
CALIFORNIA CORRECTIONAL
HEALTH CARE SERVICES
Privacy
Awareness
Exhibit E
Prepared by: CCHCS Privacy Office

Overview

This course provides an overview for:

- Privacy and understanding its importance
- Privacy laws, policies, and principles
- Your role in protecting privacy
- Consequences for violations
- How to report a privacy event

Learning Objectives

1. Recognize your role in protecting privacy.
2. Recognize the consequences for privacy violations.
3. Recognize how to report a privacy event.

What Is Privacy?

Privacy refers to freedom from intrusion into personal matters and personal information. It is a right rooted in common law.

At CCHCS privacy can relate to staff information, inmate information, electronic forms of information, hard copies, statements made verbally by individuals, etc.

Roles and Responsibilities

All members of the CCHCS workforce are responsible for following privacy policies and procedures, which include:

1. Create, collect, use, and disclose personal information for reasons that are for a legitimate job function, support the mission of CCHCS, and are allowed by law.
2. Disclose only the minimum amount of information necessary.
3. Access information only for authorized purposes.
4. Follow standards to safeguard personal information throughout the information life cycle.
5. Report suspected privacy violations or incidents.
6. Comply with all applicable privacy laws.

Possible Consequences of Privacy Violations

Privacy violations have several possible consequences:

- Embarrassment or harm to others
- Loss of trust between CCHCS and the public
- Employee discipline
- Personal fines
- Individual criminal charges

Key Privacy Laws

- Federal Privacy Act, Public Law 93-579
- Freedom of Information Act, 5 U.S.C. 552(b)(6)
- Information Practices Act, California Civil Code Section 1798 et seq.
- California Public Records Act, Government Code Section 6250 et seq.

Privacy Guidance and Policy

Guidance

Article 1, Section 1, of the Constitution of the State of California defines pursuing and obtaining ***privacy as an inalienable right***.

The Information Practices Act of 1977 (Civil Code section 1798, et seq.) places ***specific requirements*** on ***each state entity*** in the collection, use, maintenance, and dissemination of information relating to individuals.

Government Code Section 11019.9 ***requires state agencies to*** "… maintain a privacy policy and to designate an employee to be responsible for the policy."

Government Code Section 11549.3 states that CCHCS shall **ensure *compliance*** with all privacy laws, regulations, rules, and standards specific to and governing the administration of their programs.

What is Personally Identifiable Information (PII/PHI)?

Per Civil Code 1798.3: Personal Information means any information that is maintained by an agency that identifies or describes an individual, **including, but not limited to**, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history.

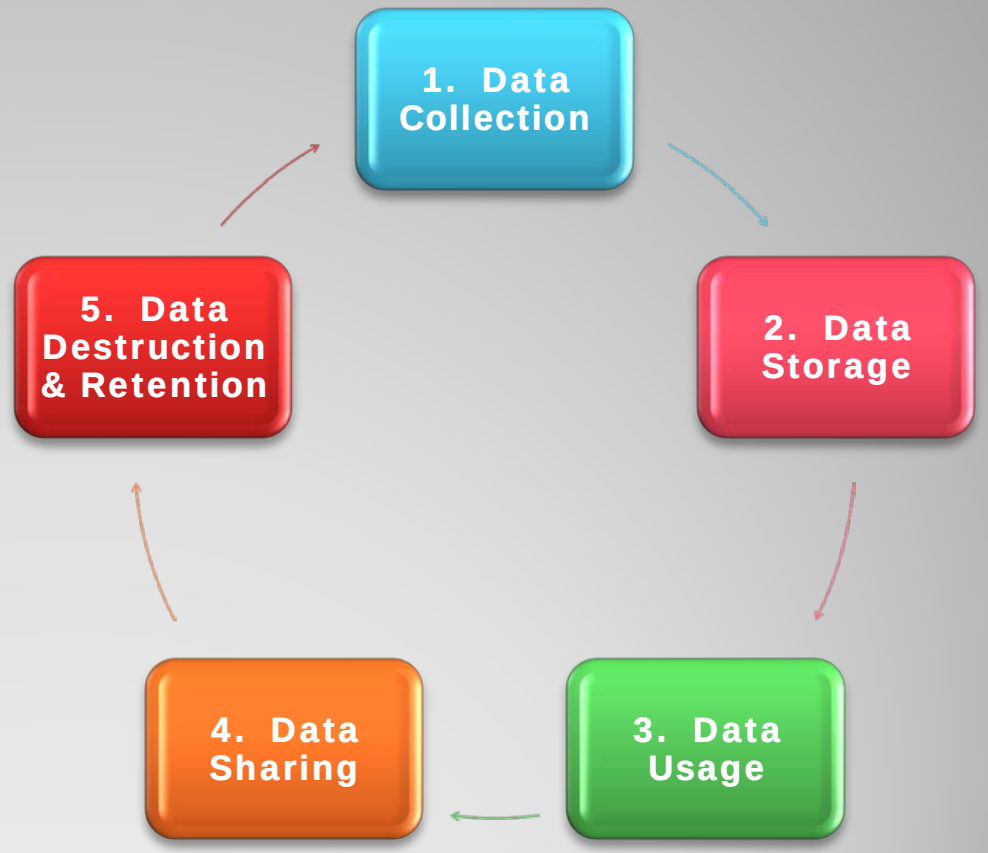
It also may include statements made by, or attributed to, the individual.

