Privacy

California Hospital Association

Agenda

- Privacy Refresher
- Breach Reporting Requirements
  - HIPAA
  - Breach - Licensed Health Facility
  - Breach of Unencrypted Computerized Data
- 42 CFR Part 2 Updates
- Reproductive Health & Privacy

.

California Hospital Association

Privacy Refresher

California Hospital Association

Health Insurance Portability and Accountability Act (HIPAA)

- **Federal Law governing the protection, disclosure, and reporting of private health information**
- **Purpose**: sets out national standards to protect patient health information from being disclosed without the patient's consent or knowledge. HIPAA's implementing regulations include:
  - *Privacy Rule* – imposes standards that address the permitted, required, and prohibited uses and disclosure of individually identifiable health information (known as "protected health information" or "PHI") by covered entities ("CEs") and their business associates (BAs)
  - *Security Rule* – establishes standards for CEs and BAs to implement reasonable and appropriate safeguards to protect electronic PHI
  - *Breach Notification Rule* – requires CEs to notify HHS Office of Civil Rights (OCR) and affected individuals when breaches of unsecured PHI occur. BAs must notify CEs of breaches.

What is Protected?

PHI = information that can identify an individual + information about that individual's health care, health condition or health status.

PHI applies to demographic information, which includes information about who an individual receives health care from.

HIPAA Privacy Rule

Permitted Disclosures: HIPAA permits covered entities to use and disclose PHI in certain circumstances, without first obtaining patient authorization, such as:

- **Treatment activities** (consultation, referral, direct patient care, etc.)
- **Payment activities** (billing, claims, eligibility and/or coverage determination, collection activities, etc.)
- **Health care operations** (peer review, quality assessment, management activities, etc.)
- **Certain judicial and administrative proceedings** (e.g. court order) and law enforcement purposes (subject to specific exceptions); and
- **Public interest activities** (disease reporting, research, worker's compensation, etc.)

Unless a disclosure of PHI is permitted or required by law, must not disclose PHI! Don't forget about state law!

California Hospital Association

CA Confidentiality of Medical Information Act

Basics:

- A provider of health care, health care service plan, pharmaceutical or contractor cannot disclose medical information without an authorization unless the disclosure is required or permitted under Civil Code Section 56.10(b) or (c), which includes disclosures:
  - To a patient or patient's legal representative
  - For TPO purposes
  - In response to subpoenas and court orders, etc.

Medical Information:

- Individually-identifiable information regarding a patient's medical history, mental or physical condition or treatment. If individually identifiable information does not include information about the individual's medical history, mental or physical condition, or treatment, it does not constitute "medical information" *Eisenhower Med Ctr. v. Sup. Ct. (Malanche),* 226 Cal. App. 4th 430 (May 21, 2014).

