

Understanding the New CDPH Privacy Breach Regulations

Title 22, California Code of Regulations, §§ 79900 – 79905

July 30, 2021

Welcome

Robyn Thomason

Director, Education Program Development
California Hospital Association



Continuing education credits will be offered for this program for compliance, health care executives, risk management and nursing. Full attendance and completion of the online evaluation and attestation of attendance are required to receive CEs for this webinar.

A recording of the program will be available.

Submit your questions through the Q & A box. (Usually located at the bottom of your screen.)



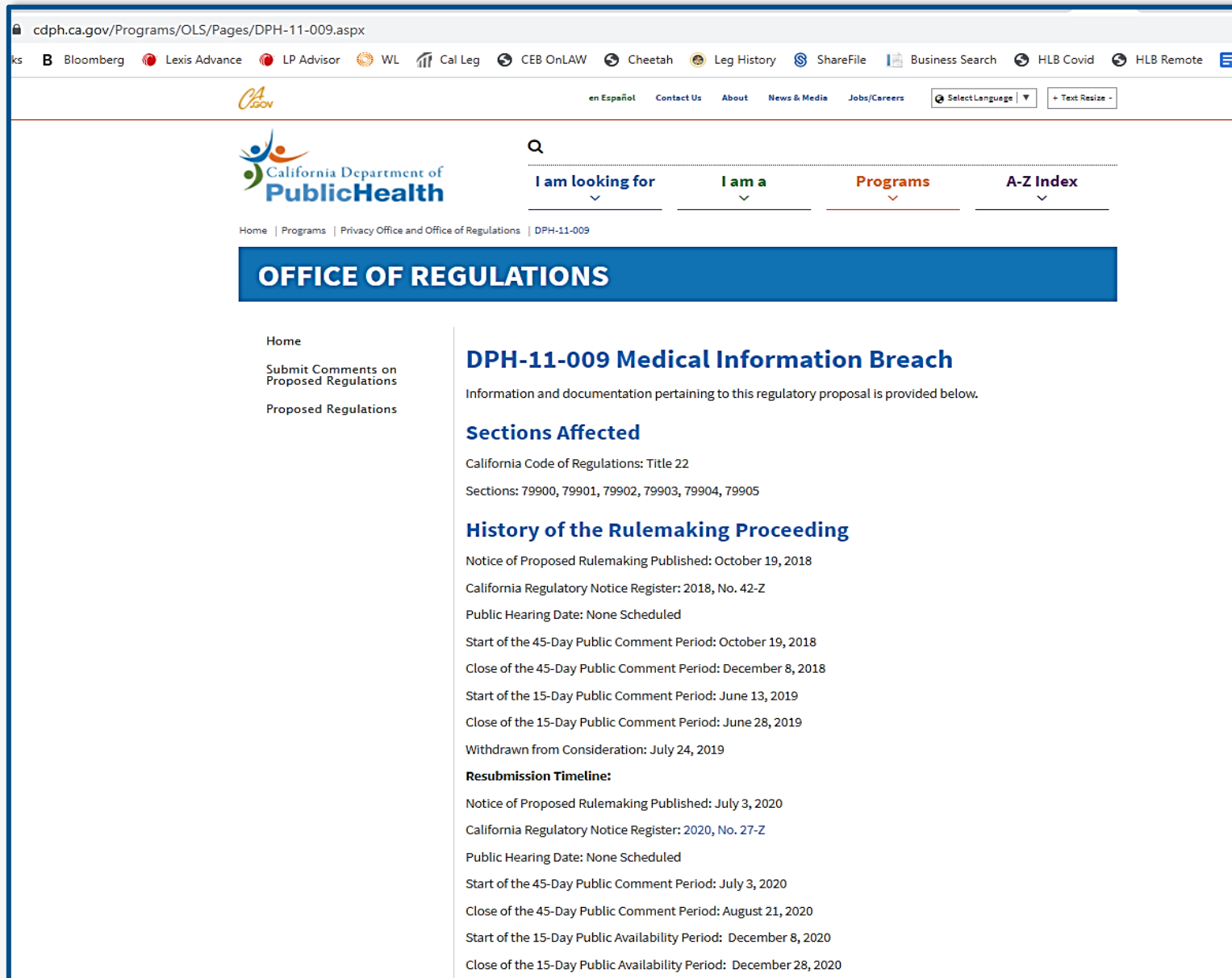
Lois Richardson
Vice President, Legal Counsel,
California Hospital Association



