COLLECTING AND PROTECTING DISASTER SURVIVOR'S INFORMATION

FEMA employees, FEMA Corps, and DHS Surge Capacity Workforce are required to safeguard Personally Identifiable Information (PII) and Sensitive PII (SPII) that is collected from Disaster Survivors.

What is PII/SPII? PII is any information that is linked or linkable to a Disaster Survivor. SPII is a subset of PII, which if lost, compromised, or wrongly disclosed could cause substantial harm to an individual. Examples of PII: name, contact information, and photo. Examples of SPII: Social Security Number and bank account/routing number.

What type of PII/SPII can I collect? You should only collect what is authorized. To ensure you are only collecting what is authorized, you should limit what you collect to what is on the approved collection instrument, for example, the Registration Intake form. Don't over collect PII.

Can I email a Disaster Survivor's PII? When emailing Disaster Survivor's sensitive information, save the information in a separate document and encrypt it with a password. Send the password protected document as an email attachment and then provide the password in a separate email or phone call. Never put SPII in the body or subject line of an email and never email PII to or from a personal email address. Emails containing PII should only be sent to those with a need to know. Avoid faxing SPII; instead, scan the document, password protect it, and email it.

What do I need to know to avoid mishandling PII? As a FEMA representative, you must take steps to ensure that you protect what you collect. Physically secure hard copies of documents containing PII in a locked file drawer, cabinet, or safe. Do not leave documents with PII unattended on printers, fax machines, copiers, or desktops. Cross-shred paper containing PII; do not recycle or place in garbage containers.

How should documents containing PII be stored on shared drives? Only store PII on shared drives if access can be restricted to persons with proper authorization. Encrypt documents and folders containing SPII.

What should I do with my mobile device when I am off duty? Keep mobile devices with you; if you must leave them at a hotel or in a car, lock them in the trunk or in a safe so they are secured and out of sight.

Instructions for encrypting a Word document with a password: 1) Save the file; 2) Select file; 3) Select password protect; 4) Select encrypt with password; 5) Enter password; 6) Enter password again; 7) Resave file; 8) Close file; and 9) Open file and test password before sending.

Can I share PII? Sharing PII outside of FEMA can only be done lawfully pursuant to a Privacy Act Routine Use, Written Consent, and/or other legal agreement. Please confirm with your supervisor, counsel, and/or FEMA Privacy Office before sharing PII.

Report suspected or confirmed privacy incidents to: 1) FEMA Privacy Office at FEMA-Privacy@fema.dhs.gov or by phone at 202-212-5100; 2) your supervisor; and 3) IT Helpdesk (if IT related) at FEMA-SOC-INCIDENT-REQUEST@fema.dhs.gov or by phone at 540-542-4762.

The goal of every FEMA employee is to maintain the trust of survivors by properly handling their information.

(Update: 10/06/2016)