EQUAL HOUSING OPPORTUNITY

OREGON HOUSING and COMMUNITY SERVICES

OREGON HOUSING and COMMUNITY SERVICES

CDBG-DR

Personally Identifiable Information (PII) Policy

November 2023

REOregon

Recover · Rebuild · Revitalize

CONTENTS

Version History and Version Policy

The version history of the policy is tracked in the table below, with notes for each change. The dates of each publication are also tracked in the table.
The State will publish a new version after making substantive changes that reflect a policy change. The updated policy manual will be assigned a new primary version number such as 2.0, 3.0, etc.

After making non-substantial changes, such as minor wording and editing or clarification of existing policy that do not affect the interpretation or applicability of the policy, the State will publish a version of the document with a sequential number increase behind the primary version number such as 2.1, 2.2, etc.

Amendments made to policy may go into effect on the date of the revision or may be applied retroactively, depending on the applicant pipeline and status of applicants in the program intake and recovery process. Whether a policy will be applied proactively or retroactively will be detailed in the version history below and/or within the relevant program sections.

Version Control Table:

Version Number	Date Revised	Key Revisions
1.0	8/29/2023	Original CDBG-DR PII Policy
1.1	11/16/2023	Added link to User Agreement and Exhibits A & B

Acronyms

Acronym	Meaning
CDBG-DR	Community Development Block Grant–Disaster Recovery
DRGR	Disaster Recovery Grant Reporting System
FEMA	Federal Emergency Management Agency
FISMA	Federal Information Security Management Act of 2002
HUD	The Department of Housing and Urban Development
OHCS	Oregon Housing and Community Services
ORS	Oregon Revised Statutes
PII	Personally Identifiable Information

Definitions

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.

Personally Identifiable Information (PII): Defined in OMB M-07-16 as "...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."

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[1]. 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 Record: 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.[2] The System of Record being referred to in this Policy is Neighborly Software.

[1] 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

[2] 3 5 U.S.C. § 552 (a) (5). Also, see https://www.hud.gov/sites/documents/OHC_PII081214.PDF

1. Introduction

1.1. Overview

Oregon Housing and Community Services (**OHCS**), as grantee, is committed to the responsible management of the Community Development Block Grant-Disaster Recovery (**CDBG-DR**) funds. In doing so, OHCS is dedicated to protecting the privacy of individual stakeholders. Through CDBG-DR program processes, program personnel are often exposed or given access to personally identifiable 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.

1.2 Scope

The Personally Identifiable Information (PII) Policy applies to OHCS 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.

1.3 Purpose

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

2. Personally Identifiable Information

2.1. Overview

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).

To implement these Federal assistance programs, OHCS, as a CDBG-DR 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 records may contain income information, insurance information, bank account numbers, passwords, housing inspection reports, and annotations of various types of assistance. Some, if not most, of the information on an applicant's record is considered personally identifiable information.

PII is information that can be used to distinguish or trace individuals' identities, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. Examples of PII include names, addresses, income verification documents, disability status, employment status, etc., which can be linked or is linkable to a specific participant and/or beneficiary of the Program. As the Program receives direct applications from homeowners requesting assistance, all PII information will be kept in the system of record for the duration of the project. If records containing PII are subject to Freedom of Information Act or Oregon Public Records Law requests, such records shall only be released in accordance with state and federal law. PII records are only stored as long as is necessary, in accordance with record retention requirements at 2 CFR part 200.333 and 24 CFR part 570.502(a)(7).

OHCS 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.

All files containing PII must be handled in a secure manner. To protect PII, files should be given a unique identification number. All records will be maintained in an electronic format. Files are secured to ensure privacy of all participant PII located within the files. Electronic files containing PII will be secured in password protected electronic folders. The CDBG-DR program will backup files on a

routine basis. Required reports to stakeholders may include participant program identification numbers or property addresses, but will not include unique identifiers such as social security number, etc.

