (1) paper records; (2) electronic records; (3) new records, that contain PII.[26]
- A procedure to monitor and track when PII is copied to another authorized or unauthorized location, such as a network share or removable media, should be developed to detect and track movement of PII.[27]
- Record files shall not be removed from the office without prior consent, even in teleworking circumstances.[28]
- Consent for file removal shall be given, in writing, by the employee/contractor's supervisor.

---

[25] See https://www.hud.gov/sites/documents/OHC_PII081214.PDF.

[26] Memorandum, HUD OIG Report: HUD PII Records protection and Management, 2019-OE-0002a, June 25, 2020, *https://www.hudoig.gov/sites/default/files/2020-06/2019-OE-0002a.pdf*.

[27] *Id.*

[28] *Id.*

- Files containing Sensitive PII, documents and removal media, should be clearly labeled (i.e. For Official Use Only, Confidential).
- Hard copy files shall be kept in file cabinets.
- Sensitive PII shall be stored only on workstations located in areas that have restricted physical access.
- File cabinets shall be locked when not in use. Only authorized employees or contractors shall have copy of the cabinet's keys.
- The protection of electronic files may include encryption, implementing enhanced authentication, and limiting the number of people allowed access to the files.
- Files or documents that leave the office must be secured and assigned to a specific designee. There must be a written record of who is in physical or electronic control of the files and documents.
- Inactive files shall have the proper record retention policy.
- Shred any duplicate documents that contain confidential or sensitive information.

7.4 Computers

- Proper barriers and controls must be put in place between unauthorized personnel and documents or computer screens containing confidential or sensitive information.
- Computer screens should be positioned in such manner that unauthorized personnel cannot have access nor read the screen.
- Information stored in computers must use a secure system.
- Confidential or sensitive information should not be emailed to anyone outside of your work facility.
- Do not leave computer unattended without locking or logging out.

7.5 Virus Protection

- Virus protection is compulsory for all equipment, workstations, servers that are used to handle PII.
- It is crucial that the antivirus software in every computer is maintained updated.

7.6 PII Breaches

- Any real or potential PII breach or violation of this Policy must be notified immediately by the employee or contractor to their supervisor at PRDOH or GM office.
- Reporting, evaluation, mitigating and notifying PII Breaches as set forth in this Policy and any other guidance document developed.
- Actions include but are not limited to risk assessment, establishing a response team, identifying the cause, identifying mitigating actions, follow-up steps to prevent future incidents.

8 Approval

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

END OF POLICY.