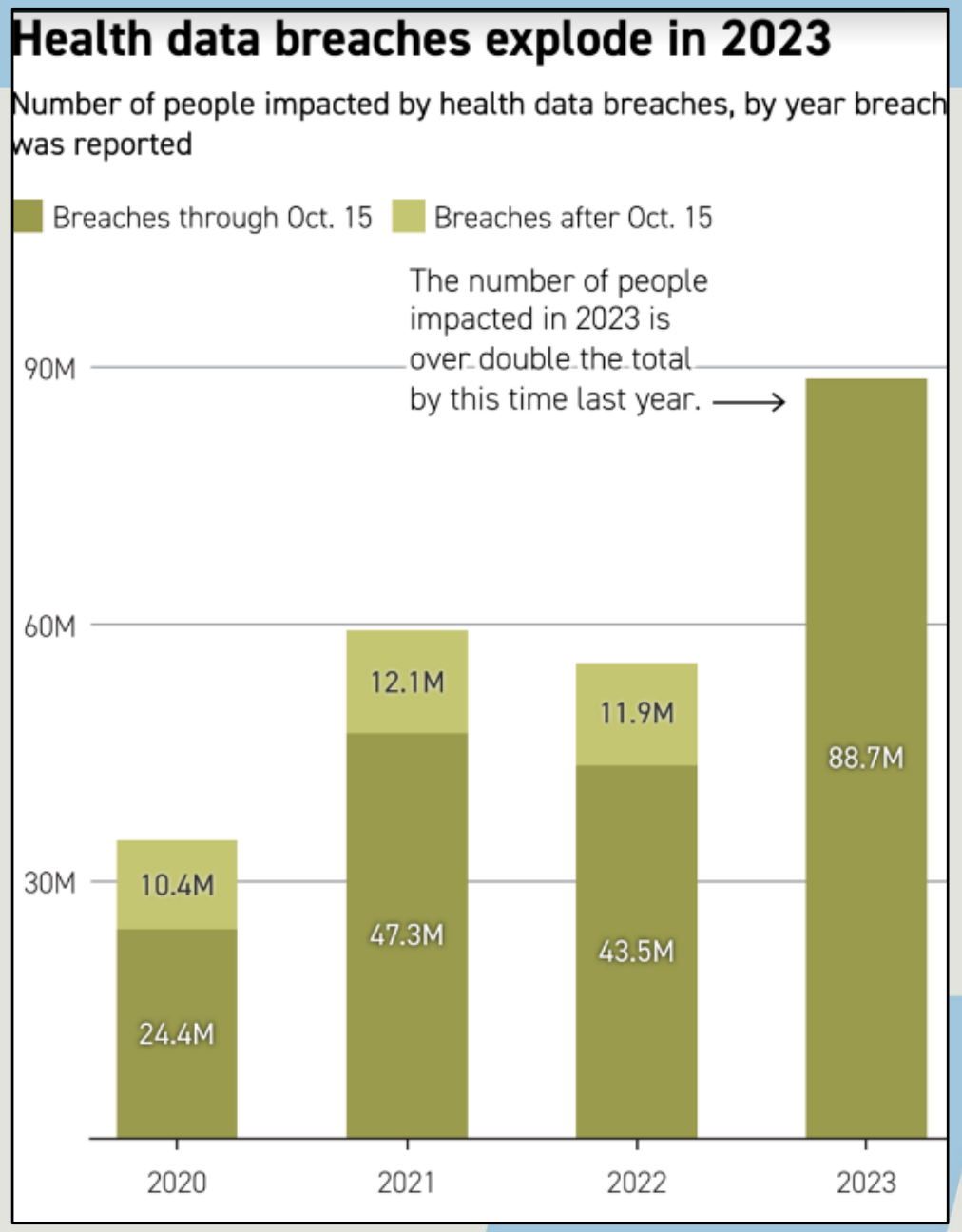
Note that CMIA does NOT apply to information protected under the CA Lanterman-Petris Short Act (W&I Code Section 5328)

Breach Reporting Requirements

California Hospital Association

Setting the Stage…

Note: Data contains breaches required to be reported to the federal government, including those archived and currently under investigation.
Source: U.S. Department of Health and Human Services Office for Civil Rights
Ben Leonard /POLITICO



Breach Reporting Requirements Overview

Part 2!

	HIPAA/ HITECH Breach Notification	Breach - Licensed Health Facility	Breach of Unencrypted Computerized Data
Legal cite:	42 USC 17932; 45 CFR 164.400	Cal. Health & Safety Code 1280.15, 22 CCR 79900	Cal. Civil Code 1798.82
Who must comply:	Covered entities, business associates	Certain licensed facilities, including hospitals, licensed clinics, SNFs, HHAs, and hospices	Any person or business that conducts business in CA

HIPAA Breach Notification Rule

Breach: "The acquisition, access, use, or disclosure of PHI in a manner not permitted [by HIPAA] which compromises the security or privacy of the [PHI]".

- Not all HIPAA violations are breaches, and breach notification isn't required in all cases of impermissible use, access or disclosure. Rather, only violations that compromise the security or privacy of the PHI must be reported.
- Breach of Secured PHI does not trigger the Breach Notification Rule.

Breach Discovery

The discovery of a breach occurs on the first day on which such breach is known to the CE or BA, or reasonably should have been known.