2.2. Types of PII

2.2.1. 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 include:

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

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.

2.2.2 Sensitive and Protected PII

Sensitive PII is the personally identifiable information that, when lost, compromised, or disclosed without authorization, could substantially harm an individual[3]. Sensitive PII can encompass standalone information or information paired with another identifier.

Examples of standalone Sensitive PII include:

- 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.

[3] 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

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 be accomplished by statute or by Executive Order of the President.[4] The Federal Privacy Act also requires that the information be maintained in systems of record , electronic and paper, that have the appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of the information.[5] 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.

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

[4] 5 U.S.C. § 552 (e) (1).
[5] 5 U.S.C. § 552 (10). Also, refer to https://www.hud.gov/sites/documents/OHC_PII081214.PDF

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 within the definition of Sensitive PII when information that is not normally sensitive is combined with another, thus becoming Sensitive and Protected PII.

2.3. Access and Management of PII

In the implementation, management, and execution of CDBG-DR programs, OHCS 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 a means of internal control when managing Federal awards funds, OHCS 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, OHCS 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.

2.3.1. Confidentiality and Non-disclosure

OHCS is committed to protecting the privacy of individuals' information stored electronically or in paper form, in accordance with the Privacy Act of 1974, as amended, other federal privacy-related laws, guidance, and best practices and in compliance with ORS 192.311 to 192.478[6].

OHCS CDBG-DR program parties shall agree to take reasonable steps or

[6] Prior to 2017, the numbering was ORS 192.410-192.505

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. OHCS CDBG-DR subrecipients and contractors shall abide by the confidentiality and non-disclosure clause in their contracts.

As part of the CDBG-DR program, OHCS 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 outlined in this Policy, OHCS has established measures for protecting PII and will train and assist employees and subrecipients in the implementation of equivalent PII strategies.

2.3.2. Termination and Information Access

OHCS, subrecipient, and contractor employees and staff should only have access to confidential or sensitive information from their own program and all will be required to read, sign, and agree to the "ReOregon CDBG-DR Data Access Acknowledgment & Agreement"[7] (see Exhibit A). Prior to being granted access to the CDBG-DR System of Record, all users will also fill out the additional acknowledgements on the form specific to handling PII within the System of Record (see Exhibit B). The direct supervisor of the user will submit a request for access form to the system administrator for review, outlining the business need for the access and what level of access is required.

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.

When an employee changes roles, it is the responsibility of the supervisor and the employee to ensure that the system administrator is notified and can properly revoke access, as agreed to in the User Data Agreement.

2.3.3. Written Consent

Applicant information is subject to the Federal Privacy Act of 1974, thus, "[p]ersonal information may be used only by authorized persons in the conduct of official business." The use of information will be limited to ensuring compliance

[7] https://app.smartsheet.com/b/form/247a0bcf9691490481f37f6b200bb5ad

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 an OHCS CDGB-DR program participant, employee, or contractor. The Right to Release form embedded into the Program applications discloses the details to be shared and will be signed and dated by the affected party. Certain CDBG-DR programs provide for Applicants to designate a third party ("alternate contact") to obtain information on their program application.

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 OHCS 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 OHCS CDBG-DR staff, subrecipient or contractor should employ. Information disclosed shall be limited to the precise program or area being monitored or overseen.

2.3.4. PII Collection and Information Sharing

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 who collect, use, maintain, or disseminate HUD information to protect the privacy of that information in accordance with applicable law.[8] Collection of Sensitive PII should be limited for set intended purposes. This information should not be collected or maintained without the proper authorization.

2.3.5. Data Sharing Agreements

As part of disaster recovery efforts, OHCS works along with federal and local agencies, partners, and subrecipients to share information, which includes Sensitive and Protected PII. To establish clear directives, OHCS has formal data sharing agreements. These legal agreements establish the parties' responsibilities in protecting, handling, and sharing PII.

[8] 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

2.3.6. 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.

