DCA SUB-RECIPIENT PROCEDURES TO PROTECT PERSONALLY IDENTIFIABLE INFORMATION (PII) FOR CDBG-DR PROGRAMS

In order to carry out CDBG-DR programs, the Department of Community Affairs (DCA) must ensure that sub-recipients 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 sufficiently protected.

This policy has been created in order to communicate DCA's requirements related to the proper handling and securing of Personally Identifiable Information (PII) for sub-recipient administered CDBG-DR programs. The purpose of this policy is to ensure the confidentiality and integrity of PII information provided in a hard copy format and/or electronically stored or transmitted over DCA, sub-recipient, contractor, and/or vendor computer networks and telephone systems.

This policy outlines the methods to collect, document, and properly dispose of applicant hard copy paperwork that contains PII as well establishing acceptable uses and methods of transmission of PII data. All program staff, to include sub-recipient, contractor, and vendor staff, will be provided a copy of the DCA's Sub-Recipient PII policies and will be required to sign an acknowledgement of 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 DCA Sub-Recipient Procedures to Protect Personally Identifiable Information (PII) for CDBG-DR Programs policy.
- Establish protocols should a breach of data occur during the administration of the Sub-Recipient's CDBG-DR Programs

Definition of PII

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 newsletter is not sensitive PII; a list of people receiving treatment for substance abuse is sensitive PII. As well as 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 two 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 in transmitting this data when associated with an individual:

- Place of birth
- Date of birth
- Full Name
- Mother's maiden name
- Biometric information and personal characteristics including; photographic images, fingerprints, handwriting, retina scan, voice signature, and facial geometry
- Medical information, except brief references to absences from work
- Personal financial information (account numbers, award amounts, income, etc.)
- Credit card or purchase card account numbers
- Passport numbers, driver's license number and taxpayer ID
- Potentially sensitive CDBG-DR information related to grant or loan awards (applicant identification number, grant/loan amounts, etc.)
- Criminal history
- Any information that may stigmatize or adversely affect an individual
- SSN and partial SSN do NOT need to be associated with an individual to be considered PII. A SSN or the last 4 digits of a SSN alone, with no other information are considered PII
- In rare cases something like age has been found by the court to be PII. A case where a 99-year-old female's patient information was viewed publicly resulted in a court finding that her age was PII. She was the only 99-year-old female in community. If in doubt, it is necessary to err on the side of caution; treat files, data and information as if it is sensitive 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. In addition, no CDBG-DR staff will be permitted access to any file where there could be a potential or perceived conflict of interest. Access to all CDBG-DR files should be subject to the Sub-Recipient's administrative "Need to Know" policy.

Non-PII

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

- Work phone numbers
- Work addresses
- Work e-mail addresses
- Documents that do not include an SSN or where the SSN is removed
- General background information about individuals found in their application for assistance

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 sub-recipient official authorized to make such determinations.

Procedures for Intake and Processing of Applicant Provided Documentation

Sub-recipients will ensure that all PII discussed with and received from program applicants will be protected. During intake with applicants, case managers must ensure that only required PII be retained by the CBDG-DR program. Only required program documents shall be scanned/filed into the DCA's system of record with original documentation returned to the applicant during the intake meeting. In the event hard copies of the documents are retained for review and use of in the sub-recipient's program, hard copy documents must be labeled confidential and appropriately stored or filed in a secure location until they can be disposed of appropriately. A secure location means that they are locked in the case manager's desk or stored in a locked file cabinet when not in use. In addition, this policy requires that all mail or written correspondence to the applicant must be uploaded into the system of record and/or hard copy file within 24 hours of any notification by regular mail. In addition, all case managers granted access to PII must acknowledge and follow the policies regarding the physical, verbal, and electronic security of PII as outlined below.

Physical Security of PII

Physical security applies to all paper documents or files, as well as CDs, USB drives, tapes, and backups containing PII. DCA requires the following for all items that should be physically secured.