Andrea Frey
Associate
Hooper, Hooper
Lundy & Bookman, P.C



**Martha Ann (Marty)
Knutson**
Deputy County Counsel
Riverside County



The screenshot shows a web browser window with the URL cdph.ca.gov/Programs/OLS/Pages/DPH-11-009.aspx. The page header includes navigation links for [en Español](#), [Contact Us](#), [About](#), [News & Media](#), and [Jobs/Careers](#). There are also utility links for [Select Language](#) and [Text Resize](#). The main navigation bar features the California Department of Public Health logo and a search bar. Below the logo, there are dropdown menus for [I am looking for](#), [I am a](#), [Programs](#), and [A-Z Index](#). The breadcrumb trail reads: [Home](#) | [Programs](#) | [Privacy Office and Office of Regulations](#) | [DPH-11-009](#).

OFFICE OF REGULATIONS

- [Home](#)
- [Submit Comments on Proposed Regulations](#)
- [Proposed Regulations](#)

DPH-11-009 Medical Information Breach

Information and documentation pertaining to this regulatory proposal is provided below.

Sections Affected

California Code of Regulations: Title 22
Sections: 79900, 79901, 79902, 79903, 79904, 79905

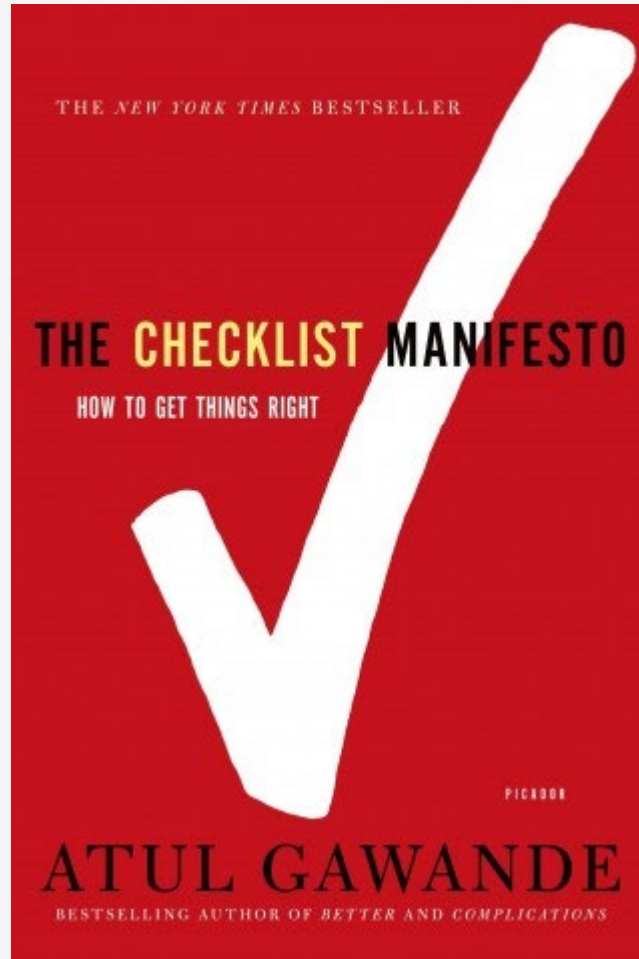
History of the Rulemaking Proceeding

Notice of Proposed Rulemaking Published: October 19, 2018
California Regulatory Notice Register: 2018, No. 42-Z
Public Hearing Date: None Scheduled
Start of the 45-Day Public Comment Period: October 19, 2018
Close of the 45-Day Public Comment Period: December 8, 2018
Start of the 15-Day Public Comment Period: June 13, 2019
Close of the 15-Day Public Comment Period: June 28, 2019
Withdrawn from Consideration: July 24, 2019

