Personally Identifying Information Policy

I. Introduction

A. Overview

The Emergency Solutions Grant (ESG) Program is a federal program operated by the U.S. Department of Housing and Urban Development (HUD) to make grants to states, local governments, and territories for the purposes of funding activities that directly serve people experiencing homelessness, including people at risk of homelessness. The California Department of Housing and Community Development (CA HCD) is a direct recipient of ESG from HUD. CA HCD administers an annual allocation of ESG and an additional one-time allocation of ESG made available under the CARES Act.

For the purposes of this document, "annual ESG" refers to CA HCD's annual allocation of ESG, "ESG-CV" refers to CA HCD's one-time allocation of CARES Act ESG, and "ESG" refers to the program in general and to aspects of the program that apply to both annual ESG and ESG-CV.

This ESG Personally Identifying Information Policy (the "Policy") provides comprehensive guidance on that subject to ESG projects.

B. Applicability

This Manual applies to ESG grants funded using:

- Annual ESG
- ESG-CV

II. General Requirements

A. Overview

The ESG Program's primary regulatory body is 24 CFR Part 576, the ESG Program Interim Rule.[1] The ESG Program Interim Rule requires that recipients (e.g. CA HCD) and subrecipients (including 'sub-subrecipients) ensure the following:[2]

- All records containing personally identifying information [PII] […] of any individual or family who applies for and/or receives ESG assistance will be kept secure and confidential;

[1] https://www.hudexchange.info/resource/1927/hearth-esg-program-and-consolidated-plan-conforming-amendments/

[2] 24 CFR 576.500(x)

- The address or location of any domestic violence, dating violence, sexual assault, or stalking shelter project assisted under ESG will not be made public except with written authorization of the person responsible for the operation of the shelter;
- The address or location of any housing of a program participant will not be made public, except as provided under a preexisting privacy policy of the recipient or subrecipient and consistent with state and local laws regarding privacy and obligations of confidentiality.

This requirement's functional impact is **recipients and subrecipients must develop confidentiality policies and procedures in writing to keep confidential every ESG applicant's or participant's personally identifiable information (PII) they receive for any reason, including participant housing locations/addresses, as well as the locations/addresses of any domestic violence shelters.** Addressing this requirement is the primary purpose of this Policy.

B. Defining and Identifying Personally Identifying Information

PII is defined by OMB M-07-116, "Memorandum for the Heads of Executive Departments and Agencies, as follows:

> "Information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual."

PII is sometimes also called "personally identifiable information," "personal protected information" or PPI, and other similar terms and acronyms.

Some examples of PII include:

When Alone	When Combined w/Other PII
Names	Date and place of birth
Social security numbers	Race or ethnicity
Drivers license numbers	Religion
Patient ID numbers	Geographical indicators
Addresses	Financial information
Personal telephone numbers	

Biometric data	

Further, sensitive personally identifying information (SPII) is defined in HUD's April 2015 "Protecting PII: Capacity Building Guidance on Protecting Privacy Information" as follows:

> "PII that when lost, compromised or disclosed could substantially harm an individual."

Some examples of SPII include social security numbers, medical records, credit/debit/bank account information, immigration status, criminal records, medical information, and any information that could be used to locate a person fleeing domestic violence.

There is no comprehensive list of every piece of information that is PII or SPII. Instead, recipients and subrecipients must assess each participant record to determine whether it contains information that, either alone or when combined with other information in the record, constitutes PII or SPII.

C. Locating Personally Identifying Information

PII can be found in any record containing participant information, and those records can in theory be found, stored, or accidentally left in any physical or digital location. For the purposes of the ESG program, PII is most often located in one of the following places:

- In HMIS;
- In a physical participant file;
- On a computer or other digital media (e.g. thumb drives, external hard drives);
- In long term physical storage.

However, PII is PII no matter where it is located, how you store it, or how well you secure it. Recipients and subrecipients must assess each ESG program record they generate or receive to determine whether they contain PII.

For service providers, the most common PII collection points are:

- Upon first contact with a participant
- At project intake
- At lease-up

The confidentiality protections in this policy do not extend to employees whose salary is paid for by ESG. Staff information, including names and salaries, is commonly shared between recipients and subrecipients, including during the grant application, contracting, and reimbursement request processes.

- During the case management process (e.g. case notes)
- At lease renewal and recertification
- At project exit

D. Protecting Personally Identifying Information

Subrecipients are required by this Policy to develop policies and procedures for protecting PII in accordance with the principles in this section. (CA HCD's policies and procedures for protecting PII are established in Section IV of this Policy.)

Most of the information in this section of this Policy is drawn from HUD's April 2015 "Protecting PII: Capacity Building Guidance on Protecting Privacy Information" guidance. For more information, please refer to that document.

1. Limit Collection

Do not collect PII unless you need it to meet a requirement.

When you collect PII, only collect the information you need.

