Town of Jay
Personally Identifiable Information (PII) Security and Client Confidentiality Policy
CDBG-DR

In order to carry out CDBG-DR programs, the Town of Jay must have adequate procedures in place to collect and process applicant provided information while providing assurances that any Personally Identifiable Information (PII) will be handled properly and is sufficiently protected. This policy has been created to communicate the Town's requirements related to the proper handling and securing of Personally Identifiable Information (PII) for contractors administering CDBG-DR programs.

PURPOSE

The purpose of this policy is to ensure the confidentiality and integrity of PII provided in a hard copy format and/or electronically stored or transmitted over Town of Jay and contractor computer networks and telephone systems. This policy outlines the methods to collect, document, and properly dispose of applicant hard copy paperwork containing PII as well as establishing acceptable uses and methods of transmission of PII data. All program staff, which includes contractor staff, will be provided with a copy of this PII policy and will be required to sign a User Policy and Responsibility Statement acknowledging understanding of these policies. Basic components of this policy are to establish proper protocols to:

- Ensure proper handling of hard copy documentation and files.
- Secure hard copy PII in applicant files or documents that are being actively reviewed or worked.
- Establish parameters related to the use of applicant data transmitted and maintained in electronic media.
- Outline potential disciplinary actions for violations of the PII policy.
- Establish protocols should a breach of data occur during the administration of the CDBG-DR Programs

CDBG-DR program staff will collect certain client data, including but not limited to, demographic information, contact information, home address, current location, insurance information, financial information, FEMA registration ids and information pertaining to the specific needs of individuals affected by the disaster. The parties agree that the storage and sharing of this data shall be used for the benefit of individuals affected by the disaster and for no other purpose.

DEFINITION

For the purposes of this policy, personally identifiable information (PII) refers to information which can be used to distinguish or trace an individual's identity, such as their full name, social security number (including only the last-4 digits), biometric data, policy numbers, award amounts, income, bank account information, etc.

Types of PII

In determining what PII is sensitive, the context in which the PII is used must be considered. For example, a list of people subscribing to a Town of Jay newsletter is not sensitive PII; a list of people receiving treatment for substance abuse is sensitive PII. In addition to context, the association of two or more non-sensitive PII elements may result in sensitive PII. For instance, the name of an individual would be sensitive when grouped with place and date of birth and/or mother's maiden name, but each of these elements would not be sensitive independent of one another. Therefore files/data may be sensitive as a whole, but individual data points or documents may not be considered sensitive. This means the file/data must be handled as sensitive PII.

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

1) Place of birth
2) Date of birth
3) Full Name, Mother's maiden name
4) Biometric information and personal characteristics including; photographic images, fingerprints, handwriting, retina scan, voice signature, and facial geometry
5) Medical information, except brief references to absences from work
6) Personal financial information (account numbers, award amounts, income, etc.)
7) Credit card or purchase card account numbers
8) Passport numbers, driver's license number and taxpayer ID
9) Potentially sensitive CDBG-DR information related to grant or loan awards (applicant identification number, grant/loan amounts, etc.)
10) Criminal history
11) Any information that may stigmatize or adversely affect an individual
12) Social Security Numbers (SSN) and/or partial SSN do NOT need to be associated with an individual to be considered PII. Social Security Numbers or the last 4 digits of a SSN alone, with no other information, are considered PII.

This list is not exhaustive, and other data may be sensitive depending on specific circumstances. In no case shall an applicant's PII be released to another party without written consent of the applicant (See Exhibits A). In addition, no CDBG-DR personnel will be permitted access to any file where there could be a potential or perceived conflict of interest.