- The breach is considered "known" once a person, other than the individual committing the breach, who is an employee, officer, or other agent of such CE or BA knows or should have reasonably known of the breach.

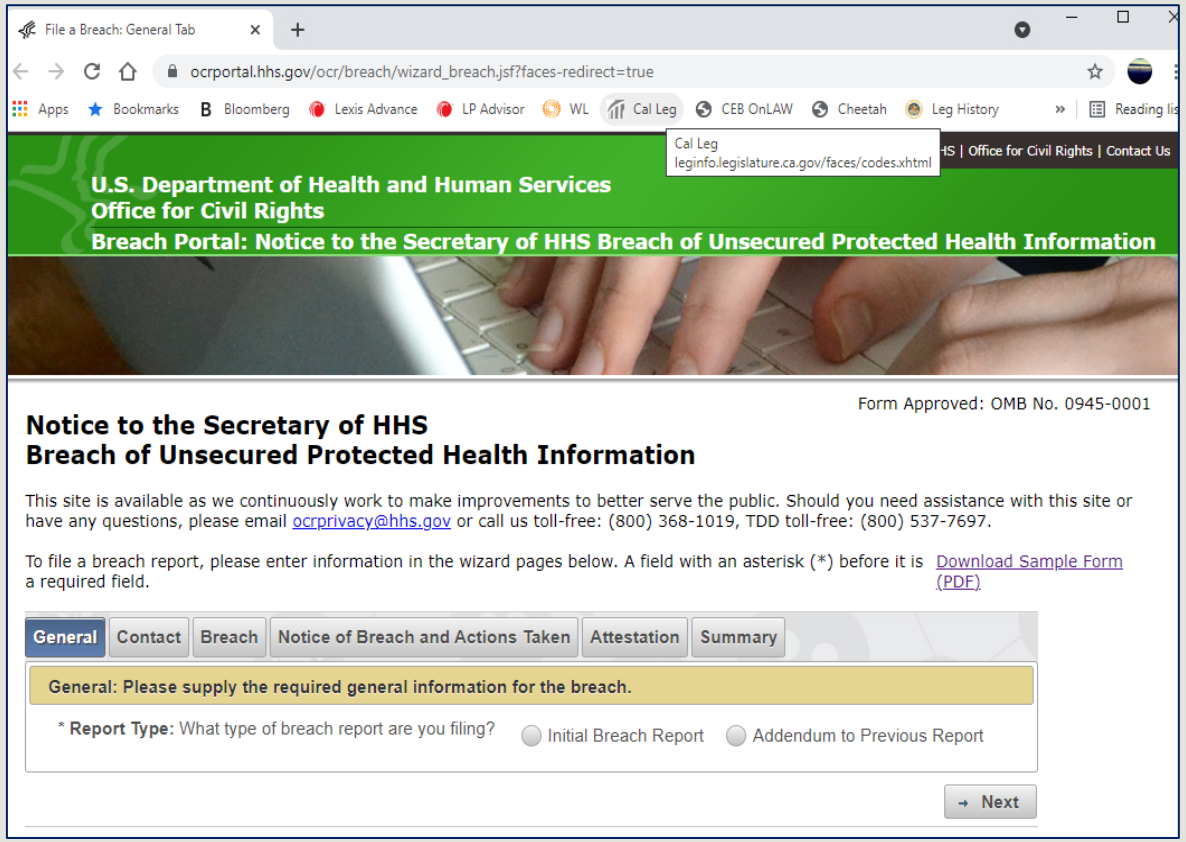
Determining If a Violation = Breach

- The HIPAA breach definition encompasses a harm threshold – specifically the phrase "compromises the security or privacy of the protected health information."
- To determine if the privacy or security of PHI has been compromised, a risk assessment must be performed.

