Personal Identifiable Information Policy

Overview

<<INSERT ORG NAME>> recognizes the need to maintain the confidentiality of Personal Identifiable Information (PII) and understands that such information is unique to each individual. The PII covered by this policy may come from various individuals performing tasks on behalf of the organization including employees, volunteers, interns, and independent contractors. This policy includes requirements for the security and protection of such information throughout the organization both on and off premises.

Personal Identifiable Information (PII): Unique information that can be used on its own or in combinations with other information to identify an individual. PII may reside in hard copy or electronic records; both forms of PII fall within the scope of this policy.

- If disclosed, it could harm a person whose name/identity is linked to the information.
- Examples of PII: SSN, Credit Card Numbers, Bank Account Numbers, Home Telephone Numbers, Birthdates, Marital Status, Spouse's Name, Biometric Identifiers (fingerprints), Medical History, Financial Information, Passwords.

***Sensitive Information*:** Some information is not formally designated as PII but could be if multiple elements together could expose someone to risk.

- Unclassified information whose loss, misuse, or unauthorized access could adversely affect programs or the privacy of individuals.
- Examples: E-Mail Addresses, Business Addresses, Business Telephone Numbers, General Education Credentials, Gender, or Race.

Policies

Responsible Staff: <<INSERT RESPONSIBLE STAFF MEMBERS>> , in conjunction with the management team is responsible for the below PII policies.

Data Breaches/ Notification: Databases or data sets that include PII may be breached inadvertently or through wrongful intrusion. Upon becoming aware of a breach, the organization will notify all affected individuals whose PII 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 no later than 60 days following the discovery.

Confidentiality Expectations: All staff, interns and volunteers are required to maintain the confidentiality of PII as well as company proprietary data to which they have access. PII is restricted to those with need to know. Staff, interns, and volunteers also receive training on confidential nature of PII, and on how to protect the information. All staff, interns and volunteers are reminded that conversations can contain PII too. Be careful where you are and who you are around when you are discussing PII – on the phone or in person.

Physical Access to PII: TI's staff offices are protected by the security personnel and physical access controls. Cabinets in offices or the file room are expected to be locked when not in use.

Physical files should remain on-site whenever possible. If a file is to be removed to provide a service to a client off-site, the Supervisor should be aware of the file and intended return date of the file.

Online Access to PII: All staff members are required to use organization issued computers and equipment for collecting and storing sensitive data. All documents with PII must be saved to a secure area of *Microsoft 365 SharePoint* or within a database system. It is imperative that PII and other sensitive data always remain encrypted, which means that the data must generally stay in secure online platforms, and only be locally downloaded to devices that are protected by full-device encryption.

All staff are assigned and maintain their own personal logins that are password protected for each Database system. These systems each include an 'Automatic Log-Out' if activity on the site has stopped for over 60 minutes. The internal help desk team can support staff in obtaining, resetting, or addressing other access issues to these systems.

<<INSERT ORG NAME>> understands that employees may need to access PII while off-site or during travel. Data access should be minimized to the degree possible to meet the client or program needs and such that the data shall reside only on assigned laptops or approved storage devices that are protected by full-disk encryption. In particular, it is strictly prohibited to access PII or any other data on a shared device such as a public kiosk or hotel business center PC.

Electronic Communication of PII: Any information sent between staff, interns, volunteers, or independent contractors containing PII must be sent through a **<<INSERT ORG NAME>>** issued email account. This ensures the information is protected through the agency's secure and protected environment which includes several protections for PII. All staff members are required to enable for multi factor authentication in order to access their email.

If email communication is necessary, staff must either encrypt their email or encrypt the document with a password to securely transmit the information. The password should then be transmitted via different channel, preferably voice or SMS communication, from the email with the attached PDF. For information on how to encrypt files, see: https://support.office.com/en-us/article/encrypt-email-messages-373339cb-bf1a-4509-b296-802a39d801dc

Upon submission, staff should contact the external provider to whom the information was sent should be contacted to alert them and either confirm they received the attachment and separate password or call them with the password.