



CDBG-DR PII Policies and Procedures

October 2026

Version 1

Table of Contents

I. Personally Identifiable Information Overview	3
a. Types of PII	3
i. Public PII	3
ii. Sensitive PII	3
II. File Security	4
a. Collection and Storage	4
i. Hard Copy	4
ii. Electronic.....	4
b. Minimization	5
i. Physical	5
ii. Technical	5
iii. Administrative.....	5
III. Access to Records	6
a. Authorized Users.....	6
b. Release of Information	6
c. Transmission Method Standards.	7
d. Disposal	7
e. Subrecipient and Contractor Obligations.	7
IV. Breaches of Privacy of PII.....	8
a. Reporting a PII Breach	8
b. Evaluation of a PII Breach	8
i. Risk Assessment	8
ii. Response and Mitigation	8
iii. Alabama Data Breach Notification Compliance.....	9

I. Personally Identifiable Information Overview

The purpose of this policy is to set minimum standards to ensure Baldwin County and its subrecipients take reasonable steps to protect all Personally Identifiable Information (PII). PII is any information that can be used to distinguish or trace an individual's identity either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. PII is defined by 2 CFR 200.82 and 2 CFR 200.79, as, but not limited to: names, addresses, income verification documents, disability status, and/or employment status. PII can be linked to current or prospective applicants and/or beneficiaries, committee members, vendors, and others involved in the CDBG-DR program. Proper measures must be taken to ensure documents that include PII are properly managed and secured from unauthorized access and inappropriate use.

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

a. Types of PII

i. Public PII

Public PII is defined by 2 CFR 200.79 as personally identifiable information that is available in public sources such as telephone books, public websites, and university listings. Examples include:

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

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

ii. Sensitive PII

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

Examples of standalone Sensitive PII include:

- Driver's license;

- Social security numbers or comparable identification numbers (i.e., passport 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;
- Account passwords;
- Last four (4) digits of Social Security number; and
- Date of birth.

II. File Security

In compliance with 2 CFR 200.303 and all U.S. Constitution, Federal statutes, regulations, and the terms and conditions of the Federal award, the County will take the following actions to ensure protection of PII.

a. Collection and Storage

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. The Federal Privacy Act also requires that information be maintained in systems of record, electronic and paper, that have appropriate administrative, technical, and physical safeguards to protect the security and confidentiality of the information.

Collection should be conducted according to best practice and legal requirements for the type and purpose of data collected. Because the collection process itself can potentially lead to unintended PII disclosure, considerations of confidentiality in collection and recording should be explicitly addressed.

The grant manager will advise the beneficiary or subrecipient prior to intake or processing of application information that PII will be required and complete the eligibility review and other required necessary steps to provide program assistance.

i. Hard Copy

Hard copies containing PII shall be stored in locked file cabinets, locked desk drawers, or secured rooms with controlled access limited to Authorized Users. Storage areas shall be locked when unattended.. Documents containing PII are not to be left on desks or in other locations that may be visible to individuals not authorized to access the PII.

ii. Electronic

All electronic files must require password-protected access. Confidential or sensitive information, if emailed, should be encrypted.

b. Minimization

In efforts to minimize the exposure of PII, the County will redact financial account information, use partial Social Security Numbers, and applicant ID numbers. The County is responsible for ensuring that the number and scope of physical and electronic copies of PII are kept to the minimum necessary and only for the period where a valid business need for the information exists. Safeguards

The County is responsible for the CDBG-DR program's accountability with upholding this policy and overseeing, coordinating, and facilitating compliance efforts. To protect PII against inappropriate access, use, disclosure or transmission, the County requires appropriate administrative, technical, and physical safeguards. The Grant Management team is responsible for documenting security controls and safeguards and risk management.

i. Physical

Cabinets and doors should remain locked to areas deemed secure containing PII. Visitor access should be limited to prevent unauthorized users from accessing information.

ii. Technical

(a) When transmitting PII via email, the sender shall:

- a. Verify recipient email addresses against the County's Authorized User list before transmission;
- b. Encrypt the email message and any attachments containing PII using [SPECIFY ENCRYPTION STANDARD, e.g., AES-256 or TLS 1.2 or higher];
- c. Transmit encryption passwords or decryption keys through a separate communication channel; and
- d. Retain transmission logs documenting recipient verification and encryption methodology.

(b) Any shared files should be password protected, or user access should be limited to authorized users.

iii. Administrative

All staff, subrecipients and contractors are required to read this policy and sign a User Policy and Responsibility Statement to demonstrate their understanding and assurance to maintain the privacy and security of PII. All Authorized Users shall complete PII protection training prior to accessing PII. The County shall maintain training completion records and require refresher training [annually].

1. Third-Party Service Providers and Cloud Storage.

- i. Vendor Due Diligence. Prior to engaging any third-party service provider that will access, process, or store PII, the County shall:
 - a. Conduct due diligence regarding the vendor's information security practices, including review of SOC 2 Type II reports,

CDBG-DR
PII Policies and Procedures

- ISO 27001 certifications, or equivalent third-party security assessments;
- b. Verify that the vendor's data storage locations comply with applicable federal data residency requirements; and
- c. Obtain written assurance of the vendor's compliance with this Policy and applicable federal and state privacy laws.
- ii. Contractual Requirements. All contracts with third-party service providers that access, process, or store PII shall include provisions requiring:
 - a. Implementation and maintenance of administrative, physical, and technical safeguards meeting or exceeding County standards;
 - b. Limitation of PII use to purposes specified in the contract;
 - c. Prohibition on sub-contracting or sub-processing without prior County approval;
 - d. Immediate breach notification to the County;
 - e. County audit rights and access to vendor security documentation;
 - f. Secure return or destruction of PII upon contract termination; and
 - g. Indemnification of the County for losses arising from vendor breaches.

