



CDBG-DR

Personally Identifiable Information, Confidentiality, and Non-disclosure Policy (PII Policy)

This page was intentionally left blank.

PUERTO RICO DEPARTMENT OF HOUSING
CDBG-DR PROGRAM
**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.

Table of Contents

1	Introduction.....	4
2	Scope.....	4
3	Purpose.....	4
4	Definitions.....	4
5	Personally Identifiable Information (PII).....	5
5.1	Types of PII.....	6
5.2	Access and Management of PII.....	8
6	PII Breach.....	16
6.1	Preventing a PII Breach.....	17
6.2	Reporting a PII Breach.....	17
6.3	Evaluation of a PII Breach.....	17
6.4	Mitigating the Risk of a PII Breach.....	19
6.5	Notification of PII Breach.....	19
6.6	Requirements for Contractors, Subrecipients, and other Partners.....	20
7	Recommended Best Practices for Safely Handling PII.....	20
7.1	General practices.....	21
7.2	User ID's and passwords.....	21
7.3	Hard Copy and Electronic Files.....	21
7.4	Computers.....	22
7.5	Virus Protection.....	22
7.6	PII Breaches.....	22
8	Approval.....	23

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**) funds. In doing so, PRDOH is dedicated to protecting the privacy of individual stakeholders. Through CDBG-DR program processes, program personnel are often exposed or given access to **Personal Identifying Information (PII)**. As a result, the proper measures must be taken to ensure documents that include **PII** are properly managed and secured from unauthorized access and inappropriate use.

2 Scope

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

3 Purpose

The purpose of this policy is to protect the right to confidentiality and the protection of confidential and/or sensitive information throughout PRDOH and CDBG-DR program processes. By establishing the importance of a strict adherence to confidentiality measures, trust and credibility are founded in PRDOH CDBG-DR programs. This policy will also help to safeguard PRDOH CDBG-DR program participants', employees', subrecipients', and contractors' confidential and/or sensitive information from any potential breach.

4 Definitions

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

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.

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.

Confidentiality: The protection of personal and/or sensitive information.

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.

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. 2 C.F.R. § 200.79. Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc., alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.¹

PRDOH: Refers to the Puerto Rico Department of Housing.

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 C.F.R. § 200.82.

Public PII: Public PII is defined as personally identifiable information that is available in public sources such as telephone books, public Web sites, and university listings. 2 C.F.R. § 200.79.

Sensitive PII: The personally identifiable information that when lost, compromised or disclosed without authorization could substantially harm an individual.² Sensitive PII can encompass standalone information or information paired with another identifier.

Subrecipient: A public or private nonprofit agency, authority or organization, or community-based development organization receiving CDBG-DR funds from the recipient or another subrecipient to undertake CDBG-DR eligible activities. 24 C.F.R. § 570.500(c). 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.

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.³

5 Personally Identifiable Information (PII)

Special measures designed to assist the efforts of disaster affected States are necessary to expedite the rendering of aid, assistance and emergency services; as well as the reconstruction and rehabilitation of devastated areas. By providing Federal assistance programs for both public and private losses, local government can carry out their responsibilities to alleviate the suffering and damage resulted from disaster. 42 U.S.C. § 5121(b)(6).

¹ OMB Memorandum 07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information, <https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2007/m07-16.pdf>

² Protecting PII Capacity Building Guidance on Protecting Privacy Information, U.S. Department of Housing and Urban Development, April 2015, https://www.hud.gov/sites/documents/OHC_PII042815.PDF

³ 5 U.S.C. § 552 (a) (5). Also, see https://www.hud.gov/sites/documents/OHC_PII081214.PDF

In order to implement these Federal assistance programs, PRDOH, as CDBG-DR funds grantee, needs to collect, maintain, use, retrieve and disseminate information related to those individuals who apply for CDBG-DR funded assistance. Due to the nature of the programs, 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. Due to the nature of personal information, the definition of PII is necessarily broad and not anchored to any single category of information or technology. Rather, it requires a case-by-case analysis of the specific risk that an individual can be identified through certain information.⁴ For instance, Non-PII can become PII when, together with additional information that has been publicly available (medium or source notwithstanding), could be used to identify an individual. 2 C.F.R. § 200.79. PII is a form of Sensitive Information, which includes, but is not limited to, PII and Sensitive PII.⁵

PRDOH and CDBG-DR program employees and staff, as well as subrecipients, contractors and partner agencies, that handle PII should exercise special care. Due to the broad nature of the PII definition, context is very important when determining the extent of the protective measures applied. However, when handling PII, it is safer to err on the side of caution.