PII should always be shared and transmitted in a safe manner that minimizes the probability of a breach. Any survivor/registrant PII that is protected by the Privacy Act, whether in physical or electronic form, must be encrypted and/or stored in a secure manner consistent with this type of data, and only stored in places and in a manner that is safe from access by unauthorized persons or for unauthorized use. At a minimum, access to subject data maintained in computer memory must be controlled by password protection and any printouts or other physical products containing PII derived from subject data must be locked in cabinets, file drawers, or other secure locations when not in use.

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.[9]
- 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 through any means of communication.
- 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.
- Meeting minutes notes should be treated as confidential when they contain PII.[10]
- Records of the date, time, place, subject, chairperson, and attendees at any meeting involving Sensitive PII shall be maintained.[11]

---

[9] 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

[10] 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.

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

- Records containing individuals' 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.
- 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 inside envelope as confidential with the statement- To Be Opened by Addressee Only).

2.3.7 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 2 C.F.R. § 200.338[12] and 24 C.F.R. § 570.508[13], OHCS shall provide citizens with reasonable access to records regarding the past use of CDBG-DR funds, in accordance with applicable State and local laws regarding privacy and confidentiality.

2.3.8 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 disposure of Sensitive PII is accomplished by permanently erasing electronic records and/or shredding hard copy records. OHCS requires CDBG-DR personnel, contractors, and subrecipients to properly dispose of 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.

2.3.9 Contractors and Subrecipients

OHCS 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

[12] See https://www.ecfr.gov/current/title-2/subtitle-A/chapter-II/part-200/subpart-D/subject-group-ECFR4acc10e7e3b676f/section-200.338
[13] See https://www.ecfr.gov/current/title-24/subtitle-B/chapter-V/subchapter-C/part-570/subpart-J/section-570.508

Funds, OHCS shall ensure that the contractors or subrecipients adopt and properly administer this Policy. OHCS CDBG-DR program contracts and subrecipient agreements contain clauses or provisions that safeguard against disclosure and inappropriate use of confidential and/or sensitive information. It is through Confidentiality and Non-disclosure Agreements that OHCS 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.

Contractors are expected to handle data and other information that includes PII with standards that meet or exceed those set forth in this Policy.

3. Security Breach

The State of Oregon defines a "security breach" as "an unauthorized acquisition of computerized data that materially compromises the security, confidentiality or integrity of personal information that a person maintains or possesses."[14]

HUD likewise identifies a PII breach as occurring "when PII is viewed, leaked, or accessed by anyone who is not the individual or someone authorized to have access to this information as part of his/her official duties."[15]

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, 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.

3.1. Preventing a Security Breach

OHCS is responsible for the CDBG-DR program's accountability with upholding this Policy and overseeing, coordinating, and facilitating compliance efforts.

[14] 646A.602 Definitions for ORS 646A.600 to 646A.628; Identity Theft Protection Act
[15] 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

OHCS shall ensure CDBG-DR employees, subrecipients, and personnel are instructed on breach confidentiality, nondisclosure, and PII protection and breach measures.

3.1.2. Training and Awareness

OHCS 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.

3.2. Reporting a PII Breach

All suspected or confirmed PII breaches in any medium or form shall be reported immediately to an individual's 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 for referring the incident to the Chief Compliance & Contracting Officer by submitting a report[16] linked to on the ReOregon public website. 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.

All "suspect compromises of sensitive PII" must be promptly reported to HUD's Privacy Officer at the National Help Desk at 1-888-297-8689 or privacy@hud.gov by the Chief Compliance & Contracting Officer. HUD will investigate the incident and will consult the Grantee (and FEMA if the breach involved FEMA

[16] Breach of Personally Identifiable Information (PII) Report
https://app.smartsheet.com/b/form/c5c6938e590140a481e16ba1bc1da84b

data) in a timely and on-going basis to diagnose, mitigate and manage the privacy incident until its conclusion. The Grantee shall be responsible for cooperating with HUD to allow HUD to comply with section XIII of the HUD-FEMA Agreement. The Grantee may be responsible for carrying out the necessary measures to remedy the effects of the privacy incident, including notification, unless mutually agreed upon otherwise, and may be responsible for bearing any costs associated with such measures.