III. Access to Records

a. Authorized Users

Authorized users are employees, contractors or subcontractors, or subrecipients who have entered an agreement with Baldwin County to comply with all requirements of the use of data contained in the HUD Data Sharing Agreement and acknowledge that under the Privacy Act.

The County prohibits data use and access by any individual that is not identified by the County as an Authorized User. If an individual requests access, and is not identified as an Authorized User, the County will notify the individual in writing within 72 hours that the request is denied. Authorized Users will be reviewed quarterly to ensure that no users maintain access when not needed.

b. Release of Information

The County releases records containing PII upon request, after verification, to federal and state auditors and other federal or state agencies for DOB analyses.

Subrecipients may be required to release records containing PII upon request from the County or a County-designated auditor, if required by federal or state auditor or other federal or state agencies.

c. Transmission Method Standards.

Transmission of PII should be done only on a need-to-know basis. PII should always be shared and transmitted in a safe manner that minimizes the probability of a breach, and the following precautions should be taken:

1. **Electronic Transmission.** PII transmitted electronically shall be encrypted using [SPECIFY STANDARD] or transmitted through secure file-sharing platforms with multi-factor authentication and access logging.
2. **Physical Mail.** Documents containing Sensitive PII transmitted via physical mail shall be sent via certified or registered mail with return receipt requested or delivered by bonded courier service.
3. **Portable Media.** Portable storage devices containing PII shall be encrypted, password-protected, physically secured during transport, and subject to chain-of-custody logging.
4. **Telephone Authentication.** Before disclosing PII over the telephone, the County employee shall authenticate the caller by verifying [SPECIFY AUTHENTICATION FACTORS, e.g., applicant ID number, date of birth, and last four digits of SSN] against County records.
5. **Prohibited Transmission Methods.** PII shall not be transmitted via unencrypted email, text message, fax, or other unencrypted electronic communication method.

Distribution of PII should only be done when authorized by written consent. To the furthest extent possible, the County will ensure emails are sent only to intended recipients.

PII should only be discussed over the phone after confirming the person is authorized to receive the information, and the information in that discussion will include Sensitive PII. PII should not be included in voice messages or discussed in public or shared spaces.

d. Disposal

Records containing PII shall not be kept longer than required by federal and state laws and regulations. 2 CFR 200.334 states that all federal awards records must be retained for three years from the date of submission of the final financial report.

Once these time frames are met, PII must be destroyed and rendered unreadable before disposal. This includes shredding hard copies, wiping electronic files, and permanently deleting emails including PII. The County will follow all guidelines regarding how long information may be retained before requiring deletion or destruction.

e. Subrecipient and Contractor Obligations.

1. **Contractual Requirements.** All subrecipient agreements, vendor contracts, and consultant engagements involving access to PII shall incorporate this Policy by reference and include provisions requiring:
 - i. Compliance with all PII collection, storage, transmission, and disposal requirements set forth herein;
 - ii. Implementation of physical, technical, and administrative safeguards meeting or exceeding County standards;

- iii. Immediate notification to the County of any suspected or confirmed PII breach;
 - iv. Submission to County monitoring, inspection, and audit of PII-handling practices; and
 - v. Indemnification of the County for losses arising from the subrecipient's or contractor's breach of PII protection obligations.
2. **Remedies for Non-Compliance.** The County reserves the right to suspend or terminate any subrecipient agreement or contract for material breach of PII protection obligations and to pursue all available legal and equitable remedies, including recovery of damages and injunctive relief.

IV. Breaches of Privacy of PII

HUD defines 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.

a. Reporting a PII Breach

Known or suspected violations of this policy should be reported within 24 hours to the Baldwin Grants Department at 251-937-6820, or BCCGrants@baldwincountyal.gov. The Grants Department must notify ADECA within 24 hours of their received known or suspected violation.

b. Evaluation of a PII Breach

i. Risk Assessment

Evaluate the type and severity of the breach.

1. Determine the intent of the breach and whether the information was compromised intentionally, unintentionally, or if the intent is unknown.
2. Determine if the recipient of the disclosed PII is known or unknown.
3. Assign classification of low, moderate, or high according to the severity of the incident.
 - a. Low impact: an unauthorized, unethical disclosure, use or disposal of information that could cause a limited adverse effect on operations or on an affected individual.
 - b. Moderate impact: disclosure of information that could cause an adverse effect.
 - c. High impact: serious adverse effect, containing Sensitive PII

ii. Response and Mitigation

Actions required to mitigate potential harm will be on a case-by-case basis. If mitigation actions are necessary, consider the following:

- Damage occurred, if any;
- Nature of the damage;
- Amount or gravity of damage;
- Type of data disclosed; and

- Reason for the disclosure.

Mitigation efforts may include countermeasures such as expiring compromised account usernames and/or passwords or guidance such as directions on how individuals may obtain more information on the breach and actions to take on their part.

iii. Alabama Data Breach Notification Compliance

If the breach involves personal information as defined by Ala. Code § 8-38-2(3) (combination of name with SSN, driver's license number, or financial account information) and affects one or more Alabama residents, the County shall provide notification in accordance with Ala. Code § 8-38-5 and -6, including but not limited to:

- Notification to affected Alabama residents without unreasonable delay;
- Inclusion of the date or estimated date of the breach, description of personal information acquired, description of the actions taken to restore the security and confidentiality of the personal information, description of steps an affected individual can take to protect himself or herself from identity theft, and County contact information; and
- Notification to the Alabama Attorney General if the breach affects more than 1,000 Alabama residents.