COMMUNITY PLANNING & DEVELOPMENT

Overview of Computer Matching Agreements and Data Sharing Agreements for CDBG-DR and CDBG-MIT Grantees

Purpose of this Training

- The longstanding data sharing agreement between FEMA with HUD and CDBG-DR grantees has been revised to address privacy-related issues identified in the applicable FEMA System of Records Notices (SORN). HUD worked with FEMA on a computer matching agreement (CMA) to ensure that HUD grantees will get the latest Individual Assistance program data from FEMA in order to build out their impact and unmet needs assessment, market their programs to potentially impacted individuals, and complete their duplication of benefits analyses for individual benefits.

I. Computer Matching Agreement (CMA)

Training Objectives

- Understanding the purpose of the CMA
  - Authorized use of data
- Reviewing the approval process of the CMA
  - Publishing of the agreement
  - Applicability date of the agreement
  - Renewal process for the agreement
- Grantee request for data from HUD
  - Grantee Authorized Users
  - Independent verification of data by grantee
- Overview of the requirements related to the use and protection of the data

The Purpose of the CMA

- Governs the grantee's use of the shared FEMA data in the administration of CDBG-DR and CDBG-MIT grants
- Supports duplication of benefits checks conducted by grantees for CDBG-DR grant-funded programs
- Expedites the recovery process with immediate availability of data, once the CMA is signed and effective

Authorized Use of Data

- The agreement covers data sharing for the purpose of determining individual benefit amounts for approved activities under the grantee's approved CDBG-DR Action Plan
- Grantees will conduct computer matching with the data provided by HUD to ensure that CDBG-DR assistance provided to grantee program applicants is not duplicative of FEMA assistance received by the grantee program applicant
  - The grantee has the responsibility to prevent the duplication of benefits using the data provided
  - For each grantee program applicant, the grantee will use the amount of FEMA assistance received by the grantee program applicant to calculate the grantee program applicant's unmet need and calculate a maximum award amount

Computer Matching Agreement

- The grantee and HUD sign the CMA
  - The summarized agreement is published in a *Federal Register* notice and must allow for a 30-day public comment period
  - HUD addresses any public comments that may result from the publication in the *Federal Register* notice and if significant changes to the notice are necessary, HUD shall publish a revised notice and provide an additional 30-day public comment and review period
  - The agreement takes effect 30 days from the date the final agreement is published in the *Federal Register* notice

CMA Extensions

- The CMA is valid for 18 months
  - Grantees can receive one 12-month extension on their CMA
  - The extension must be requested and occur within 3 months of the expiration date of the CMA
    - A grantee would request an extension by sending an email to the grant manager 90 days prior to the expiration of the agreement
  - Renewals are subject to the requirements of the Privacy Act including certification by grantee and HUD that the matching program will be conducted without change and conducted in compliance with the original Agreement

Termination of the CMA

- The grantee's CMA will terminate when the purpose of the computer match has been accomplished, or after 18 months from the effective date of the Agreement, unless an extension has been granted

- The Agreement may also be terminated, nullified, or voided by either the grantee or HUD if:
  - Either party violates the terms of the Agreement
  - The grantee or its authorized users misuse or improperly handle the data provided by HUD
  - The grantee and HUD mutually agree to terminate the Agreement prior to its expiration after 18 months
  - Either agency provides the other with 30 days written notice
  - The HUD-FEMA computer matching agreement pursuant to which HUD may request data from FEMA is terminated

Process for Requesting FEMA Data

- Grantees will request FEMA data from HUD on an “as needed” basis. The request must be based on specific program requirements specified in the grantee's approved Action Plan
  - The grantee will email the grant manager to make the request for the data and submit a data request template
  - The grant manager will ensure all information is correct on the data request template
  - The template will then be sent to HUD’s Office of Policy Development and Research (PD&R) to request the data from FEMA
  - Once FEMA provides the data, the data will be made available to the grantee via a password protected email

Authorized Users

- Authorized Users are employees, agents (including contractors or subcontractors), or subrecipients (including an agent or employee of its subrecipients) who have entered an agreement with the grantee to comply with all requirements on the use of data contained in the CMA and acknowledged 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

- Authorized Users will have signed an enforceable agreement with the grantee that when given access to the subject HUD database or file, the Authorized User will not:
- Use or reveal any individually identifiable information furnished, acquired, retrieved or assembled by the Authorized User or others for any purpose other those in the CMA;
- 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; or
- Permit anyone other than the Grantee's Authorized Users to access the data
- A grantee will not authorize more than the number of Authorized Users of data that the Grantee determines is necessary to accomplish the purposes of the use of the data outlined in the CMA

Independent Verification of Data

- Grantees and their authorized users will perform an independent verification of the information obtained in a match before taking an adverse action
  - The grantee will comply with its policies and procedures for verifying the matched FEMA data and for allowing individuals to contest benefit determinations
  - Individuals must be given at least 30 days to contest the grantee's findings before any adverse action can be taken by the grantee