5.1 Types of PII

5.1.1 Public PII

Public PII is defined as personally identifiable information that is available in public sources such as telephone books, public Web sites, and university listings. 2 C.F.R. § 200.79. Examples of Public PII:

- First and last name;
- Address;
- Work telephone number;
- Email address;
- Home telephone number;
- Driver's license; and
- General educational credentials.

⁴ OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, January 2, 2017, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

⁵ Sensitive information is any information, which if lost, misused, disclosed, or, without authorization is accessed, or modified, could adversely affect the national or homeland security or interest, the conduct of federal programs, or the privacy of individuals, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense, homeland security or foreign policy. DHS Sensitive Systems Policy Directive 4300A, version 13.1, July 27, 2017.

As a general rule, Public PII is not subject to the rigorous protective measures applicable to protected and Sensitive PII because they are not considered sufficiently sensitive to require protection. Nevertheless, the determination that certain PII is not sensitive does not mean it is publicly releasable.

5.1.2 Sensitive and Protected PII

Sensitive PII is the personally identifiable information that when lost, compromised, or disclosed without authorization could *substantially harm* an individual.⁶ Sensitive PII can encompass standalone information or information paired with another identifier.

Examples of standalone Sensitive PII are:

- Social Security numbers or comparable identification numbers (i.e., passport number, driver's license ID number, alien registration number, etc.);
- Financial information associated with individuals; and
- Medical information associated with individuals.

Examples of information that, when paired with another identifier, becomes Sensitive PII:

- Citizenship or immigration status;
- Medical information;
- Ethnic or religious affiliation;
- Sexual orientation;
- Account passwords;
- Last four (4) digits of Social Security number;
- Date of birth;
- Criminal history; and
- Mother's maiden name.

Sensitive PII, as a subset of PII requires additional levels of security controls. It requires stricter security handling procedures as it possesses an increased risk to an individual if that information is inappropriately accessed or compromised.

As part of the United States Department of Housing and Urban Development's (**HUD**) program requirements, in compliance with the Federal Privacy Act, 5 U.S.C. § 552a (Federal Privacy Act), the collection, maintenance, use, and dissemination of Social Security numbers, Employer Identification numbers, any information derived of the former, and income information shall be conducted, to the extent applicable, with the Federal Privacy Act and all other provisions of Federal, State, and local law. 24 C.F.R. § 5.212.

The Federal Privacy Act requires agencies to collect and maintain only such information about an individual that is relevant and necessary to accomplish its purpose, required to

⁶ Protecting PII Capacity Building Guidance on Protecting Privacy Information, U.S. Department of Housing and Urban Development, April 2015, https://www.hud.gov/sites/documents/OHC_PII042815.PDF

be accomplished by statute or by Executive Order of the President.⁷ The Federal Privacy Act also requires that the information be maintained in systems of records, electronic and paper, that have the appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of the information.⁸

Agencies are required to protect this information from any anticipated threats or hazards to their security or integrity, which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom the information is maintained, and must not disclose this information except under certain circumstances.⁹

As defined in this Policy, Protected PII refers to an individual's first name or first initial and last name when combined 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 and financial records or educational transcripts. Protected PII does not include information that is required by law to be disclosed. 2 C.F.R. § 200.82. As the definition states, Protected PII is encompassed in the definition of Sensitive PII when information that is not normally sensitive is combined with another, thus becoming Sensitive and Protected PII.

5.2 Access and Management of PII

In the implementation, management and execution of CDBG-DR Programs, PRDOH personnel, subrecipients, contractors and partner agencies will collect, use, process, store, disseminate, come across, and have access to an unprecedented quantity of applicants' personal information. All individuals who are provided access to confidential applicant information are responsible for the protection of passwords information, equipment, case files and communication pathways.