Additionally, under ORS 646A.604 any breach of security must be reported to the Oregon Department of Justice[17].

3.3. Evaluation of a PII Breach

When evaluating the type and severity of a breach, OHCS shall consider intent and recipient. Analyzing intent in a PII breach refers to whether the information was compromised intentionally, unintentionally or if the intent is unknown. OHCS will also evaluate if the recipient of disclosed PII is known or unknown, as well as the trustworthiness of that recipient, if it is a known recipient.[18] This evaluation will provide a frame of reference in evaluating 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.

An incident is classified as low-level impact 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. An incident is classified as a moderate-level impact 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 effect".[19] An incident that contains Sensitive PII will automatically be classified as a high-level impact incident.

---

[17] Oregon DOJ Report Data Breaches form (https://justice.oregon.gov/consumer/DataBreach/Home/Submit)
[18] OMB Memorandum M-17-12 "Preparing for and Responding to a Breach of Personally Identifiable Information" https://osec.doc.gov/opog/privacy/Memorandums/OMB_M-17-12.pdf
[19] HUD Breach Notification Response Plan, https://www.hud.gov/sites/documents/INCIDENT_RESPONSE.PDF

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 in order to gain additional information.

3.4. Mitigating the Risk of a PII Breach

OHCS is prepared to act promptly when a PII breach occurs in order to reduce the potential harm to the affected individuals. Once a full risk assessment has been performed, adequate measures to mitigate the possible harm to individuals that the potential or confirmed PII breach may cause must be applied. 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.

3.5. Notification of a PII Breach

In accordance with Oregon law[20] and federal guidance, affected parties of a PII breach should be notified no later than forty-five (45) days after the breach has been detected and parties affected have been identified[21].

When notifying an affected party, timing, source of the notice, content, and the method of notification should be considered. OHCS 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 OHCS 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 and their information.

3.6. 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 OHCS 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 OHCS to effectively report and manage possible or actual breaches. When this information exchange is occurring, safety and security best practices are to be implemented.

---

[20] Oregon's Data Breach Law (ORS 646A.600-646A.628) https://www.doj.state.or.us/wp-content/uploads/2017/10/oregon_data_breach_reporting.pdf

[21] 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

4. Recommended Best Practices for Safely Handling PII

OHCS 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.

4.1. 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;[22]
- Following proper disposal methods of documents that contain PII; and
- Immediately reporting suspected or confirmed acts or incidents of privacy violations.

4.2. User IDs and Passwords

- User IDs 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 complex, be changed quarterly for the system of record, and must comply with all requirements in the Statewide Standards.[23]
- Not be easily guessed.
- Neither should be allowed to be included in automated login process or saved by browsers.

[22] See https://www.hud.gov/sites/documents/OHC_PII081214.PDF
[23] See Oregon Statewide Standards https://www.oregon.gov/das/OSCIO/Documents/2019StatewideInformationAndCyberSecurityStandardsV1.0.pdf

4.3. Hard Copies and Electronic Files

- PII inventories shall be maintained with identifying lists of (1) paper records; (2) electronic records; and (3) new records that contain PII.
- 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.
- Record files shall not be removed from the office without prior consent, even in teleworking circumstances.
- Consent for file removal shall be given, in writing, by the employee/contractor's supervisor.

4.4. 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. Emails should be encrypted.
- Do not leave computers unattended without locking or logging out.