- Access to documents containing PII is limited based on a legitimate business need for the information and document. Only CDBG-DR designated staff shall have access to PII. Sensitive documents shall not be left out when CDBG-DR staff is away from their desk.
- CDBG-DR staff must log off their computers and lock their desks and file cabinets at the end of the day.
- Access to PII shall be limited or not granted for any CDBG-DR staff with an actual or perceived conflict of interest.
- Documents containing PII must be disposed of appropriately when no longer required for the CDBG-DR purpose for which they were collected. Further details on disposal of records can be found below under Document Disposal.
- Documents containing PII should be stored in locked drawer or program file cabinets when not in use.
- Access-control to spaces containing CDBG-DR documents with keyed or electronic locks will be used if locked file cabinets are not in use. Access control may also be used in conjunction with locked file cabinets.
- Files are only to be removed from locked cabinets when in use.
- Keys to secure spaces are controlled and logged/assigned.
- Access Controls given out to staff are logged.
- Management is to review access controls, such as changing locks and combinations upon staff changes.
- CDBG-DR staff should notify sub-recipient management immediately if they see an unfamiliar person on or around any premises that store applicant PII.

Verbal Security

Sub-Recipient, contractor and vendor staff granted access to PII must exercise precautions when discussing PII.

- PII should not be shared with coworkers unless it is required for them to complete their job duties.

- Limit information when leaving voicemail to name of case manager and return phone number.
- No PII should be discussed in public places, such as waiting rooms, hallways, elevators, etc.

Electronic Transmission of PII

Examples of electronic transmission of PII, include, but are not limited to:

- E-mail, text, and instant messages
- Document(s) attached to an e-mail message
- File Transfer Protocol (FTP)
- General Web Services
- File Sharing Services
- Electronic Data Interchange (EDI)

If there is any question concerning the sensitive or non-sensitive nature of the PII, staff should contact the CDBG-DR Program Manager or other authorized sub-recipient official.

Methods of Safe Transmission of PII

Although the transmission of PII is strongly discouraged, there may instances when this type of information must be shared among program staff. If this situation arises during the administration of a CDBG-DR program, there are several methods considered acceptable when transmitting PII:

- Using encryption software to encrypt the sensitive PII before sending it electronically, e.g., as an e-mail attachment. The password key should be forwarded to the recipient in a separate e-mail from the attached file or mailed. (PKZip is not considered a valid solution due to the ability to "break" the encryption).
- Using an application designed to protect the transmission of sensitive PII, e.g., Web- based applications that use TLS1.0, secure file share, or secure file transfer applications such as Secure Shell File Transport Protocol (SFTP).
- Sending documents with sensitive PII by facsimile is permissible if the sender alerts the designated recipient that sensitive PII is being sent. The recipient must then verify by phone or e-mail that the information has been received.
- Transfer of information via secure web applications.
- Transfer of information via Virtual Private Network (VPN).
- FTP in conjunction with encryption unless secure/encrypted FTP protocols have been put into place.

In addition to the above listed protocols, anti-virus and anti-spyware programs on individual computers and on servers on the CDBG-DR network should be regularly run by agency.

Password Management

This policy also requires that CDBR-DR sub-recipient, contractors and/or vendor staff control access to sensitive information by requiring the use of "strong" passwords, i.e. a mix of letters, numbers, and characters.

Passwords to sub-recipient's CBDG-DR system(s) should be frequently changed.

In addition, this policy requires the following in the execution of CDBG-DR activities:

- Sharing passwords or posting them near CDBG-DR workstations is not permitted.

- Password-activated screen savers must be used to lock staff computers after a short period of inactivity.
- Users who don't enter the correct password within a designated number of logon attempts should be locked out of the CDBG-DR system.

Acceptable Methods for Disposal of CDBG-DR PII

This policy requires all CDBG-DR sub-recipient, contractor, and vendor staff to properly dispose of sensitive information so that it cannot be read or reconstructed. Acceptable disposal methods are as follows:

- Paper Shredding / shred boxes
- Burning
- Pulverizing
- Electronic Media- If the media cannot be physically destroyed like a CD or DVD, data wiping software that permanently removes the PII data from the storage device must be used
- CDs and DVDs can be shredded or burned

In order to effectively carry out these procedures the following must occur:

- Document shredders and/or shred boxes should be made available throughout the workplace, including near the photocopier.
- Disposal of computers and portable storage devices must include the use of software for securely erasing data and hard drive so that the files are no longer recoverable.