As means of internal control when managing Federal awards funds, PRDOH staff, subrecipients, contractors, partner agencies, and non-Federal entities 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". 2 C.F.R. § 200.303(e).

In accordance with 2 C.F.R. § 200.303, regarding internal controls of a non-Federal entity, the PRDOH has systems in place for the protection of PII obtained. These systems include the management of username and passwords, physical and digital files and archives, use of programs, applications and software, etc. This Policy includes suggested general best practices for these cases.

⁷ 5 U.S.C. § 552 (e) (1).

⁸ 5 U.S.C. § 552 (10). Also, refer to https://www.hud.gov/sites/documents/OHC_PII081214.PDF

⁹ Id.

5.2.1 Confidentiality and Non-disclosure

PRDOH is expected to protect the information entrusted to it by the people looking for CDBG-DR Program assistance. The right to privacy and protection of personal information is embedded in the Puerto Rico Penal Code of 2012, 33 LPRA § 5021 *et seq.* Art. 173 of PR Penal Code states that any person that disseminates, publishes, reveals or gives away to a third party, data, communications or images referred to in Art. 171¹⁰ and Art. 172¹¹ of PR Penal Code, or either offers or solicits such distribution or access, shall be sanctioned. 33 LPRA § 5239.

The Puerto Rico Open Data Act, Act 2019-122, states as public policy of the Government of Puerto Rico that the effective management of government data is essential to support processes of innovation of all sectors, to facilitate a culture of continuous improvement and accountability, for sustainable economic development and growth, and to generate tangible, valuable, and impactful results for its citizens. Confidentiality exceptions to this Act include that the information is protected by law, that revealing the data would cause harm to third parties, information that, if divulged, could invade the privacy of a third party, and all information related to the physical address, phone number, emergency contact information, Social Security number, credit card number, financial or tax information, bank activity, and confidential information of private third parties. PR Open Data Act- 2019-122, Art. 4.

PRDOH CDBG-DR Program parties shall agree to take reasonable steps or measures to protect confidential or sensitive information and will not, without express written authorization from the affected party, use, market, or disclose confidential or sensitive information. PRDOH CDBG-DR contractors and subcontractors shall abide by the confidentiality and non-disclosure clause in their contracts.

5.2.2 Termination and Information Access

Employee or staff off-boarding process shall involve the Human Resources, Operations, Information Technology (IT), and any other identified area to which that employee or staff member has, or has had, any access to files, drives, applications, or any other information handling method. During this process, these areas will work together to identify what information, drives or applications that employee has, or has had, access to in order to properly deactivate all login credentials and privileges assigned to them. It is the employee's supervisor or department head's responsibility to notify the IT Department and request the removal of all access to all employee, that employment has been terminated, through the "Network Access Request Form" and submit it to the

¹⁰ Art. 171 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. 33 LPRA § 5237.

¹¹ Article 172 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. 33 LPRA § 5238.

IT Department.¹² If an employee's device or mobile phone has applications that synchronize information from emails, contacts, calendars, and/or remote storage drives, all of these shall be verified and deactivated immediately. Through the off-boarding process, PRDOH will:

- Reinforce the importance of confidentiality;
- Request any information still in the employee's possession;
- Request 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

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”.¹³ 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 CDBG-DR program participant, employee, or contractor. The Consent form discloses the details to be shared and be signed and dated by the affected party. Certain CDBG-DR 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 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, Subrecipient 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 or local. Monitoring and oversight activities are very important roles in helping PRDOH with the proper implementation of CDBG-DR programs and funds. Notwithstanding this exception, **Monitoring or Oversight** personnel who is granted access to files, documents, computers, and other devices, containing PII must employ the same level of caution any PRDOH CDBG-DR 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.

¹² PRDOH CDBG-DR Information Technology Security Policies, August 23, 2019, page 13.

¹³ 5 U.S.C. § 552a.

In compliance with 2 C.F.R. § 200.303, personnel who have access to confidential or sensitive information are responsible for taking the means necessary to adequately provide for the protection of equipment, files, passwords, and communications managed. PRDOH and Subrecipient 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 parties, nor any of its employees shall divulge or release data or information developed or obtained from the contractual relationship. Personnel shall ensure proper handling of hard copy documentation and files and establish parameters when handling confidential or sensitive information.