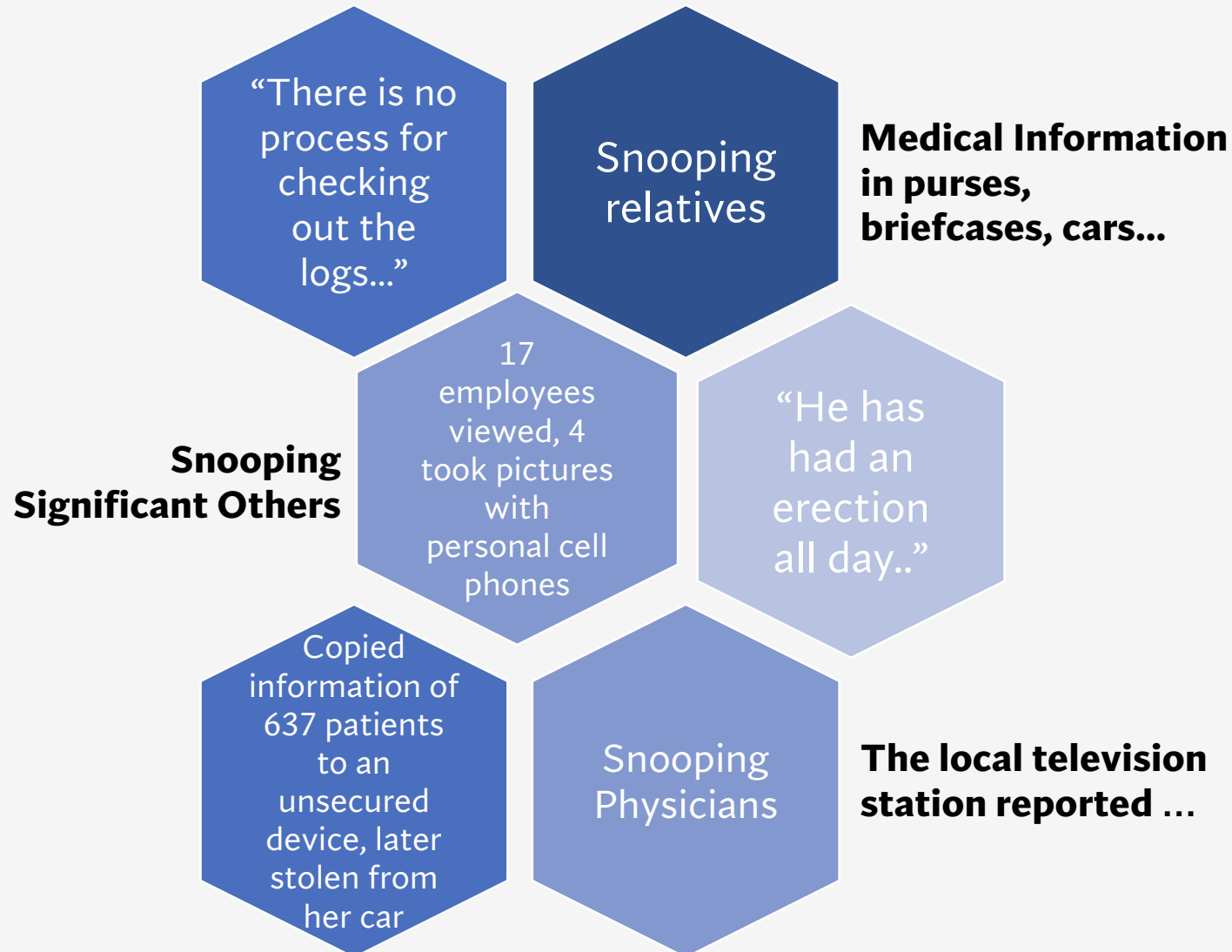
Resubmission Timeline:

Notice of Proposed Rulemaking Published: July 3, 2020
California Regulatory Notice Register: 2020, No. 27-Z
Public Hearing Date: None Scheduled
Start of the 45-Day Public Comment Period: July 3, 2020
Close of the 45-Day Public Comment Period: August 21, 2020
Start of the 15-Day Public Availability Period: December 8, 2020
Close of the 15-Day Public Availability Period: December 28, 2020

In the Event of a Potential Breach...



<http://atulgawande.com/book/the-checklist-manifesto/>



<https://www.cdph.ca.gov/Programs/CHCO/LCP/Pages/MedicalBreaches.aspx>



WHETHER TO REPORT?



**WHEN AND HOW TO
REPORT ?**



WHAT HAPPENS NEXT?



Whether to Report?

(1) Is there a breach?

HIPAA

- Unauthorized acquisition, access, use or disclosure
- Involves “**unsecured**”** “**protected health information**”

CA

- “Unlawful” or “unauthorized” access to, use or disclosure of
- **Patient “medical information**” – “individually identifiable” information “regarding a patient’s medical history, mental or physical condition, or treatment”

** “**unsecured**” = not encrypted or destroyed

(1)(a) HIPAA exclusions from “Breach”



Good faith, unintentional access / use by workforce member or BA without further access, use or distribution



Mistaken / accidental disclosure between similarly situated individuals that routinely handle PHI *at the same CE / BA / OHCA*



“Good faith belief” that the unauthorized person *could not reasonably have been able to retain [the] information*

"OCR acknowledges that the incident does not constitute a reportable breach under the Breach Notification Rule because the laptop was sufficiently encrypted."