Addressing Duplication of Benefits

- To comply with the Stafford Act and appropriations acts, grantees must prevent the duplication of benefits and must have adequate policies and procedures for this purpose

- If the grantee discovers an individual is receiving benefits through both HUD's CDBG-DR/CDBG-MIT and FEMA assistance programs, the grantee will be responsible for addressing the duplication of benefits non-compliance, if there is any

Additional CMA Requirements

Records Retention Requirements

- Grantees will retain FEMA data received from HUD under the CMA only for the processing time required to verify the data, which is typically until grant closeout

- FEMA data obtained by the grantee but not used must be deleted after application processing is complete

Data Security Safeguards

- Grantees must comply with the existing and future requirements set forth by the Privacy Act
- Grantees are responsible for all individuals who have access to data and must:
  - Restrict access to the data to only authorized users
  - Confirm that their authorized users receive training to ensure proper information security and privacy protections are adhered to in a manner consistent with the Agreement
  - Advise anyone with access to the data of the confidential nature of the data and the safeguards required to protect the data
  - Notify authorized users of the civil and criminal sanctions for noncompliance contained in the applicable federal laws

Technical Data Security Safeguards

- Grantees must employ appropriate technical, physical, and administrative safeguards to secure all FEMA applicant PII shared under the Computer Matching Agreement, whether in physical or electronic form, only in places and in a manner that is safe from access by unauthorized persons or for unauthorized use

Technical Data Security Safeguards, cont.

- To ensure the security of the data, grantees must:
  - Ensure compliance with applicable laws including but not limited to FISMA and associated NIST standards
  - Ensure that any cloud-based system that stores, analyzes, processes, or uses FEMA PII has an Authority to Operate (ATO) approved by the Federal Risk and Authorization Management Program (FedRAMP)
  - Ensure that every IT system that stores, analyzes, processes, or uses FEMA PII, regardless of configuration or location, undergoes routine cybersecurity scans and has a valid ATO

Incident Reporting and Notification Responsibilities

- Grantees must track and report all potential PII security incidents and must:
  - Promptly notify the HUD National Help Desk by calling 1-888-297-8689 or the HUD Help Desk at (202) 708-3700 if unable to reach HUD's Security System Contacts within one hour of the incident or if the incident occurs outside of normal business hours
  - Conduct a breach and risk analysis and determine the need for notice and/or remediation to individuals affected by the loss
  - Provide notice and credit monitoring to the affected individuals at no cost to HUD

II. Data Sharing Agreement (DSA)

Training Objectives for DSA

- Understanding the purpose of the DSA
  - Authorized use of data
- Discerning the effective date, the duration and the termination of the agreement
- Reviewing the grantees responsibilities as defined in the agreement
  - Use and maintenance of the data
  - Identifying grantee authorized users
  - Grantee authorized user access requirements
- Establishing and implementing minimum standards for access and storage of data
  - Protection and storage of PII data
- Complying with privacy incident handling requirements

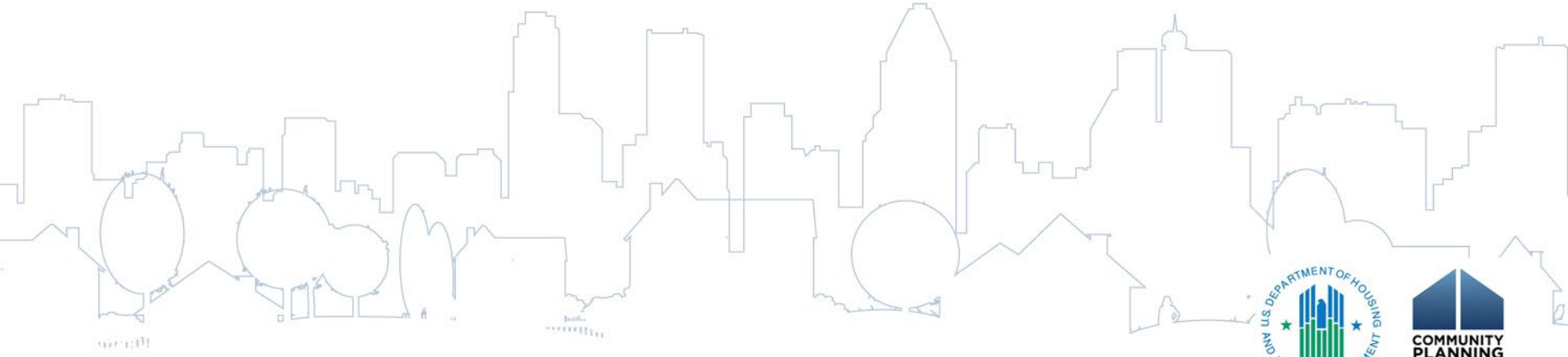
The Purpose of the DSA

- The purpose of the DSA is to enable HUD to share with the grantee the data it receives from FEMA, including personally identifiable information (PII) that is protected by the Privacy Act of 1974 (Privacy Act), as amended, 5 U.S.C. § 552a, for two purposes:
  - To assess unmet needs resulting from major disasters in which grantees receive a CDBG-DR allocation, including funds for mitigation or resilience purposes awarded as CDBG-MIT or CDBG-NDR grants; and
  - To market activities to potential applicants that may be eligible for assistance funded by the Grant(s)
  - NOTE: The DSA cannot be used for checking for duplication of benefits or for determining individual eligibility