As part of the CDBG-DR Program, PRDOH and subrecipients will engage and maintain several means of informing applicants on the status of applications for recovery assistance throughout different phases of program activities. Multiple standard methods of communication, such as but not limited to, postal and electronic mail, will be provided to ensure applicants receive timely, accurate information regarding their applications. Therefore, as established in this Policy, PRDOH has established measures for protecting PII and will train and assist employees and subrecipients in the implementation of equivalent PII strategies.

5.2.4 PII Collection and Information sharing

The right to privacy and control over Applicant's personal information is embedded in the Constitution of the Commonwealth of Puerto Rico. Article II, Section 8, Constitution of Puerto Rico (1952). As part of this constitutional protection, it is in the interest of the State to safeguard the person's right to their dignity, intimacy, and personal integrity.

Generally, HUD establishes its commitment to protecting the privacy of individuals' information stored electronically or paper form, in accordance with federal privacy laws, guidance, and best practices. HUD expects its third-party business partners, including Public Housing Authorities, who collect, use, maintain, or disseminate HUD information to protect the privacy of that information in accordance to applicable law.¹⁴

Collection of Sensitive PII should be limited for set intended purposes. This information 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 provides for the protection and collection of the Social Security number by agencies, dependencies and instrumentalities of the Government of Puerto Rico and its three branches, its municipalities, public corporations, and their contractors (among

¹⁴ Privacy statement included in different HUD assisted programs – The statement was extracted from a Section 8 Project Contract, <https://www.hud.gov/sites/dfiles/OCHCO/documents/52530Bpt1.pdf>

others), within designated parameters and for means that are stated and authorized by Federal legislation.

The Parameters of the Use of Social Security Number of Entities that Provide Services to the Government Act, Act 187-2006, as amended, 18 LPRC § 926(f), establishes as a requisite for contracting with the government, that private entities must guarantee to every citizen that their Social Security number will not be transmitted, displayed, or revealed on accessible or visible documents available to those with unauthorized access.

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 27-2006, 29 LPRC § 621a, establishes that no employer, either private or of any public corporation of the Commonwealth of Puerto Rico, will show or display an employee's Social Security number in their identification card, neither will show or display said number in any place visible to the general public or document of general circulation. The protections granted by this law can be renounced by the employee, only if it is voluntarily and in writing; although, it cannot be imposed as a job condition. Exemptions to the applicability of the provisions of Act 27-2006, are those instances or purposes where the use of the Social Security number is required by law, or it is authorized or regulated by federal laws or regulations. This Act will also not apply when the use of the Social Security number is for identity verification purposes, contributions, contracting, and payroll, subject to the employer's adequate security measures to safeguard and maintain its confidentiality.

The Public Policy for the Use of the Social Security Number as Identification Verification and the Protection of its Confidentiality Act, Act 243-2006, as amended, 29 LPRC § 621 (b), states in its Article 3 that the aforementioned entities can collect the Social Security number of the persons with whom they make official transactions with and use those numbers to verify their identity, cross-reference internal information, and to harmonize internal proceeding of information exchange. It also establishes limitations and prohibitions, as well as general steps the State shall adopt to safeguard the confidentiality of the information.

5.2.5 Information Sharing Agreements

As part of disaster recovery 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 Agreement (**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 ISAA¹⁵, FEMA

¹⁵ 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.

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. As established in DHS/FEMA 008 – Disaster Recovery Assistance Files System of Records¹⁶, 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 employees.
- Parties shall ensure the accuracy of the information.
- PII should only be used to administer Program objectives.
- 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.

5.2.6 Methods of safe transmission of PII

At times, PII will have to be transmitted to another person, agency, program staff, etc. Transmission of PII should be done only on a need to know basis and precautions should be taken such as encryption, if email is used. As precautionary actions, encryption software should be used on desktop designed for the transmission of PII, Sensitive PII should be encrypted before sending, transmitting PII via secure web applications and assuring that protocols have been put in place.