Make sure you are authorized to collect the PII you are collecting. Authorization can come either from an internal authority (e.g. your supervisor), an external authority (e.g. a statute or regulation, written standards), or your organizational obligations (e.g. contracts, non-disclosure and confidentiality agreements).

2. Manage Access

Only share or discuss PII on a 'need to know' basis.

Never discuss or release PII without authorization.

Before discussing PII over the telephone or a video call, confirm that you are speaking to the right person and inform them that the conversation will include PII.

Avoid discussing PII if there are people around who aren't authorized to hear it.

Hold meetings where PII might be discussed in in secure spaces.

Treat meeting minutes and notes as confidential until and unless you can verify that they do not contain PII.

For meetings that do include PII: record their date, time, place, subject, chair, and attendees.

Do not leave PII in a voicemail.

Do not text PII.

Do not send PII via unencrypted email or between email servers that do not share security protocols.

3. Protecting Physical Files

Clearly label all files containing PII.

Store all files in in lockable storage containers (e.g. lockable file cabinets). Lock them when not in use.

Do not leave PII in open areas unattended.

Do not access records containing PII except in work areas that are secure.

Develop a centralized record of where PII is stored. Develop a policy that specifies when and how you will periodically check that the storage is secure and the record is correct.

Treat external digital media (e.g. thumb drives, external hard drives) the same as physical files.

4. Protecting Electronic Files

Develop a policy that specifies where files containing PII will be stored in your digital filing system. Include information regarding when and how you will periodically check that PII is being stored in accordance with the policy.

Clearly distinguish between files that do and do not contain PII.

Consult with your organization's information technology experts to deploy appropriate security measures (e.g. file and digital media encryption, two factor authentication, limiting which users can access files containing PII).

5. Additional File Protection Guidance

Do not remove PII from authorized facilities without approval from an appropriate party (preferably in writing).

Do not use interoffice or translucent envelopes to send PII within or between agency facilities; instead, use sealable (and sealed) envelopes marked to the recipient's attention.

Double-wrap any envelopes sent through via the United States Postal Service (USPS) or equivalent service and mark them as confidential to the recipient's attention.

Require a signature from the recipient when sending PII via courier or equivalent service.

6. Electronic Transmissions of PII

When faxing PII: use date stamps, confirm the recipient's fax number, confirm the recipient is available to receive the fax, and confirm that they receive the fax. Also, ensure that your fax

machine does not store a record of the transmission that renders PII retrievable, shred your physical copy of the transmission once you have confirmed it arrived, and, whenever possible, use a fax machine with a secure transmission line.

When emailing PII: confirm the recipient's email address, confirm receipt of the email, and whenever possible, send PII exclusively between two secure (encrypted) email servers. (Consult with your organization's information technology experts if you aren't sure.)

If you must send PII to an unencrypted email server, ensure that the PII is contained within an encrypted file attached to the email.

Do not store PII on shared drives, calendars, your intranet, or any unsecured or publicly accessible location on the internet.

7. Record Management, Retention, and Disposal

Do not maintain records for longer than required (by statute, regulation, or contract) unless there is a compelling reason to do so and unless the extended period of retention is approved by the appropriate person within your agency. (For the record retention period for ESG participant information, refer to 24 CFR 576.500(x-z).)

Once you have determined that a record can be disposed of, destroy the record permanently. Physical records should be shredded. Electronic records should be permanently erased; for more information about how to permanently erase an electronic record, consult with your information technology experts.

8. Data Breach Response

A data breach means that PII has been viewed by, leaked to, or accessed by someone who was not authorized to view, access, or receive it.

Responses will depend on the nature or severity of the breach, but in general and at minimum should involve re-securing the information.

HUD requests that ESG recipients and subrecipients report any breaches or suspected breaches of SPII within the ESG program to HUD's National Help Desk at 1-888-297-8689.

III. Subrecipient-Specific Requirements

A. Overview

Subrecipients are required to develop a policy that meets the following requirements:

- In general, the policy must provide for how the subrecipient will secure and keep confidential any participant PII it receives for any reason;

- The policy must incorporate every element of Section II.D. of this Policy that states that an entity "must" or "shall" take a specific action, or is otherwise clear and specific that an entity must take a specific action.

Further, CA HCD strongly encourages subrecipients' policies to incorporate every element of Section II.D. of this Policy that states that an entity "should" take a specific action.

Subrecipients are required to monitor their subrecipients (sometimes referred to as "sub-subrecipients") to ensure that their sub-subrecipients have policies that meet the requirements of this section of this Policy.

B. Redacting PII

Subrecipients are required to redact all PII on all documents submitted to their grantors unless their grantor explicitly requests an unredacted document. This includes but is not limited to documents submitted as part of the monitoring process, including client files.

"Redacted" means that PII has been permanently erased, covered, or removed such that it cannot be retrieved by anyone in possession of the document. This is often accomplished by using correction fluid, correction tape, or an opaque black marker.

Note that when using an opaque black marker, a single layer is often not sufficient to completely redact a file. Instead, a file should be redacted using an opaque black marker, scanned, printed, and redacted a second time; the second redaction should permanently remove all redacted PII.