PII Security Practices of Program Contractors and Sub-recipients

All CDBG-DR contracts or grant agreements with DCA will require that all sub-recipients, contractors and vendors adopt and properly administer DCA's Sub-Recipient Procedures to Protect Personally Identifiable Information (PII) for CDBG-DR Programs policy. Failure to effectively carry out these policies or any breach of information may cause DCA to terminate the sub-recipient's contract or grant agreement. In addition, DCA requires that all sub-recipients, program contractors, and vendors maintain files and procedures regarding:

- Reference or background checks conducted prior to onboarding CDBG-DR staff who will have access to sensitive data.
- Staff review and acknowledgement of DCA's PII policy.
- Restricting access to CDBG-DR PII to a limited number of staff.
- Identification of staff with an actual or perceived conflict of interest. Identified staff shall not be granted access to information or PII that is the source of the conflict of interest.
- Zero tolerance policy related to the release of any applicant provided information without written consent of the applicant.
- PII Training provided to CDBG-DR sub-recipient, contractor, and vendor staff.
- Procedures in place for ensuring that CDBG-DR sub-recipient, contractor, or vendor staff who leave the project or employment no longer have access to sensitive information, i.e. timely termination of passwords, and collection of keys and identification cards as part of the out-processing routine.

DCA's Community Finance Division will conduct an initial monitoring of all CDBG-DR sub-recipients for compliance with these policies and procedures. In addition, PII security will be regularly monitored by DCA.

CDBG-DR PII Training

The DCA Community Finance Division will conduct broad level initial PII training for all CDBG-DR sub-recipient management staff. Sub-recipients will then be responsible for conducting PII training with all staff, including contractor and vendor staff, as necessary.

In addition to PII training, DCA requires:

- All Chief Elected Officials read and acknowledge understanding of this document by affixing signature to Exhibit A: Protection of Personally Identifiable Information (PII) Policy Agreement (Elected Official Acknowledgement) and ensure that:
- All CDBG-DR sub-recipients, contractors, and vendor staff must read this policy and acknowledge understanding of this document by affixing signature to Exhibit B: Protection of Personally Identifiable Information (PII) Policy Agreement (Subrecipient Acknowledgement).
- Any suspicious activity shall be immediately reported to sub-recipient management and forwarded to DCA.

Compromises of PII Security

All compromises or potential compromises of PII security shall immediately be reported, by sub-recipient management staff, to the Director of the Community Finance Division in order to assess the situation and determine the appropriate action to be taken.

Division Director, Community Finance Division CDBG-DR@da.ga.gov

In addition, the following steps should be taken:

- Immediate investigation of the security incident and termination of any existing vulnerabilities or threats to personal information.
- Any compromised computer should be immediately disconnected from any CDBG-DR network.
- Suspension of access to physical or electronic information for any staff suspected of creating a breach of PII security.

The Director of the Community Finance Division will be responsible for notifying all appropriate DCA departments, affected applicants, and law enforcement agencies, as applicable. In addition, the Director will be responsible for the termination of any contracts or grant agreements as determined necessary.

Responsible Agency

The Sub-Recipient will be responsible for the administration and enforcement of DCA's Sub-Recipient Procedures to Protect Personally Identifiable Information (PII) for CDBG-DR Programs to ensure that all CDBG-DR sub-recipient, contractor, and vendor staff understand, acknowledge, and comply with the policy in order to adequately protect applicant PII. The Community Finance Division will be responsible

for ensuring that all sub-recipient contracts and grant agreements contain references and strict adherence to these policies. In addition, the Community Finance Division will monitor all sub-recipients for compliance with PII requirements and provide training and technical assistance as necessary.