¹⁶ DHS/FEMA 008 – Disaster Recovery Assistance Files System of Records, 78 FR 25283 (Apr. 30, 2013). Document can be accessed at: <https://www.govinfo.gov/content/pkg/FR-2013-04-30/html/2013-10173.htm>.

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 PII, only controlled fax machines shall be used, not central receiving centers.¹⁷

PII should not be placed on shared drives, Intranet or Internet; nor should physical documents be left out on desks, printers, or areas where unauthorized personnel could have access to the information. Sensitive PII must not be transmitted via an unsecured information system (i.e. electronic mail, Internet, or electronic bulletin board) without first encrypting the information.¹⁸

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

- PII should be shared only on a need-to-know basis.¹⁹
- Distribution of PII should only be done when authorized by written consent.
- Discussions of 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 Sensitive PII.
- PII shall not be included in voice messages on any communications mean.
- PII should not be discussed in public or shared spaces where unauthorized persons can overhear.
- Meetings where PII will be discussed should be held in secure spaces.
- Minutes on these notes should be treated as confidential when they contain PII.²⁰
- Records of the date, time, place, subject, chairperson, and attendees at any meeting involving Sensitive PII shall be maintained.²¹
- 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.²²
- Interoffice or translucent envelopes shall not be used to mail Sensitive PII. Instead, sealable opaque envelopes should be used.
- When using the U.S. Postal Service to deliver Sensitive PII, documents shall be double-wrapped (using two envelopes, one inside the other) and mark only the

¹⁷ See https://www.hud.gov/sites/documents/OHC_PII081214.PDF

¹⁸ Id.

¹⁹ DHS Management Directive 11042.1: Safeguarding Sensitive But Unclassified (For Official Use Only) Information defines *need-to-know* as the determination made by an authorized holder of information that a prospective recipient requires access to specific information in order to perform or assist in a lawful and authorized Governmental function, i.e., access is required for the performance of official duties. Document can be accessed at:

https://www.dhs.gov/sites/default/files/publications/Management%20Directive%2011042.1%20Safeguarding%20Sensitive%20But%20Unclassified%20%28For%20Official%20Use%20Only%29%20Information_0.pdf

²⁰ Protecting PII Capacity Building Guidance on Protecting Privacy Information, U.S. Department of Housing and Urban Development, April 2015, https://www.hud.gov/sites/documents/OHC_PII042815.PDF.

²¹ See https://www.hud.gov/sites/documents/OHC_PII081214.PDF

²² Id.

inside envelope as confidential with the statement- *To Be Opened by Addressee Only*).

5.2.7 Public Access to Records containing PII

As required by federal and state laws and regulations, 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 shall 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, available in English and Spanish at <https://www.cdbg-dr.pr.gov/en/resources/policies/general-policies/> and <https://www.cdbg-dr.pr.gov/recursos/politicas/politicas-generales/>.

5.2.8 Disposing of PII

Records containing PII should not be kept longer than required. Once these time frames are met, these records should be destroyed. An appropriate disposal of Sensitive PII is accomplished by **permanently** erasing electronic records and/or shredding hard copy records.²³ PRDOH requires CDBG-DR personnel, contractors, and subrecipients to properly dispose Sensitive PII in accordance with recordkeeping timelines, so that it 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/or 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.

5.2.9 Contractors and Subrecipients

PRDOH expects CDBG-DR Program partners, subrecipients, consultants, contractors, and their personnel to abide by this Policy. When a contractor or subrecipient uses or operates PII systems or creates, collects, uses, stores, maintain, disseminates, discloses or disposes PII within the scope of CDBG-DR Funds, PRDOH shall ensure that the contractors or subrecipients adopts and properly administer this Policy. PRDOH CDBG-DR Program contracts and subrecipient agreements contain clauses or provisions that safeguard against disclosure and inappropriate use of confidential and/or sensitive information. Contractors will not use, sell, market or disclose any confidential or sensitive information to any third party without written consent from the Secretary of PRDOH. It is **by Confidentiality and Non-disclosure agreements** that PRDOH and CDBG-DR Programs set forth fair information practices to ensure personal information is accurate, relevant and current; that uses of information are known and appropriate; and personal or sensitive information is protected.

This Section also includes a series of best practices action steps:

²³ Id.