Common Examples of PII/PHI

(Typically a combination of two or more)

- Name
- Social Security number (SSN)
- Date of birth (DOB)
- Mother's maiden name
- Financial records
- Email address
- Driver's license number
- Passport number
- Health information
  - Including patient identification number

5 Key Areas - Information Lifecycle and Privacy



- ✓ Ensure you are allowed to collect the PII/PHI (law, regulation, policy, etc.).
- ✓ Validate you have a legitimate business need to collect the PII/PHI.
- ✓ Determine if you are obtaining the PII/PHI in a secure manner so it cannot be overheard or seen by others.
- ✓ Request, create, or collect only the minimum amount of PII/PHI necessary to do your job.

- ✓ Determine whether or not you need to store the PII/PHI (it may be readily available elsewhere).
- ✓ Secure documents and files that contain PII/PHI for use by authorized persons only.
- ✓ When storing PII/PHI on mobile devices it can only be stored on authorized CCHCS issued portable encrypted electronic devices.
- ✓ Follow proper procedures to ensure the privacy of the stored PII/PHI.

3. Data Usage

- ✓ Only use the PII/PHI for the purpose it was provided.
- ✓ Use only the minimum amount of PII/PHI necessary to complete your job functions.
- ✓ Access PII/PHI using authorized procedures.
- ✓ Use secure authorized equipment and technology connections.

- ✓ Verify the sharing is allowed.
- ✓ Validate that everyone sharing the PII/PHI has a need to know.
- ✓ Share only the minimum amount of PII/PHI and follow proper disclosure procedures.
- ✓ Make sure you share PII/PHI using the appropriate safeguards (e.g., encryption, sealed envelope).

5. Data Destruction & Retention

- ✓ Ensure the PII/PHI has a valid retention schedule.
- ✓ Shred papers containing PII/PHI when no longer needed.
- ✓ Return unused equipment (e.g., computer, copiers, fax machines) to the IT department for proper disposal.

Differences Between Privacy and Information Security

The General Rule – "W" and "H"

Privacy: the "**W**" questions:

- **Why** am I creating, collecting, storing or sharing the PII/PHI?
- **What** are the data elements of the PII/PHI?
- **Who** am I collecting the PII/PHI from?
- **Who** am I going to share the PII/PHI with?
- **When** might I share the PII/PHI?
- **Where** am I going to store and save the PII/PHI?
- **When** am I going to need to destroy the PII/PHI?

Differences Between Privacy and Information Security

Information Security: the "**H**" questions:

- **How** am I going to securely create, collect, store and share PII/PHI to ensure it is private?
- **How** does CCCHS require me to ensure certain types of information are kept private?
- **How** do I find out the proper way to securely share information verbally, in writing and electronically to ensure privacy?
- **How** am I supposed to securely store and destroy PII/PHI?

What is a Breach of Privacy?

A privacy breach occurs when there is unauthorized access, collection, creation, use, or impermissible disclosure of private information.

Common Scenarios

Common privacy breaches include:

- Private conversations in public places.
- Paper and other documents stored in incorrect folders and accidently disclosed.
- Inadvertently sending email containing PII/PHI to a person not authorized to view it.
- Allowing an unauthorized person to use your computer.

The Effects of Compromised Privacy

Privacy breaches ARE SERIOUS; outcomes can include:

- Exploitation of an individual's medical/financial status
- Harm to unintended individuals
- Personal fines, sanctions, and fees
- Job loss
- Criminal charges and prison

How and When to Report

- ✓ Do not investigate an incident on your own.
- ✓ Immediately report suspected incidents within 3 days to the Information Security Office (ISO) via E-mail CCHCS-ISO@CDCR.ca.gov and/or Telephone Number (916) 691-3243.
- ✓ The ISO is the **first point** of contact for **all** information security incidents (even those that affect PII/PHI).
- ✓ Incidents relating to PHI and a California Department of Public Health (CDPH) licensed facility (e.g. General Acute Care Hospital) must be reported to the CCHCS ISO within **24 hours**. The facility must also follow their procedures for reporting to CDPH.

Policies and Procedures

- **It is your responsibility** to read, understand, and abide by CCHCS privacy policies and related policies and procedures.
- Policies can be found on the CCHCS Internet.
- You can request hard copies from your supervisor.

Privacy Guidance

For specific privacy-related policy questions:

- See Chapter 13 of the Inmate Medical Services Policy and Procedures Manual
- Email the CCHCS Privacy Office at privacy@cdcr.ca.gov
- Call the CCHCS Privacy Office 1-877-974-4722

Course Summary

This course provided you information on:

- The definition of privacy and understanding its importance.
- Privacy laws, policies, guidance, and principles.
- Your role in protecting privacy and the consequences for violations.
- Reporting a privacy breach.

How to Protect PII/PHI

For more information on how to protect PII/PHI, refer to the Information Security Awareness training.

Self-Certification of Completion

For County Business Associates

California Correctional Health Care Services Privacy Awareness Training

I certify I have completed the Privacy Awareness Training course. I have read, understand and shall comply with the California Correctional Health Care Services (CCHCS) Privacy policies, related policies and understand it is my responsibility to comply with related state and federal privacy law. I shall ensure a copy of this training certificate is maintained and can be provided upon request for at least six years.

Please complete all of the information below:

Name of County Facility/Jail:

_____

Unit Name (If applicable):

_____

Legibly PRINT Last Name:

_____

Legibly PRINT First Name:

_____

Phone:

_____

E-Mail:

_____

Manager's Name/Project Manager's Name (In MOU):

_____

Date Privacy Awareness Training completed:

_____

Contractors complete this section:

Name of County:

_____

MOU Agreement Number:

_____

_____ _____ _____ _____

Signature *Date* *EDSA Manager's Signature* *Date*