(1)(b) CA Exclusions from “Breach”

NEW

Any paper record, electronic mail, or facsimile transmission inadvertently accessed, used, or disclosed **within the same health care facility or health care system** and the information “is not further accessed, used, or disclosed”

“Any paper record, electronic mail or facsimile transmission**sent to a covered entity** ...inadvertently misdirected within the course of coordinating care or delivering services.”

“*would not reasonably have been able to retain* such medical information” = HIPAA

“Any lost or stolen **encrypted electronic data** ...[that] has not been accessed, used, or disclosed in an unlawful or unauthorized manner.”

A disclosure where “there is a **low probability that the medical information has been compromised** based on a risk assessment”

- Encrypted hard drive with 50,000 patient HIV test results is lost. **HIPAA = No breach**
- Billing manager loses 3 patient “face sheets” when they blow off her car hood while she’s unlocking the door.
HIPAA = Breach
- An email about a dietary program is sent to 1000 patients in which the names and email addresses were visible to all recipients. **HIPAA = Breach**

- Encrypted hard drive with 50,000 patient HIV test results is lost. **HIPAA and CA = No breach**
- Billing manager loses 3 patient “face sheets” when they blow off her car hood while she’s unlocking the door.
HIPAA and probably CA = Breach
- An email about a dietary program is sent to 1000 patients in which the names and email addresses were visible to all recipients.
HIPAA = Breach, CA = No breach

- 1. Nature and extent of the PHI** involved
Limited? Partly deidentified? Diagnosis?
- 2. Who was the unauthorized person** who used / received the PHI
Another workforce member / CE /BA?
- 3. Was PHI actually viewed or acquired**
- 4. Extent of mitigation**
Returned? Reliably destroyed?

“At least”

- ❑ **Checklist** / Standardized format for evaluating
- ❑ Keep with related documentation
 - ❖ **CA “Centralized record” – at least 6 years**
- ❑ How would Aunt Matilda see it? (“Good Faith”)
- ❑ Show your work – because you might have to later
- ❑ Look for trends and take action to break them



(2) Is it reportable?

