County of San Bernardino Human Services

Privacy and Security Guide 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 guidance of all Contractors and Contractor's employees who are granted access to Personally Identifiable Information (PII).

Federal and state laws require the County of San Bernardino Human Services (HS) to implement safeguards which provide for the privacy and security of PII. In addition, the law require a breach report when PII is lost, stolen, destroyed, disclosed or accessed without authorization, compromising the security, confidentiality or integrity of the information. Federal and state mandates further require that all Contractors that receive PII from the County of San Bernardino HS comply with the applicable privacy and security laws, regulations, and agreements. A violation of confidentiality may be punishable under civil and criminal law and may include a minimum monetary fine of $1,000.00 per offense and/or imprisonment.

Personally Identifiable Information (PII)

Federal and state laws govern the protection of PII, such as:

- Name,
- Social security number,
- Date of Birth (DOB),
- Address,
- Drivers License,
- Photo Identification, and/or
- Identifying number/document (i.e. Case number).

PII can be used alone or in conjunction with other personal or identifying information which is linked or linkable to a specific individual.

Federal/State Mandates

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

- Agreement between the Social Security Administration (SSA) and State of California Department of Health Care Services
- Medi-Cal Data Privacy and Security Agreement between the State of California Department of Health Care Services and the County of San Bernardino
- Health Insurance Portability and Accountability Act (HIPAA)
- Health Information Technology for Economic and Clinical Health Act (HITECH Act)
- Confidentiality of Medical Records Act (CMIA)
- Patients Access to Health Records Act (PAHRA)
- Health and Safety Code, Division 109
- Welfare and Institutions Code
- Internal Revenue Code

Privacy and Security Overview

On an ongoing basis, Contractors and Contractors' employees must comply with all privacy and security requirements at the federal/state/county level. On a yearly basis, Contractors and Contractors' employees granted access to a county facility and/or resources containing PII, must:

- Read and understand the requirements as outlined in this guide, and
- Sign the Certificate of Completion.

Any Contractor or employee of the Contractor who refuses to review this guide and sign the Certificate of Completion will not be allowed access to PII or be assigned to work in a County facility that contains PII.

Note: A copy of the signed Certificate must be maintained by the Contractor.

Privacy and Security Requirements

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

- Understand and utilize necessary safeguards to protect and secure PII from unauthorized or unlawful access, use, and/or disclosure.
- Must only access PII that is necessary to perform a 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 the assigned job function(s).
- Must have knowledge of, and remain in compliance with all County of San Bernardino HS privacy and security policies/standard practices.

Inappropriate Access

Access Authorization

Contractors and Contractors' employees authorizing access to PII, must secure, monitor and control PII access, systems, areas and resources. Access must be authorized prior to working with or in a location where PII resides. Only those that require access to PII for work related purposes shall be granted access.

Accessing Information

PII must remain protected and secured from all threats of loss or unauthorized disclosure. Therefore, Contractors and Contractors' employees granted access, must not access, use or disclose PII unless there is a legitimate business need to look at such information. 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 HS Privacy and Security Officer.

Reasonable Safeguards

Verbal Information

Contractors and Contractors' employees granted access to PII must take precaution when discussing PII. If possible, avoid using names or other identifiers when discussing customers/clients. Don't disclose PII to others unless it is absolutely necessary to complete an assigned job function. Caution must be taken when leaving messages for a customer/client on an answering machine. Leave only the name of the facility and a return phone number if possible.

Printed Information

Printed documents containing PII may include, but are not limited to hand written notes, printed computer information (such as reports), a printed fax or other documents. Proper steps to protect printed information include locking file cabinets, offices or other doors or areas where printed information may be stored, and securing printers and other devices that produce printed information. Printed information must always be disposed in confidential shred bins and must never be placed in the trash.

Electronic Information

PII stored electronically includes information stored on computer systems, hard drives, PDA's, cell phones, email, CDROM's, memory sticks, flash drives and any other device capable of storing data in an electronic format. Federal/State mandates require that information stored electronically be protected from anything that would be a threat to the confidentiality, integrity and availability of that information. HS utilizes various administrative, physical and technical safeguards to protect this information.

Examples of these types of safeguards include requiring that all Contractors and Contractors' employees have a unique user ID and password in order to access PII on computers. Users are to log off of computers promptly when completed with work or lock the computer before leaving it unattended. PII may not be stored on a device that does not have security or access controls. Never remove or transfer electronic PII from a county facility, unless authorization is granted and only the minimal amount necessary to perform the required job function. PII may not be stored on home computers, accessed on a public computer or posted to a personal or unauthorized website. PII may not be transmitted through personal email.

Incident Reporting

All suspected or actual security incidents **must** be reported to a manager/supervisor and to the HS Privacy and Security Representative/Officer **immediately**. Thereafter, HS investigations are conducted by:

- HS Privacy and Security Officer,
- County Compliance and Ethics Officer,
- County Human Resource Officer (HRO), and/or
- State/Federal officials (depending on the level and/or type of breach of information).

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

Contact and Resource Information

If you have questions, concerns or need to report a situation of possible non-compliance, please contact the HS Privacy and Security Officer via e-mail at: HSPrivacyandSecurityOfficer@hss.sbcounty.gov.

County of San Bernardino

Human Services

Privacy and Security Guidance for Contractors/Service Providers

I have read and understand the County of San Bernardino Human Services Privacy and Security Guide. I agree to comply with the terms and requirements contained therein regarding the privacy and security of Personally Identifiable Information (PII). 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.