Chapter 02

Personally Identifiable Information

STATE OF MISSOURI CDBG
POLICY STATEMENT
IN EFFECT FOR ANNUAL GRANTS:

Year	Award Number
2015	B-15-DC-29-0001
2016	B-16-DC-29-0001
2017	B-17-DC-29-0001
2018	B-18-DC-29-0001
2019	B-19-DC-29-0001
2020 (CV)	B-20-DW-29-0001
2020	B-20-DC-29-0001
2021	B-21-DC-29-0001

IN EFFECT FOR DR/MIT GRANTS:

DR-4317: B-18-DP-29-0001
DR-MIT: B-18-DP-29-0002
DR 4451: B-19-DF-29-0001

POLICY CHANGES OR UPDATES TABLE

ACTION	VERSION #	CHANGE #	PAGE #	SUMMARY OF ACTION	APPROVAL DATE
Approval	1.0	0	Entire document	Creation of Personally Identifiable Information Policy	12/1/2022

2.1 INTRODUCTION

The State of Missouri Department of Economic Development Community Development Block Grant Program (DED) is required to collect and maintain Personally Identifiable Information (PII) for a variety of reasons related to the administration of the CDBG Program. This information is collected as part of the beneficiary intake process wherein information that may be used to identify individual beneficiaries is necessary to carry out the program.

DED recognizes its need to maintain the confidentiality of Personally Identifiable Information (PII) and understands that such information is unique to each individual. The PII covered by this policy may come from local government Subrecipients, Subrecipient non-profits or districts, construction contractors, professional service providers and other entities working on a CDBG financed project. The scope of this policy is intended to be comprehensive and will include CDBG requirements for the security and protection of such information throughout the Program (internally) and its approved Subrecipients, as well as all contracted professional service providers, both at the offices in Jefferson City as well as locally at each Subrecipient office and other related entity locations.

2.1.1 Regulations

Enacted in 1974, the Privacy Act (5 USC 552a) establishes controls on personal information collected, maintained and used by the government and it establishes information practices for the transfer, storage and sharing of that information. The Act also provides for requirements of the dealing with personal information including notifying the individuals of the purpose, use and sharing of that information, allowing access to the records to the individuals whose records are retained, conducting privacy reviews, and ensuring key personnel are trained.

The Act limits the retention collection and maintenance of records to only those necessary to accomplish the purpose and that electronic and paper files are safeguarded. The Act extends from HUD to State grantees, and from the State to all local Subrecipients. The Act outlines civil penalties for non-compliance. 24 CFR 214 provides the regulations related to PII. HUD has also produced handbooks, specifically for training housing counseling agencies but much of the information is relevant to State Grantees.

Privacy Act Handbook
https://www.hud.gov/program_offices/administration/hudclips/handbooks/admh/1325.1
HUD's Privacy Principle
https://www.hud.gov/program_offices/officeofadministration/privacy_act/documents/privprin

PIH Notice 2014-10, HUD Privacy Protection Guidance for Third Parties
https://www.hud.gov/sites/documents/PIH2014-10.PDF
The E-Government Act of 2002,
https://www.justice.gov/opcl/e-government-act-2002
Federal Information Security Modernization Act of 2014, (Public Law 113-283; December 18, 2014)
https://csrc.nist.gov/topics/laws-and-regulations/laws/fisma

2.1.2 DED Authority

As the State's administering agency, DED has the delegated authority for developing and implementing procedural guidance for ensuring that their departmental responsibilities under this policy are communicated and enforced and consistent with the law. This compliance requirement applies to DED staff and all Subrecipients, and contracted agents working under a

CDBG grant project.

This policy, as it applies to DED employees, is under-pinned by several DED policies, which include:

- DED Confidentiality Oath – an oath each employee is required to execute which outlines the treatment of confidential information and the disciplinary action for any violations.
- Ethics and Conflict of Interest – policy which ensures all ministerial decisions are made impartially and without conflicts of commitment or interest.
- Personal Accountability and Conduct – policy which addresses penalties for falsifying or altering work records or reports and security and confidentiality of information.
- Acceptable Computer Use – policy which limits all devices to business use only.
- Drug Free Workplace
- Nepotism – policy which outlines guidance for nepotism, relatives, intimate relationships to avoid conflicts of interest or the perception of such.

2.1.3 Subrecipient Responsibility

The protection of PII data applies to all CDBG Subrecipients and contracted agents. Requirements of PII protection must be adhered to and as such are set forth in:

- Grant agreements
- Subrecipient contracts and agreements

2.1.4 Definitions

Privacy Act information is any data about an individual that is retrieved by name or other personal identifier assigned to the individual.

Personally Identifiable Information (PII) is any information about an individual maintained by an agency, which can be used to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual. Examples of PII include name, email, home address, and phone number.

