SAN BERNARDINO COUNTY

Human Services

# Privacy and Security Training for Contractors/Service Providers

## Introduction

This handbook provides a general overview of the federal and state regulations which protect the privacy and security of confidential information. Protection of confidentiality is a very important subject, which requires the training of all Contractors and Contractors' employees who are granted access to County client/customer Personally Identifiable Information (PII).

Federal and state laws require the County of San Bernardino Human Services (HS) implement privacy safeguards, which provide for the privacy and security of PII. Additionally, a Privacy/Security Incident Report is required when County PII is lost, stolen, disclosed or accessed without authorization, compromising the security, confidentiality or integrity of the information. Contractors and Contractors' employees that receive PII from the County of San Bernardino HS must comply with applicable privacy and security laws, regulations and agreements. A violation of confidentiality is punishable under civil and criminal law and may include a monetary fine and/or imprisonment.

## Personally Identifiable Information (PII)

Federal and state laws govern the protection of PII. PII may be used alone or in conjunction with any other reasonably available information, to identify a specific individual. PII may be electronic, paper, verbal or recorded. PII includes, but is not limited to:

- Name,
- Social Security Number (SSN),
- Date of Birth (DOB),
- Address,
- Drivers License,
- Photo Identification,
- Biometric record,
- Place of birth,
- Mother's maiden name, and
- Identifying number/document (i.e. Case number, Client Index Number (CIN), etc.).

For the purpose of this training, PII will be used to refer to both confidential information and County client/customer PII.

## Federal/State Mandates

The use, access and disclosure of PII is primarily governed by the following laws, regulations and agreements:

- Social Security Administration (SSA) Information Exchange Agreement (IEA)
- Medi-Cal Data Privacy and Security Agreement (PSA) between the State of California Department of Health Care Services and the County of San Bernardino
- Information Practices Act California Civil Code section 1798 et. seq. (IPA)
- Health and Safety Code, Division 109

- Welfare and Institutions Code
- Internal Revenue Code

## Privacy and Security Overview

It is the policy of HS to establish protocols to effectively protect and secure PII against any inappropriate use or disclosure. On an ongoing basis, Contractors and Contractors' employees must comply with all privacy and security requirements at the Federal, State and County level.

## Privacy Training Requirements

Contractors and Contractors' employees granted access to a county facility and/or resources containing PII, must:

- Read, understand and comply with the requirements as outlined in this training, and
- Sign the Privacy and Security Training Acknowledgement (at the end of this training packet)

This mandatory training must be completed within the first thirty (30) days of hire and prior to accessing PII. Thereafter, Contractor must provide annual refresher training, or three or more reminders per year of the privacy and security safeguards in this Agreement to all employees and volunteers. Anyone who refuses to review this training and sign the required documents must not be allowed access to County PII or be assigned to work in a County facility that contains PII.

**Note:** A copy of the signed Privacy and Security Training Acknowledgement must be maintained by the Contractor for three (3) years after completion of the training.

## Background Check

Contractor must ensure a background check is:

- Completed for all employees before they may access PII.
- Commensurate with the appropriate level of access granted to perform administrative functions according to position or title.
- Retained for three (3) years following the conclusion of employment.

## Badges

To prevent unauthorized access to facilities where PII is stored, Contractors must ensure employees:

- Wear an identification badge at all times.
- Contact their supervisor immediately to report a lost or stolen ID badge and request a new one.
- Obtain/wear a visitor's badge if ID badge is temporarily misplaced.
- Surrender ID badge and any keys or access control devices when access is no longer required or upon leaving employment.

## Privacy and Security Requirements

Contractors and Contractors' employees granted access to County PII must:

- Read and understand the contract requirements.
- Understand and utilize necessary safeguards outlined at http://hss.sbcounty.gov/Privacy/default.htm to protect and secure PII from unauthorized or unlawful access, use, and/or disclosure.
- Only access the minimum amount of PII necessary to perform a required business function, activity or service directly related to the assigned duty.
- Be diligent in their efforts to protect PII, sharing only with authorized persons who have a legal/reasonable need to know in order to perform their assigned job function(s).

## Accessing Information

### Access Authorization

Contractors and Contractors' employees authorizing access to PII, must secure, monitor and control PII access, systems, areas and resources. Access to PII must only be authorized on a "need-to-know" basis and not merely by position or title.

### Visitor Access

Contractors and Contractors' employees must control visitor access where PII is maintained. All visitors must:

- Enter through the reception area,
- Obtain/wear a visitor badge (i.e., paper nametags, permanent visitor badges, etc.) at all times while in the facility,
- Be escorted through the facility by staff, and
- Never have viewable access to PII.

## Inappropriate Access

PII must remain protected and secured from all threats of misuse, disclosure, damage or loss. Therefore, Contractors and Contractors' employees granted access, must not access, disclose or use PII in a manner or purpose not authorized by a legitimate business need. In other words, PII must never be accessed or viewed due to curiosity. Unauthorized access, use, or disclosure of PII is considered a breach of privacy/security and must be reported to the Human Services (HS) Privacy and Security Officer.

## Access Termination

Contractors must track and control access to PII by staff, including but not limited to:

- Immediately terminating access to PII and computer systems containing PII when access is no longer needed, including upon termination of the employee.
- Ensuring an individual who is terminated from access to the facility is promptly escorted from the facility by an authorized employee.