IV. CA HCD-Specific Requirements

A. Overview

In general, CA HCD has adopted the recommendations in Section II.D. of this Policy. Those recommendations have been codified as specific procedures in this section of this Policy. CA HCD staff working on the ESG Program are required to adhere to the procedures in this section of this Policy.

B. Requirements

Do not collect PII unless you are required to do so by HUD, CA HCD policy, your supervisor, or an existing contract or grant agreement. When you collect PII, only collect the information you need to meet the aforementioned requirement. Do not collect PII unless you are explicitly authorized to do so in one of the following ways:

- As part of a routine job duty that is part of your position description that requires the collection of PII (e.g. subrecipient monitoring);
- As part of an irregular job duty, you are assigned in writing by your supervisor that requires the collection of PII;
- As otherwise authorized or required in writing by your supervisor.

Do not discuss or release PII to any party without authorization from your supervisor.

Before discussing PII, ensure that you are speaking to the right person; this is especially important during remote meetings when you cannot see the person you are speaking to. Hold meetings involving PII in secure spaces, which can include online spaces where all participants are visible and known. If you are meeting with any person (inside or outside CA HCD) who might not be authorized to receive the PII in question, inform them that the conversation will include PII and provide them an opportunity to excuse themselves. Treat meeting notes as confidential until you have reviewed them and determined they do not contain PII. For meetings that include PII, record their date, time, place, subject, chair, and all attendees.

Do not leave PII in a voicemail. Do not text PII. Do not send PII via instant messenger except via Microsoft Teams to someone who is authorized to receive it. Do not place PII on a calendar, in an unsecured shared drive, or in any unsecured location on the internet. Do not send PII to an unencrypted email server; if you are unsure whether a destination email server is encrypted, consult with the appropriate CA HCD information technology experts.

When emailing PII: confirm the recipient's email address in advance and confirm their receipt of the email after you have sent it.

When faxing PII: confirm the recipient's address and that the recipient is ready to receive the transmission, confirm their receipt of the transmission, destroy your copy of the transmission after it has been received, and erase any record of the transmission within the fax machine. Whenever possible, use a fax machine with a secure line.

Do not remove physical files or external digital media containing PII (e.g. thumb drives, external hard drives) from CA HCD facilities without authorization in writing from your supervisor. Do not send physical files or external digital media containing PII via USPS or any mailing service except courier. When using a courier, use a double-wrapped opaque envelope, address the package to the recipient's attention, and require the recipient's signature upon delivery.

Clearly label all files containing PII. Store all files in a lockable storage container, which may include a lockable filing cabinet, regardless of whether you are working from a CA HCD facility or from a remote location. Lock them when not in use. Do not leave PII unattended outside a lockable storage container. Do not access PII except in a secured area of a CA HCD facility or from a remote location where you can ensure no one without authorization can access it.

CA HCD shall develop a centralized record of where physical PII is stored at CA HCD facilities and in long term storage. CA HCD shall review the centralized record at least annually to ensure that the record matches actual storage.

CA HCD shall develop an electronic filing system for storing digital PII records. CA HCD shall develop a centralized record of where digital PII records are stored. CA HCD shall review the centralized record at least annually to ensure that the record matches actual storage. CA HCD shall further review this procedure with each CA HCD staff person involved with the ESG Program at least annually to ensure they are correctly implementing it.

CA HCD shall, whenever possible, encrypt all digital records containing PII. CA HCD shall, whenever possible, implement two factor authentication to access any digital record containing PII.

The period of record retention for ESG is enumerated in 24 CFR 576.500(y). For any record containing PII: after that record's period of retention has expired, that record should be permanently destroyed unless there is a compelling reason to retain it and a period of extended retention is approved by someone with supervisory authority. Records shall be destroyed in accordance with standard CA HCD policies and procedures.

In the event of an internal data breach (i.e. a data breach instigated by or beginning with a CA HCD staff person) as defined in this Policy, CA HCD shall take the following actions:

- Determine the nature and extent of the breach;
- Re-secure the information to the extent possible by retrieving records, destroying copies, overseeing the process for permanently digitally erasing records, etc.;
- Consult with the appropriate legal authority at CA HCD to determine what information should be disclosed about the breach to external stakeholders, including participants, and to what extent;
- Act as quickly as possible in accordance with the legal advice provided in response to the above.

In the event of a data breach involving a CA HCD subrecipient, CA HCD shall:

- Work with the subrecipient to determine the nature and extent of the breach;

- Ensure the subrecipient is following their internal processes related to ESG data breaches;
- Consult with the appropriate legal authority at CA HCD to determine any additional actions that CA HCD or the subrecipient should take;
- Act as quickly as possible in accordance with the legal advice provided in response to the above, including encumbering subrecipients with any applicable or appropriate requirements.

Appendix A: Changelog

Date Effective	Description
5.11.2022	Updated draft into new format