Non-PII

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

1) Work phone numbers
2) Work addresses
3) Work e-mail addresses
4) Documents that do not include an SSN or where the SSN is removed or other applicant sensitive information (CDBG-DR applicant identification number or award amounts)
5) General background information about individuals found in their application for assistance

PUBLIC RECORDS AND THIRD-PARTY REQUESTS FOR INFORMATION

The determination that certain PII is non-sensitive does not mean it is publicly releasable. The determination to publicly release any information can only be made by the official authorized to make such determinations. Florida Statute 119.071 defines the general exemptions for public records. Any request for release of information not covered under normal job duties as well as any media inquiries must be directed to the Town of Jay Town Clerk for review. No replies to media shall be provided by staff without prior authorization from the Town Manager.

Authorized Data Uses

PII gathered from program applicants, including any written or verbal disclosure of information, may be used only to determine applicant eligibility, verify duplication benefits, and conduct other required actions necessary to facilitate the provision of services and assistance to clients with their informed consent.

CDBG-DR project contractors shall, at all times, have rights to data pertaining to their clients that was created and/or entered by the client for CDBG-DR projects or provided by assistance agencies (e.g., FEMA, SBA, NFIP, etc.). Contractors shall follow all applicable rules and policies pertaining to the restrictions on use of personal data that a client has not formally released.

Authorized Users

Authorized Users are employees and agents (including contractors or subcontractors), who have entered an agreement with the Town of Jay to comply with all requirements on the use of data contained in the HUD Data Sharing Agreement 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. Authorized users must have executed a CDBG-DR User Policy and Responsibility Statement indicating that they have reviewed and understand this policy and will ensure the protection of PII.

The Town of Jay prohibits data use and access by any individual that is not identified by the Town as an Authorized User.

PROCEDURES

Staff Onboarding

All Town of Jay staff, or staff of sub-recipients and contractors are required to read this policy and execute a User Policy and Responsibility Statement during initial onboarding to demonstrate their understanding and assurance to maintain the privacy and security of PII. User Policy and Responsibility Statements are reviewed by the Town Manager.

Electronic Transfer of Files

Designated Town of Jay staff will have access to shared data files from other agencies that contain PII. These files will be stored on a protected network drive that has special permissions for a small group of users. These files will be transferred to the contractor using an encrypted website for uploading into the system that will be used to validate applicants for duplication of benefits.

Document Retention and Destruction

The Town of Jay will maintain records in accordance with State guidelines for record retention (See Recordkeeping Policy and Procedures). Upon completion of the retention period, the Town of Jay shall destroy data provided under the HUD Data Sharing Agreement and all PII gathered to provide assistance through the CDBG-DR program.

Hard copy data will be manually shredded, and a *Records Disposition Document* will be completed to keep a record of the general type and size of records that have been destroyed. Shredding may be completed by Town staff or a contracted vendor to provide confidential document destruction services. The Town of Jay will notify Florida Commerce in writing when the data provided under the agreement is destroyed. If recordkeeping periods extend beyond the required period after grant closeout, the Town of Jay shall retain records of decisions based on the use of the data for the recordkeeping period required by the grant(s). (See Recordkeeping Policy and Procedures.)

Breach of PII

A privacy incident is a violation or imminent threat of a violation of privacy laws, principles, policies, and practices. Breaches, which are situations where unauthorized individuals have access or potential access to PII, are one type of privacy incident. However, there are other types of privacy incidents, which includes using PII for purposes other than the stated purpose for which the information was originally collected, exceeding the retention period for PII, and collecting and/or using PII without first providing proper notice. The term "privacy incident" encompasses both suspected and confirmed incidents involving PII.

A PII breach, according to OMB M-17-12, is an incident involving the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access, or any similar occurrence where PII is accessed or potentially accessed by a person other than an authorized individual or for an unauthorized purpose whether physical or electronic."

A PII breach can occur in various ways including when personal information about clients is stolen, lost, or mistakenly disclosed (examples include a loss or theft of mobile devices, misdirected communications, like an email going to the wrong person). Breaches may also be intentional when personal information is accessed, used, disclosed, destroyed, or altered without authority (examples include snooping, hacking, and ransomware).