4.5. Virus Protection

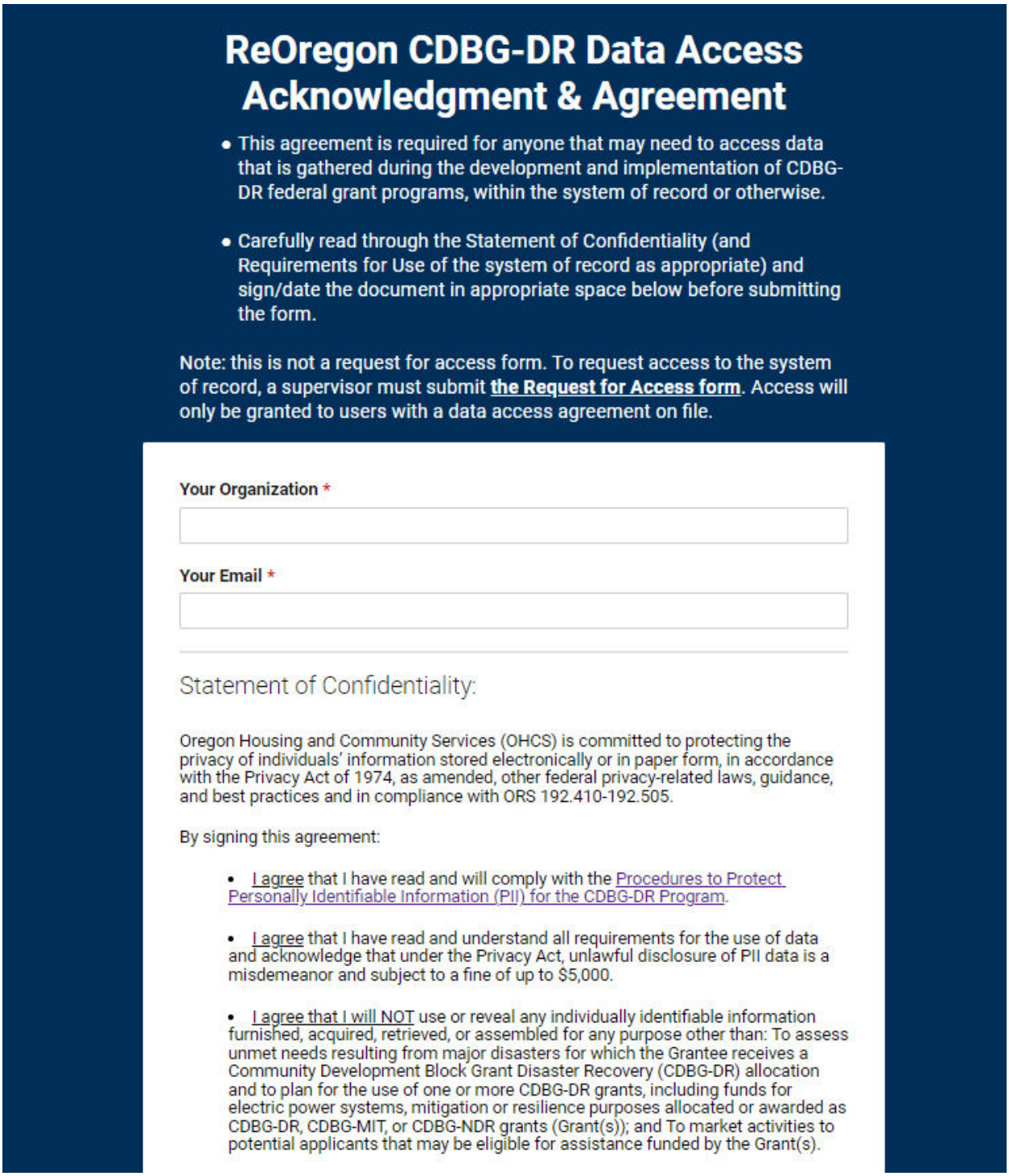
- Virus protection is compulsory for all equipment, workstations, and servers that are used to handle PII.
- It is crucial that the antivirus software in every computer is maintained and updated.