1. Nature/extent of PHI, including types of identifiers and likelihood of re-identification
2. The unauthorized person who used the PHI or to whom the PHI was disclosed; and
3. Whether the PHI was actually acquired or obtained
4. The extent to which risk to PHI has been mitigated

California Hospital Association

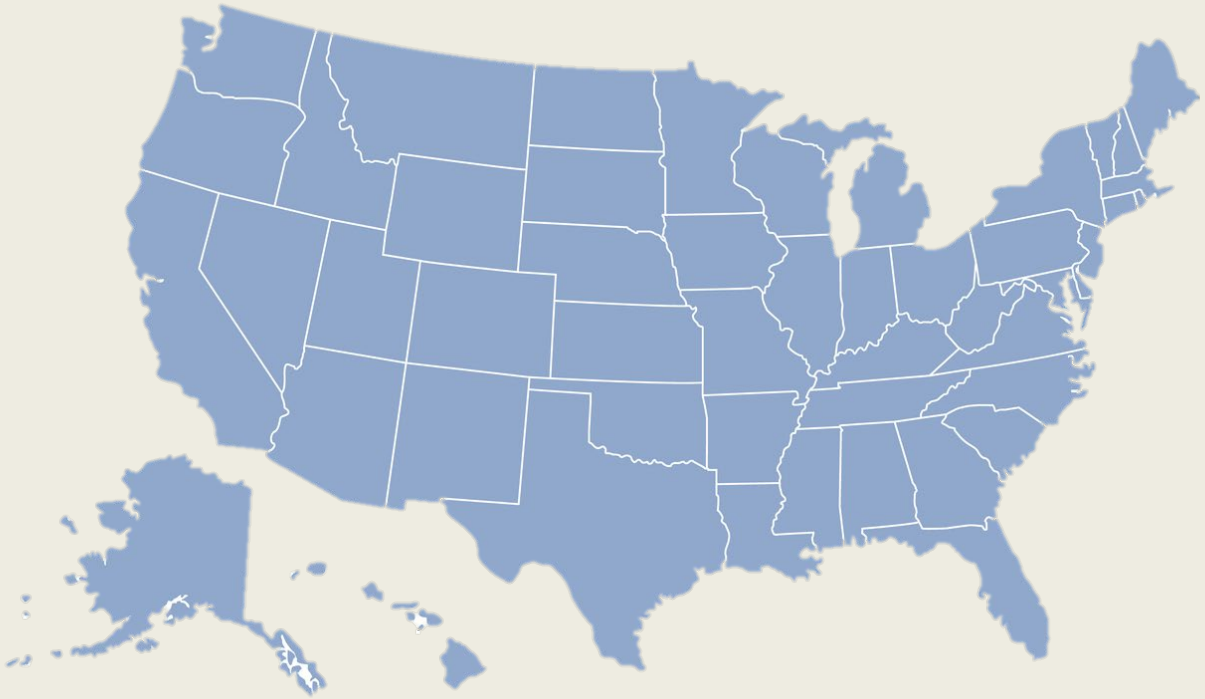
Breach Notification Rule Requirements



- Notice required to the affected individuals and OCR* “without unreasonable delay” and in no case later than 60 calendar days from time the CE or its BA knew or should have known of the breach.
- Media notice if breach affects more than 500 residents of a jurisdiction.
- Notice may be delayed if a law enforcement official determines that the notice would impede a criminal investigation or cause damage to national security.
- Business associates need only notify the covered entity of a breach unless the applicable BAA states otherwise.

California Hospital Association

State Requirements



Depending on where a patient and health care provider are located, state law may impose additional privacy or security requirements.

- HIPAA preempts state laws providing a lesser level of privacy/security protection to patients and allows stronger state privacy requirements to co-exist with HIPAA requirements.
- HIPAA compliance sets a floor on requirements for PHI security/privacy, not a ceiling.

California Breach Reporting Laws and Regs

- **H&S Code § 1280.15:** Notice required to the affected individuals and CDPH **no later than 15 business days** after detection of breach by CE or BA

- **Civil Code § 1798.82:** Notification must be "in the most expedient time possible without unreasonable delay"
  - Notify affected CA residents
  - Notify CA Attorney General (with sample resident notice) if more than 500 residents

State of California – Department of State Hospitals
Department of State Hospitals - Sacramento
1600 9th Street
Sacramento, CA 95814
www.dsh.ca.gov