## Conflict of Interest

Contractor and Contractors' employees must avoid access to information from any PII which involves a:

- Relative
  - Any individual related by blood, marriage or adoption
- Person with whom the employee lives
  - Sharing a residence with another individual regardless of relationship
- Friend
- Colleague
- Acquaintance

## Incident Reporting

**Immediately upon discovery** Contractor and Contractors' employees must report to the Human Services (HS) Privacy and Security Office (PSO) any suspected or actual event that threatens the confidentiality of client/customer information ("security incident"), including but not limited to:

- Lost information,
- Stolen information,
- Mis-sent information, and
- Unauthorized access or disclosure.

Contractors and Contractors' employees responsible for a substantiated breach are subject to criminal and/or civil penalties, corrective and disciplinary action(s) and/or sanction(s), as appropriate.

## Reasonable Safeguards

Contractors and Contractors' employees granted access to PII must adhere to the following:

### Verbal Information

- Keep conversations general and brief; if possible, avoid using names or other identifiers when discussing customers/clients.

- PII must only be disclosed to authorized persons when it is absolutely necessary to complete an assigned job function.
- Exercise caution when leaving a message on an answering machine.
  - Leave only the name of the facility and a return phone number if possible.

## Printed Information

- Paper records containing PII must be locked and stored when left unattended.
  - When leaving the work area, employees must:
    - ✓ Clear their desk of all PII, and
    - ✓ Secure PII in a cabinet, desk or office. (Do not leave keys in your desk or an obvious place).
- When disposing of PII, secure in a locked shred container. Never place in a trash can.
- When faxing PII:
  - Always use a FAX coversheet which includes a confidentiality statement notifying persons receiving faxes in error to destroy them.
  - Verify destination fax with the intended recipient before sending.
  - Review every page of a printed document prior to sending.
  - Never leave unattended, retrieve immediately and keep fax machines in secured areas away from unauthorized persons, including unauthorized staff.

## Electronic Information

Contractors and Contractors' employees must:

- Utilize unique User Identification (ID) and passwords to protect PII.
- Never share (or make accessible) User ID and/or passwords.
- Change password if revealed or compromised.
- Lock/Log off computer workstations when left unattended.
- Never store PII on home computers, access PII on a public computer or post PII to a personal or unauthorized website.
- Secure information on monitors so that it cannot be viewed easily by unauthorized persons.

Storage devices, removable media or mobile devices used to view, access, transmit or store PII must be approved for use by the Contractor/Contractors' employees and appropriately secured in conformity with information technology requirements, such as encryption. Types of devices include, but are not limited to:

- CD/DVD
- Memory cards/sticks (USB thumb drives)
- Smart phones, tablets, phablets
- Wireless devices
- External portable hard drives
- Floppy disks, etc.
- Computer systems
- PDA's
- Email

## Emailing PII

Contractors and Contractors' employees must:

- Utilize encryption when transmitting County client/customer PII via email.
- Submit an encrypted test email to the County's Information, Technology & Support Division (ITSD) for review, test run and approval at: EncryptionCheck@hss.sbcounty.gov

## Transporting PII

Contractors/Contractors' employees transporting PII must adhere to the following requirements:

- Obtain approval (as appropriate) prior to removing PII from office.
- Limit information to that which is the minimum necessary to perform the designated job function.
- Keep PII secured and in possession at all times.
- Never leave PII unattended/unsecured at any time in:
  - A vehicle unless locked and secured in the trunk, but never overnight, or for other extended periods of time.
  - Airplanes, buses, trains, etc., including baggage areas, and
  - Any public location.
- Return PII to the office immediately.

**Note:** At a minimum PII must be secured in a file, manila envelope, etc., to prevent documents from slipping out. When possible, it is recommended to use a lock-box or locking bag.

## Mailing PII

When mailing PII, Contractors and Contractors' employees must:

- Review every page of a printed document and verify address before sending.
- Ensure correspondence is not visible through the envelope window.
- Seal and secure PII from damage.
- Use a secure courier and tracking method that includes verification of delivery and receipt when mailing 500 or more individual records in a single packet.
- Encrypt all mobile media (USB drives, discs, etc.).

## Contact and Resource Information

For questions, concerns or to report a situation of possible non-compliance, please contact your supervisor/manager and they will contact the Human Services Privacy and Security Office via e-mail at: HSPrivacySecurityOfficer@hss.sbcounty.gov.

**County of San Bernardino**
**Human Services**
**Privacy and Security Training Acknowledgement**

I, _____, acknowledge that I have read and understand
(Please Print Legibly)
the County of San Bernardino Human Services Privacy and Security Training for Contracted Service Providers. I agree to comply with the terms and requirements contained therein regarding the privacy and security safeguards of Personally Identifiable Information (PII) and agree to not disclose any information acquired in the course of my assigned duties to unauthorized persons. I understand that violation of these requirements may result in disciplinary action, up to and including termination of employment, as well as civil and criminal liability.

_____ _____
Signature Date

☐ Employee was provided a copy of the Privacy and Security Training on _____
Date

_____ (____)_____
Supervisor (Please Print) Supervisor Phone No.

_____ _____
Supervisor Signature Date

cc: Employee
Supervisor
Employee folder