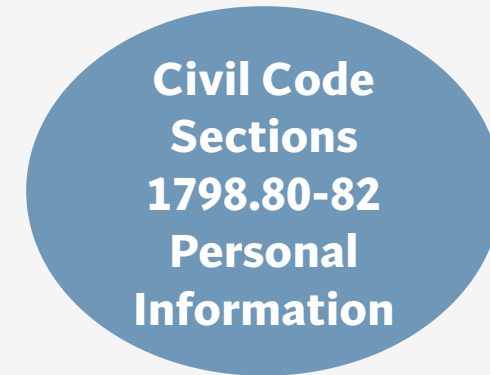
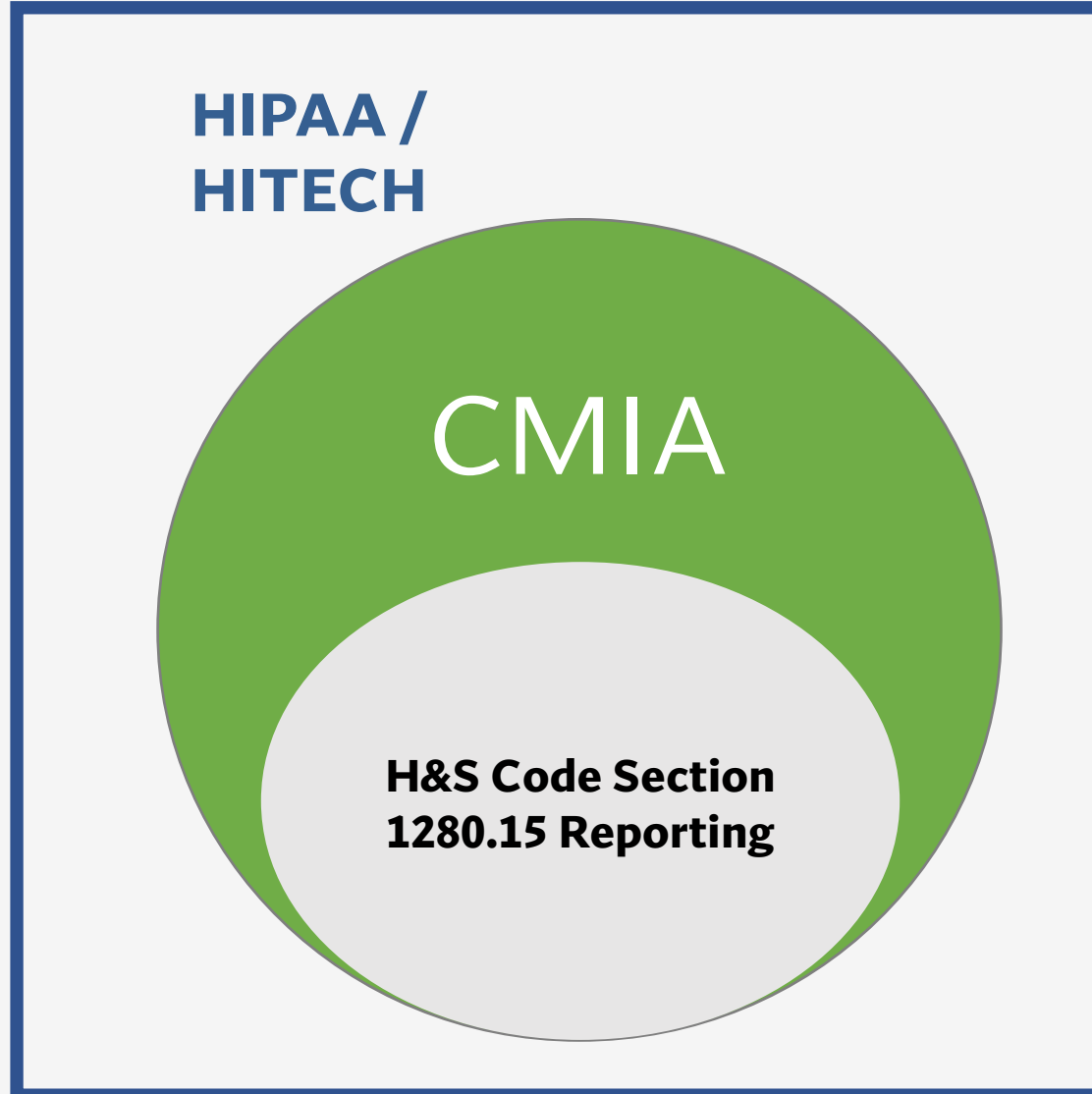
HIPAA

- “Covered entities” (CE) report
- “Business Associates” report to their CE – check BAA for time frame
- “Presumed” reporting unless the CE can document “low risk of compromise”




CA

- Reporting obligation limited to Licensed Health Facilities, Clinics, Home Care Agencies and Hospices

Who's covered?



Duty to report?

HIPAA / HITECH	CMIA	1798.82
<p>Providers</p> <p>Health Plans</p> <p>Healthcare Clearinghouses</p> <p>Their “Business Associates”</p>	<p>Providers</p> <p>Health Care Service Plans</p> <p>Pharmaceutical</p> <p>“Contactors”</p> <p>Business organized for the purpose of maintaining medical information</p>	<p>Businesses that own or license “personal information” of California residents</p>
<p>BAs do not self-report</p>	<p>Only certain providers self-report</p>	<p>But not “covered entities” required to provide notice by HIPAA / HITECH</p>
		



When and How to Report

HIPAA (45 CFR § 164.400-412)

- Notice required to the affected individuals and OCR* “without unreasonable delay” and in no case later than **60 calendar days** from time the CE knows or should have known of the breach

H&S Code § 1280.15 / 22 CCR § 79902

- Notice required to the affected individuals and the Department no later than **15 business days** after the health care facility detects that a breach occurred “or a breach [is] reasonably believed to have occurred”



UNLESS →



BA knowledge of breach now imputed to Facility?

- **Section 79901(j):** “Health care facility” means a clinic, health facility, home health agency or hospice licensed pursuant to section 1204, 1250, 1725, or 1745 of the Health and Safety Code. **For purposes of this chapter, a “health care facility” as it relates to a breach of a patient’s medical information shall include workforce members, medical staff, and business associates at the time of the breach and the detection of the breach.”**



TIP: Check the reporting requirements in your BAAs!

Don't forget....