Gavin Newsom, Governor

DSH

April 5, 2021

Reference #ISO01297

Notice of Data Breach

What Happened? On March 15, 2021, during the investigation into this incident, DSH discovered that the same employee had improperly accessed personal information, including addresses, phone numbers, email addresses, social security numbers, date of birth, and health information related to employment, of approximately 1735 employees and former employees, and 1217 DSH job applicants who never became DSH employees. This was discovered during the investigation of the same employee who was found to have improperly accessed approximately 1,415 patient and former patient, and 617 employee names, COVID-19 test results, and health information necessary for tracking COVID-19 on February 25, 2021. At this time, DSH has no evidence that there has been any use or attempted use of the information compromised by this incident. DSH is providing this notice so that those individuals potentially affected may be aware of what happened and can take steps to monitor any unusual activity regarding their personal information.

What information was involved?

(The following four paragraphs set out the four versions of the Notice of Data Breach provided to the four groups of impacted individuals.)

The confidential information contained:

- 2822 individuals' names, addresses, phone numbers, email addresses, social security numbers, dates of birth, along with dates and general outcomes of various health-related tests done for purposes of employment with DSH, such as their physical and tuberculosis tests;
- two individuals' names, addresses, phone numbers, email addresses, dates of birth, along with dates and general outcome of various health-related tests done for purposes of employment with DSH;
- 77 individuals' names, general outcome of various health-related tests done for purposes of employment with DSH, and information regarding interviews they had for certain position(s) at DSH;

"Caring Today for a Safe and Healthy Tomorrow"

Rev. (11/2018)

42 CFR Part 2 – Updates!

California Hospital Association

42 CFR Part 2

- **Purpose:** Part 2 protects the confidentiality of SUD patient records by restricting the circumstances under which “Part 2 Programs” or other lawful holders can disclose such records.
- Part 2 is intended to ensure that a patient receiving treatment for a SUD in a Part 2 Program does not face adverse consequences in connection with seeking or receiving treatment for a SUD.
- **General Rule:** Part 2 Programs are prohibited from disclosing any information that would identify a person as having or having had a SUD unless that person provides written consent *OR* a valid court order requires the disclosure.

What is a Part 2 Program?

- Part 2 covers “federally assisted programs” that offer rehabilitative substance use treatment, diagnosis, or referrals for treatment.
  - (1) An **individual** or **entity** (other than a general medical facility) who **holds itself out** as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
  - (2) An **identified unit within a general medical facility** that **holds itself out** as providing, and provides, substance use disorder diagnosis, treatment, or referral for treatment; or
  - **(3) Medical personnel or other staff in a general medical facility** whose **primary function** is the provision of substance use disorder diagnosis, treatment, or referral for treatment and who are identified as such providers.

New HHS Final Rule – 42 CFR Part 2

- As mandated by the CARES Act, the final rule seeks to align 42 CFR Part 2 more closely with HIPAA.
- First, what has ***not*** changed?
  - SUD treatment records cannot be used to investigate or prosecute the patient without written patient consent or a court order
  - Clarifies that segregating or segmenting Part 2 records is not required

What's New?

- What *has* changed?
  - A **single patient consent** for all future uses and discloses for treatment, payment, and health care operations (TPO)
    - Permits redisclosure of Part 2 records in accordance with the HIPAA Privacy Rule
  - **Permitted disclosure** of de-identified records to public health authorities without patient consent
  - **Penalty, breach notification, and patient notice** requirements align with HIPAA regulations
  - **Safe harbor** for investigative agencies that act with reasonable diligence
  - **Defines SUD counseling notes** to require specific consent separate from TPO consent, like HIPAA psychotherapy notes

***Effective* April 16, 2024**
***Compliance Date* February 16, 2026**

California Hospital Association

Reproductive Health & Privacy

California Hospital Association

HIPAA Privacy Rule to Support Reproductive Health Care Privacy

- **Final Rule adopts:**
  - Changes to definitions, "person," "public health," and "reproductive health care"
  - "Purpose-based prohibition"
  - Applies when relevant activity is related to reproductive health care, and the HIPAA-regulated entity that receives the request for PHI has reasonably determined that:
    - Lawful under state where care is provided and under the circumstances in which it is provided;
    - Care is protected, required, or authorized under federal law; or,
    - The Final Rule's "presumption" applies.
  - Attestation Requirement
  - Notice of Privacy Practices Updates