Sensitive Personally Identifiable Information (SPII) is Social Security numbers or comparable identification numbers like a state ID or driver's license number, passport number, alien registration number; financial information including financial account numbers; and medical information associated with individuals such as biometric numbers. The following information, when paired with a second identifier, becomes SPII: citizenship or immigration status, medical information, ethnic or religious affiliation, sexual orientation, account passwords, last four digits of SSN, date of birth, criminal history, and mother's maiden name.

2.2 DATA INTAKE

The typical reasons for collection of data include but are not limited to: proof of income for verification of low and moderate income status, payroll records for labor standards, federal government benefit information for duplication of benefit research, and employment records for economic development projects requiring new job creation.

2.2.1 Training

All new hires entering the DED CDBG Program who may have access to PII are provided with training regarding the provisions of this policy, a copy of this policy and implementing procedures. All new Subrecipient training and annual Administrative Training shall cover PII data as part of CDBG Recordkeeping, according to Chapter 4 Financial Management and Reporting.

2.2.2 Policy Certification

All entities participating with CDBG shall indicate their recognition, acceptance and concurrence with this policy by executing the PII Policy Certification for each individual, including subrecipient staff and its contractors, who are responsible for beneficiary intake and/or the management of files and documentation which may contain PII or SPII. All individuals must provide an executed copy of the PII Policy Certification to DED prior to managing any data falling under the protections of this policy. The existence of a signed copy for all entities will be a monitoring function and non-compliance may cause penalties for future grant awards.

As part of this certification, the subrecipient must identify the contact information for the individual(s) responsible for transferring PII data to DED for review and concurrence.

2.2.3 PII Data Determination

The Subrecipient must determine whether documentation for submission to DED contains PII. The types of SPII collected and maintained by the CDBG Program may include, but is not limited to:

- Social Security Numbers
- Taxpayer Identification Numbers
- Employer Identification Numbers
- State or foreign driver's license numbers
- Date(s) of birth
- Corporate or individually held credit or debit transaction card numbers (including PIN or access numbers) maintained in organizational or approved vendor records
- Address of primary residence

The requirement for the protection of PII data applies to data received or sent electronically, by CD, or in paper record once it is made available to the subrecipient and/or its contractors. All standard practices of redaction and encryption shall apply to CDBG records.

Additionally, unless the specific field of information is necessary for the CDBG staff to administer a function whereas otherwise the data would be held in a protected location in the Subrecipients offices and accessible for inspection upon demand, the default practice should be to redact such information when transmitted or transferred to the CDBG Program.

2.2.4 Data Storage

All PII paper files shall be filed, labeled as Official Use Only, and stored in locked cabinets. Encryption for electronic transfers and virtual storage must include passwords sent separately and storage of such information shall remain separate and labeled as PII so that no individuals other than the subrecipient's certified staff members may access the data. Any PII sent through the regular mail must be double wrapped and marked.

2.2.5 Data Transmission to DED

Subrecipients may submit PII data to DED in one of several formats, although electronic submission should be used unless the subrecipient can demonstrate hardship in complying with that process.

<u>Electronic</u>

PII data must be submitted to DED using the State's file transfer protocol (MoFTP). This encrypted data transfer system will upload PII data into a protected folder on the State server that is rated to accept PII data in compliance with federal regulations. The subrecipient must upload files to the MoFTP, using their individual login provided by the State of Missouri, for submitting PII data. Files must be named individually to be accepted by the FTP system; therefore, files must use the

following naming convention:

<CDBG Project Number> <Beneficiary Name> <Document Name>

2.3 DATA MANAGEMENT

2.3.1 Retention

Retention of documentation which includes PII data is the same as all CDBG grant data and shall be maintained in accordance with all applicable local and state policy, as well as federal regulation.

2.3.2 PII Data Destruction

Any paper documentation containing PII data that is no longer required to be maintained must be destroyed by shredding the original documents and all copies. Digital storage must be erased in such a way that the PII data is not accessible.

2.4 Policy Violations

2.4.1 Data Breaches

Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a data breach, the CDBG Program will notify the DED legal team and implement a notification of all affected individuals whose PII data may have been compromised. The notice will be accompanied by a description of action being taken to reconcile any damage as a result of the data breach. Notices will be provided as expeditiously as possible.

2.4.2 Policy Infractions

Infractions of this policy or its procedures will result in disciplinary actions to employees under the DED discipline policy and may include recommendations to Human Resources for suspension or termination in the case of severe or repeat violations. Discipline to Subrecipients and other contracted agents may include restrictions applied to future grant awards.

2.4.3 Policy Violation Notification

DED must be notified as soon as the subrecipient and/or its contractors realize a violation of this policy has occurred. If an employee has reason to believe that PII data security has been breached or that DED employees, Subrecipients or contracted agents are not adhering to the provisions of this policy, an employee should contact:

Missouri Department of Economic Development
Offices of the General Counsel
301 West High Street, Harry S Truman State Office Building
Suite 680
Jefferson City, MO 65102
573-751-4770

Missouri Department of Economic Development
CDBG Manager
301 West High Street, Harry S Truman State Office Building
Suite 770
Jefferson City, MO 65102
573-751-3600