Terms of the Agreement

- The DSA will become effective upon the signature of both HUD and the grantee and will remain in effect until the closeout of the last grant for which the grantee receives data under the agreement

- Either HUD or the grantee may terminate the agreement upon written notice to the other party



Grantee's Responsibilities

- The grantee must use and maintain the data it receives under the DSA only for assessing the unmet needs of approved disasters and plan for the use of one or more CDBG-DR grants, including funds for mitigation or resilience purposes awarded as CDBG-MIT or CDBG-NDR grants; and to market activities to potential applicants that may be eligible for assistance funded by the Grant(s)

- The grantee must limit access to the data to only Authorized Users

Grantee's Authorized Users

- The grantee must identify to HUD the Authorized Users of data received under this DSA
  - Authorized Users are employees, agents (including contractors or subcontractors), or subrecipients (including an agent or employee of its subrecipients) who have entered an agreement with the grantee to comply with all requirements on the use of data contained in the DSA
  - HUD may periodically request that the grantee update its list of Authorized Users and revoke access to individuals that are not identified as Authorized Users
  - HUD will prohibit data access to data on its systems by any individual that is not identified by the grantee as an Authorized User

Grantee's Authorized Users, cont.

- The grantee's Authorized Users must sign an enforceable agreement with the grantee when given access to the HUD database or file. The agreement acknowledges that under the Privacy Act, unlawful disclosure of PII data is a misdemeanor and subject to a fine of up to $5,000
- The agreement prohibits Authorized Users from:
  - Using or revealing any individually identifiable information furnished, acquired, retrieved or assembled by the Authorized User or others for any purpose other the purposes stated in the DSA,
  - Making 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, and
  - Permitting anyone other than the grantee's Authorized Users to access the data

Protecting and Securing Data

- The grantee must establish and implement minimum standards to:
  - Encrypt and store the applicant PII that is protected by the Privacy Act, whether in physical or electronic form, in a secure manner consistent with this type of data, and only in places and in a manner that is safe from access by unauthorized persons or for unauthorized use

    - At a minimum, access to the data maintained in computer memory must be controlled by password protection and all printouts, CD-ROMS, or other physical products containing PII derived from the data must be locked in cabinets, file drawers, or other secure locations when not in use

Protecting and Securing Data, cont.

- Take reasonable precautions to ensure that only Authorized Users have access to PII data, that PII data is encrypted prior to allowing authorized users access, and that authorized users only access PII data with an officially sanctioned application for the purposes described in the DSA

- Instruct all Authorized Users regarding the confidential nature of the information, the requirements of the Agreement, and the criminal penalties and civil remedies specified in federal, state, and local laws against unauthorized disclosure of PII covered by the Data Sharing Agreement, and require Authorized Users to take any mandatory training offered by HUD regarding proper information security and privacy protections

Protecting and Securing Data, cont.

- To ensure protection of the data received, grantees must also:
  - Employ appropriate technical, physical, and administrative safeguards to secure any and all PII shared under the provisions of the DSA, whether in physical or electronic form. PII is only permitted to be used in places and in a manner that is safe from access by unauthorized persons or for unauthorized use
  - Prevent disclosure of PII provided under the DSA to any person or entity that is not an Authorized User

Protecting and Securing Data, cont.

- Edit all printouts, tabulations, and reports to ensure they do not contain unauthorized disclosures of data provided under the DSA
- Destroy the data provided under the DSA for any Major Disaster(s) at the time of closeout of the Grant that assists the Major Disaster(s) for which the data was provided and notify HUD when the data provided under the agreement is destroyed. Where recordkeeping periods extend beyond grant closeout, the grantee shall retain records of decisions based on the use of the data for the recordkeeping period required by the Grant(s)
- Submit to monitoring or inspection by HUD
- Establish and implement policies and procedures to comply with the requirements of the agreement

Privacy Incident

- In the event of a breach of the DSA or any exposure, unauthorized release, or misuse of PII shared under the provisions of the DSA, the grantee will immediately report the incident to the HUD Privacy Officer

- 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

Helpful Resources

- The Privacy Act: https://www.justice.gov/opcl/privacy-act-1974
- HUD's Privacy Website: https://www.hud.gov/program_offices/officeofadmininistation/privacy_act/pia/polyref
- DSA and CMA data sharing resources: https://www.hud.gov/program_offices/comm_planning/cdbg-dr/data-sharing