4.6. PII Breaches

- Any real or potential PII breach or violation of this Policy must be reported immediately to a supervisor by the employee or contractor. Supervisors then must follow up immediately with the DRR Chief Compliance & Contracting Officer.
- Actions in the case of a PII breach 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.

Exhibit A

ReOregon CDBG-DR Data Access Acknowledgement and Agreement



ReOregon CDBG-DR Data Access Acknowledgment & Agreement

- This agreement is required for anyone that may need to access data that is gathered during the development and implementation of CDBG-DR federal grant programs, within the system of record or otherwise.
- Carefully read through the Statement of Confidentiality (and Requirements for Use of the system of record as appropriate) and sign/date the document in appropriate space below before submitting the form.

Note: this is not a request for access form. To request access to the system of record, a supervisor must submit **the Request for Access form**. Access will only be granted to users with a data access agreement on file.

Your Organization *

Your Email *

Statement of Confidentiality:

Oregon Housing and Community Services (OHCS) is committed to protecting the privacy of individuals' information stored electronically or in paper form, in accordance with the Privacy Act of 1974, as amended, other federal privacy-related laws, guidance, and best practices and in compliance with ORS 192.410-192.505.

By signing this agreement:

- I agree that I have read and will comply with the Procedures to Protect Personally Identifiable Information (PII) for the CDBG-DR Program.
- I agree that I have read and understand all requirements for the use of data and acknowledge that under the Privacy Act, unlawful disclosure of PII data is a misdemeanor and subject to a fine of up to $5,000.
- I agree that I will NOT use or reveal any individually identifiable information furnished, acquired, retrieved, or assembled for any purpose other than: To assess unmet needs resulting from major disasters for which the Grantee receives a Community Development Block Grant Disaster Recovery (CDBG-DR) allocation and to plan for the use of one or more CDBG-DR grants, including funds for electric power systems, mitigation or resilience purposes allocated or awarded as CDBG-DR, CDBG-MIT, or CDBG-NDR grants (Grant(s)); and To market activities to potential applicants that may be eligible for assistance funded by the Grant(s).

- I agree that I will NOT make any disclosure or publication whereby an individual or household could be identified, or the data furnished by or related to any particular person could be identified.
- I agree that I will NOT permit anyone other than Authorized Users to access the data.

Will you need access to the system of record?

○ Yes ◉ No

☐ **I have read and agree to all of the above and understand my responsibilities over any CDBG-DR data I access.** *

My signature below indicates my agreement to comply with the Statement of Confidentiality, as written above.

Signature *

Enter your full name below:

Date Signed *

☐ Send me a copy of my responses

Submit

Exhibit B

Will you need access to the system of record?

(•) Yes ( ) No

Requirements for Use of the System of Record:

- The User shall be provided information on all data standards, policies, and procedures; User must comply with all data standards and policies and procedures.
- System User credentials (user ID and password) must be kept secure and are not to be shared.
- The User is expected to physically enter the password each time the User accesses the system. DO NOT save passwords in auto-complete settings.
- The User shall access only the case records pertaining to User's assigned work duties.
- Should the User download PII in any format, the User will securely store and/or dispose of all electronic and hard copy in a manner to protect the information. At a minimum this will require the use of strong password protection, preferably including encryption.
- Should the User no longer need access to the system of record to perform their work, the User will inform the Business System and Reporting Team as soon as reasonably possible (BSR.Help@hcs.oregon.gov).
- This agreement will be superseded by any additional or alternative agreements presented by System Administrators.

Failure to comply with the provisions of this User Agreement may result in the termination of the User License. There is no expiration date of this agreement.

☐ **I have read and agree to all of the above and understand my responsibilities over any CDBG-DR data I access.** *

My signature below indicates my agreement to comply with the Statement of Confidentiality and Requirements for Use of the System of Record, as written above.

Signature *

Enter your full name below:

Date Signed *

☐ Send me a copy of my responses

Submit