***Effective* June 25, 2024**

***Compliance Date* December 23, 2024 ***

***NPP Compliance Date* February 16, 2026**

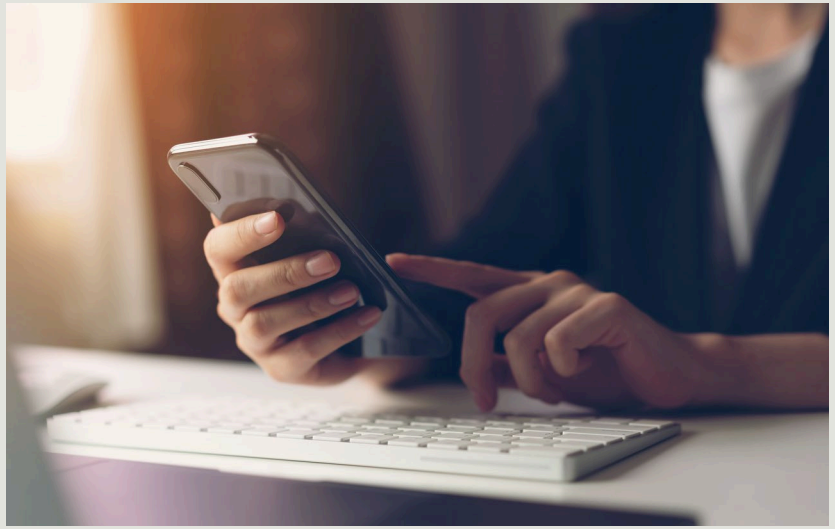
California Updates

AB 254

Amends CMIA to:

- expressly include businesses that offer a reproductive or sexual health digital service as "providers of health care," and,
- revise the definition of "medical information" to include reproductive and sexual health information collected by such businesses.

Attorney General Becerra Announces Landmark Settlement Against Glow, Inc. – Fertility App Risked Exposing Millions of Women's Personal and Medical Information



AB 352

Amends CMIA to:

- include privacy protections for information electronically stored or maintained by EHR developers, digital health companies, and other businesses related to gender affirming care, abortion, abortion-related services and contraceptives
- prohibits disclosures of medical information to anyone or any entity from another state related to abortion or abortion-related services that are lawful under California law unless authorized under statute

California Hospital Association

Additional California Privacy Laws; Resources

California Hospital Association

Appendix: California Health Privacy Laws

- **California Confidentiality of Medical Information Act**
  - CA's analog to HIPAA
  - The CMIA generally prohibits covered health care providers from disclosing medical information regarding an individual without authorization or some other permitted basis (e.g. for TPO), among other obligations.
- **H&S Code Section 11845.5**
  - Protects SUD records
- **H&S Code Section 120975**
  - Protects HIV test results from unauthorized disclosure
- **Lanterman-Petris Short Act**
  - Protects info and records created by certain mental health providers obtained in the course of providing health care services
- **22 C.C.R. § 51009**
  - Protects individual Medi-Cal records
- **Others**
  - Such as statutory privileges for certain patient records (e.g., psychotherapist-patient privilege); gender-affirming care; and reproductive health information protections, *etc.*

Online Resources

The Office of Civil Rights website: https://www.hhs.gov/hipaa/index.html

- Has downloadable PDF versions of all HIPAA rules plus training materials, FAQs, official guidance materials, white papers and much more.

National Institute of Standards and Technology (NIST) website: http://csrc.nist.gov/publications/PubsSPs.html

- This link is to the Special Publications, which are the reference documents for the Security Rule's implementation.

CA CDII State Health Info Guidance: https://www.cdii.ca.gov/compliance-and-policy/state-health-information-guidance-shig/

CA OAG Data Security Breaches: https://oag.ca.gov/privacy/databreach/reporting

California Hospital Association

Questions?

California Hospital Association

Thank you

California Hospital Association