- Reference or background check on CDBG-DR employees who will have access to Sensitive PII;
- Employee acknowledgement of PII policy and procedures (through Policy Alert Notifications, trainings, etc.);
- Restricting access of PII;
- PII training;
- Redacting Sensitive PII in subrecipient agreements and contracts;
- Nondisclosure of applicant provided information; and
- Proper response and management of a breach.

Contractors are expected to handle data and other information that includes PII with standards that meet or exceed those set forth as part of this Policy. As part of the CDBG-DR program Monitoring, PRDOH will verify program subrecipients and contractors are in compliance with this Policy.

6 PII Breach

The Office of Management and Budget (**OMB**) identifies a PII breach as a type of incident. An *incident* is "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".²⁴

On the other hand, OMB defines a *breach* as the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, or any similar occurrence where a person other than the authorized user accesses or potentially accesses PII for any other than the authorized purpose.²⁵

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

- Loss, damage, theft, or improper disposal of files, documents, equipment that contain PII;
- 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 scenario that could compromise PII (computer virus, phishing, etc.).

Application of the Federal Information Security Management Act of 2002 (**FISMA**), 44 U.S.C. § 3541, as amended by the Federal Information Security Modernization Act of 2014,

²⁴ OMB Memorandum 17-12, issued on January 3, 2017, on Preparing for and Responding to a Breach of Personally Identifiable Information, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

²⁵ Id.

requires each federal agency to develop, document, and implement an agency-wide program to provide information security for its information system and data within to support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. FISMA applies to all agencies within the Federal government and includes state agencies administering federal programs.

Allegations of PII breaches will be subject to investigation and possible disciplinary action in compliance with FISMA requirements.

Failure to abide by this Policy may result in disciplinary action by PRDOH and sanctions and/or additional conditions imposed by HUD, as established in 2 C.F.R. § 200.338.

6.1 Preventing a PII Breach

PRDOH is responsible for the CDBG-DR Programs' accountability with upholding this Policy and overseeing, coordinating and facilitating compliance efforts. PRDOH shall ensure CDBG-DR employees, subrecipients, and personnel are instructed on breach confidentiality, nondisclosure, and PII protection and breach measures.

6.1.1 Training and Awareness

PRDOH ensures that all employees, contractors and subrecipients have sufficient training in handling and protecting PII, as well as identifying and responding to security incidents, including, but not limited to, CDBG-DR personnel and staff who have access to PII and systems that are used to collect, manage, transmit, or dispose of PII. Trainings shall emphasize the information set forth in this Policy and any other guiding document developed herein including, but not limited to:

- The importance of protecting a person's confidentiality;
- Identifying the information that needs to be protected;
- Protecting data and files;
- Proper storage of information;
- How to avoid improper or unintentional data sharing; and
- Identifying and responding to security incidents involving PII.

6.2 Reporting a PII Breach

All suspected or confirmed PII breaches in any medium or form, shall be reported **immediately** to their supervisor, consistent with this Policy. The person who identifies the incident shall not await confirmation that a breach has in fact occurred before reporting it to their supervisor. In turn, the supervisor is responsible to refer the incident to PRDOH's Deputy Secretary. Failure to immediately report an incident may undermine the ability to promptly mitigate the situation and apply preventative and/or remedial measures to protect PII or reduce the harm the incident may potentially cause to individuals. 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.²⁶ 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 PII involved;
- The number of individuals affected; and
- The harm that may result or has resulted from the incident.

It is classified as a low-level impact incident when an unauthorized, unethical disclosure, use or disposal of information that could cause a limited adverse effect on organizational operations or on affected individuals occurs. A moderate-level impact incident is defined when that disclosure of information could cause an adverse effect. However, on a high-level impact incident, the effect caused by the incident is a serious adverse one.²⁷ An incident that contains Sensitive PII, will automatically be classified as a high-level impact incident.

The following are examples of possible incidents that involve PII breach:

- Loss of equipment;
- Security break-in;
- Unauthorized disclosures;
- Unauthorized acquisitions; and
- Unauthorized access.

The evaluation of the incident will be part of the incident report, along with the description of the incident. The report 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?