If a breach, or a suspected breach of PII occurs the following steps will be followed:

1) Immediately inform a supervisor upon discovery or detection. Communication is the key.
2) Determine if the incident occurred within a Town of Jay system or a contractor's system.
3) Contain the breach. A program team including Town of Jay and contractor staff will be formed to immediately act and prevent further disclosure of PII. These steps may include:
    - Stopping an unauthorized practice, such as ceasing transmission of email or correspondence to an incorrect recipient.
    - Removing, moving, or isolating exposed information or files, to prevent further unauthorized access or disclosure.
    - Retrieving any documents or copies of documents that were wrongfully disclosed or taken by an unauthorized person.
    - Conducting physical searches for records that were lost or stolen.

- Returning physical records to their original location or providing them to the intended recipient.
- Requesting and verifying that an unintended recipient double-deleted all affected email, correspondence, and records.
- Shutting down the system that was breached or correcting weaknesses in security.
- Revoking access to the system.
- Changing passwords.
- Contacting the person responsible for security in the organization so that further security measures can be put in place.

4) Evaluate the risks associated with the breach and provide that evaluation to the Town Manager.
   To consider what steps are necessary to take in response to a breach, the Town Manager will need to determine if the privacy breach created any harm for affected individuals. Examples of harm which could impact an individual include:
   - Physical or bodily harm
   - Social harms - inconvenience, distress, humiliation, damage to the individual's reputation or relationships
   - Financial harms - loss, identity theft, negative effects on the individual's credit rating or report, loss of employment, business, or professional opportunities, or damage to or loss of the individual's property
5) Next, the team evaluating the breach will determine the probability of harm by summarizing the incident to include:
   - Cause and extent of the breach which could include determining if the act was deliberate or accidental and what was the number of people that actually or potentially accessed the information.
   - Nature of the data elements breached, to include context and potential harm from disclosure.
   - Number of individuals affected by the breach, to include how many are affected and are they vulnerable individuals.
   - Likelihood the information is accessible and useable, which includes determining if unauthorized copies have been destroyed or committed to non-use while considering the level of encryption and proof of destruction; length of time that the information was available to be accessed, used, or disclosed, destroyed, or altered; risk of ongoing or further exposure; amount of information; was the information recovered; and was the information adequately encrypted, anonymized or not easily accessible.
   - Evidence of harm from the breach, to include if harm has already materialized or the likelihood harm will occur, and the broad reach of the harm.
   - Ability to mitigate the risk of harm, to include if there is mitigation that can avoid further compromise of the data; and if so, that should be included in a notification.
6) Notify and report those affected as determined by the evaluation of the risks. Notification can also be an important risk mitigation strategy in the appropriate circumstances, whether it is deemed mandatory or not. A key consideration in deciding whether to notify affected individuals should be whether notification is necessary to avoid or mitigate harm to an individual whose personal or personal health information has been affected by the privacy breach.

If a notification is deemed appropriate, it should include:

- A description of the circumstances of the privacy breach.
- The date or period of time that the privacy breach occurred or is believed to have occurred.
- The name of the public body who had custody or control of personal information at the time of the privacy breach.
- A description of the PII that was the subject of the privacy breach.
- A description of the steps that the Town of Jay has taken or is intending to take, as of the date of the notice, to reduce the risk of harm to the individual as a result of the privacy breach and to reduce the risk of a similar privacy breach in future.
- A description of the steps that the individual can take to reduce the risk of harm that could result from the privacy breach or to mitigate that harm.
- The name or contact information of an employee of the Town of Jay who is able to answer questions about the privacy breach.
- Any other information that the Town of Jay considers relevant.

The method of notification can align with the number of individuals affected and the urgency to which notification is required. Possible methods include telephone, first- class mail, email, existing government-wide services, newspapers or other media outlets, or substitute notice. The selected notice will be Section 508 compliant.

7) Finally, the Town of Jay will work to prevent future breaches.

This policy has been adopted by the Town of Jay Town Council by a vote of four (4) yeas and zero (0) nays on October 6, 2025.

Donna Bullock, Town Clerk

Shon Owens, Mayor