Although proper documentation is crucial, it is important to note that reporting should not delay the necessary actions to mitigate and respond to an incident nor should these actions be delayed to gain further additional information.

²⁶ OMB Memorandum 17-12, Preparing for and Responding to a Breach of Personally Identifiable Information, https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/m-17-12_0.pdf

²⁷ HUD Breach Notification Response Plan, https://www.hud.gov/sites/documents/INCIDENT_RESPONSE.PDF

6.4 Mitigating the Risk of a PII Breach

PRDOH is 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 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 or gravity of damage;
- 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. Countermeasures should be put in place immediately and these include, for example, expiring compromised account usernames and/or passwords or placing an alert in a database containing potentially compromised PII. Guidance actions are to be provided, such as offering direction on how individuals may obtain more information on the breach and actions to take on their part. Service actions, for example, identity recovery or credit monitoring services, are not always available to mitigate potential harm, however, information, orientation and/or methods for acquiring such services, may be offered.

6.5 Notification of PII Breach

Affected parties of a PII breach should be notified **forty-five (45) days**²⁸ after the breach has been detected and parties affected have been identified. When notifying an affected party, timing, source of the notice, content, and the method of notification should be considered.²⁹ PRDOH is responsible for notifying the parties affected by the breach. The communication should include a description consisting of dates, the type of PII involved, steps that the PRDOH CDBG-DR Program have taken to mitigate harms caused by the breach, steps they would need to take to further protect themselves from the breach, as well as a point of contact person along with their information.

6.5.1 Data Bank Security Breach and Notification to Citizens

The PR Citizen Information on Data Banks Security Act, Act 111-2005, as amended, 10 LPRA § 4051, *et seq.*, states that any entity³⁰ who owns or has under its custody a data bank that includes personal information³¹ of Puerto Rican resident citizens shall notify said

²⁸ The forty five (45) day term is a term established by HUD, sourced from HUD Breach Notification Response Plan, https://www.hud.gov/sites/documents/INCIDENT_RESPONSE.PDF

²⁹ HUD Breach Notification Response Plan, https://www.hud.gov/sites/documents/INCIDENT_RESPONSE.PDF

³⁰ 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).

³¹ 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,

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 PRDOH CDBG-DR's 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 148-2006, as amended, 10 LPRR § 4081 note. 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. 10 LPRR § 4053.

6.6 Requirements for Contractors, Subrecipients, and other Partners

Contractors, subrecipients and partners shall ensure that processes within their PII Policies include proper training, management, and breach responses policies. It is suggested to require training for contractors on PII Breach policies (which shall include identification, reporting, mitigating, and preventing PII breach); have adequate systems and the capability to determine access information (when, where and by whom) to monitor PII information security; and allow inspections or investigations to ensure compliance with this Policy. These should allow PRDOH to adequately and timely respond to any possible or actual PII breaches. As part of the breach response measures, they shall cooperate and exchange information with PRDOH to effectively report and manage possible or actual breaches. When this information exchange is occurring, safety and security best practices are to be implemented.

7 Recommended Best Practices for Safely Handling PII

PRDOH is administering high volumes of PII in the implementation of CDBG-DR programs. Its personnel, subrecipients and partner agencies, along with their staff are expected to protect the information entrusted to them by the 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;³²
- 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 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 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.³³
- 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.³⁴
- Record files shall not be removed from the office without prior consent, even in teleworking circumstances.³⁵
- Consent for file removal shall be given, in writing, by the employee/contractor's supervisor.

³² https://www.hud.gov/sites/documents/OHC_PII081214.PDF

³³ Memorandum, HUD OIG Report: HUD PII Records protection and Management, 2019-OE-0002a, June 25, 2020.

³⁴ Id.

³⁵ 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.
- Electronic Files protection 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

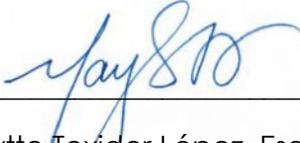
- Virus protection is compulsory for all equipment, workstations, servers that are used to handle PII.
- It is crucial that the antivirus software in every computer is maintained updated.

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.



Maytte Texidor López, Esq.
Legal Director
CDBG-DR Program

September 17, 2020

Date

END OF POLICY.