Civil Code Section 1798.82

- Notice to affected CA residents shall be provided “in the most expedient time possible and without unreasonable delay, consistent with the legitimate needs of law enforcement ... or any measures necessary to determine the scope of the breach and restore the reasonable integrity of the data system.”

HIPAA (45 CFR § 164.400-412)

- Patient(s)/patient representative
 - In writing by first-class mail at last known address or by e-mail (if patient has agreed)
- HHS Secretary
 - 500 or more affected – Electronically submit notice via [OCR breach portal](#) + “prominent media outlets”
 - < 500 affected – within 60 days of calendar year end on [OCR breach portal](#)
- Media

Note: Substitute notice available in certain circumstances

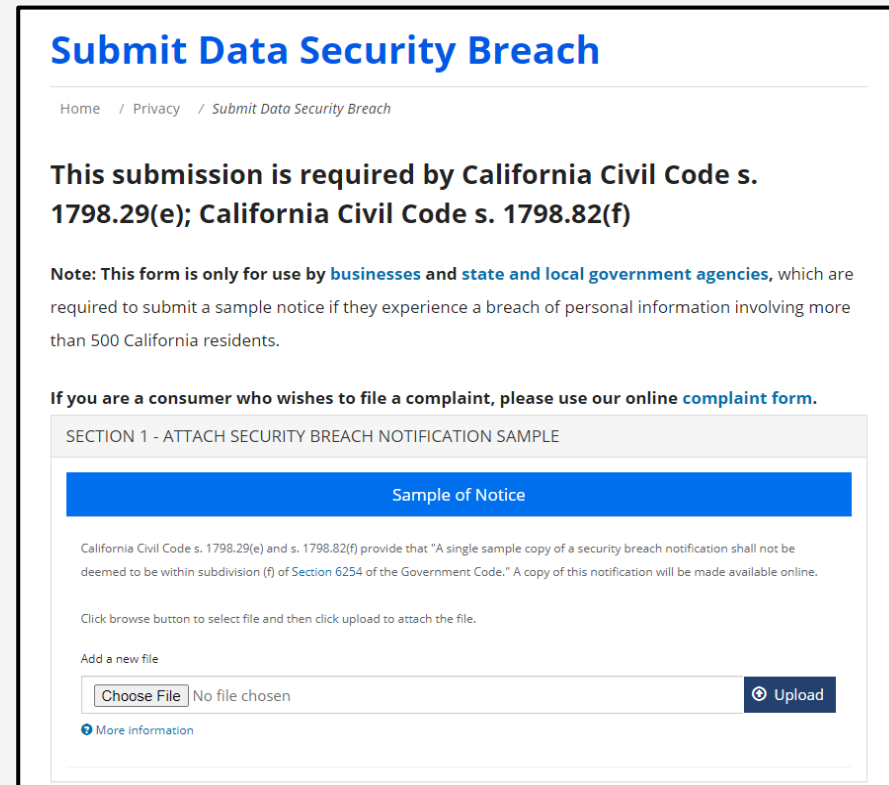
H&S Code § 1280.15 / 22 CCR § 79902

- Patient(s)/patient representative
 - In writing by first-class mail at last known address or by e-mail (if patient has agreed)
 - Substitute notice?
- CDPH
 - To local District Office by:
 - electronic mail,
 - telephone,
 - fax,
 - first-class mail, or
 - through an internet website maintained by the Department



Civil Code § 1798.82

- Affected CA Residents
 - Either by:
 - Written notice;
 - Electronic notice; or
 - Substitute notice (if cost of notice will exceed \$250,000, more than 500,000 affected, or insufficient contact information)
 - Patient notice meeting HIPAA requirements sufficient
- California Attorney General's Office (for 500+ residents)
 - Electronically submit template patient notice via [OAG Online Portal](#)



Submit Data Security Breach

Home / Privacy / Submit Data Security Breach

This submission is required by California Civil Code s. 1798.29(e); California Civil Code s. 1798.82(f)

Note: This form is only for use by **businesses and state and local government agencies**, which are required to submit a sample notice if they experience a breach of personal information involving more than 500 California residents.

If you are a consumer who wishes to file a complaint, please use our online [complaint form](#).

SECTION 1 - ATTACH SECURITY BREACH NOTIFICATION SAMPLE

Sample of Notice

California Civil Code s. 1798.29(e) and s. 1798.82(f) provide that "A single sample copy of a security breach notification shall not be deemed to be within subdivision (f) of Section 6254 of the Government Code." A copy of this notification will be made available online.

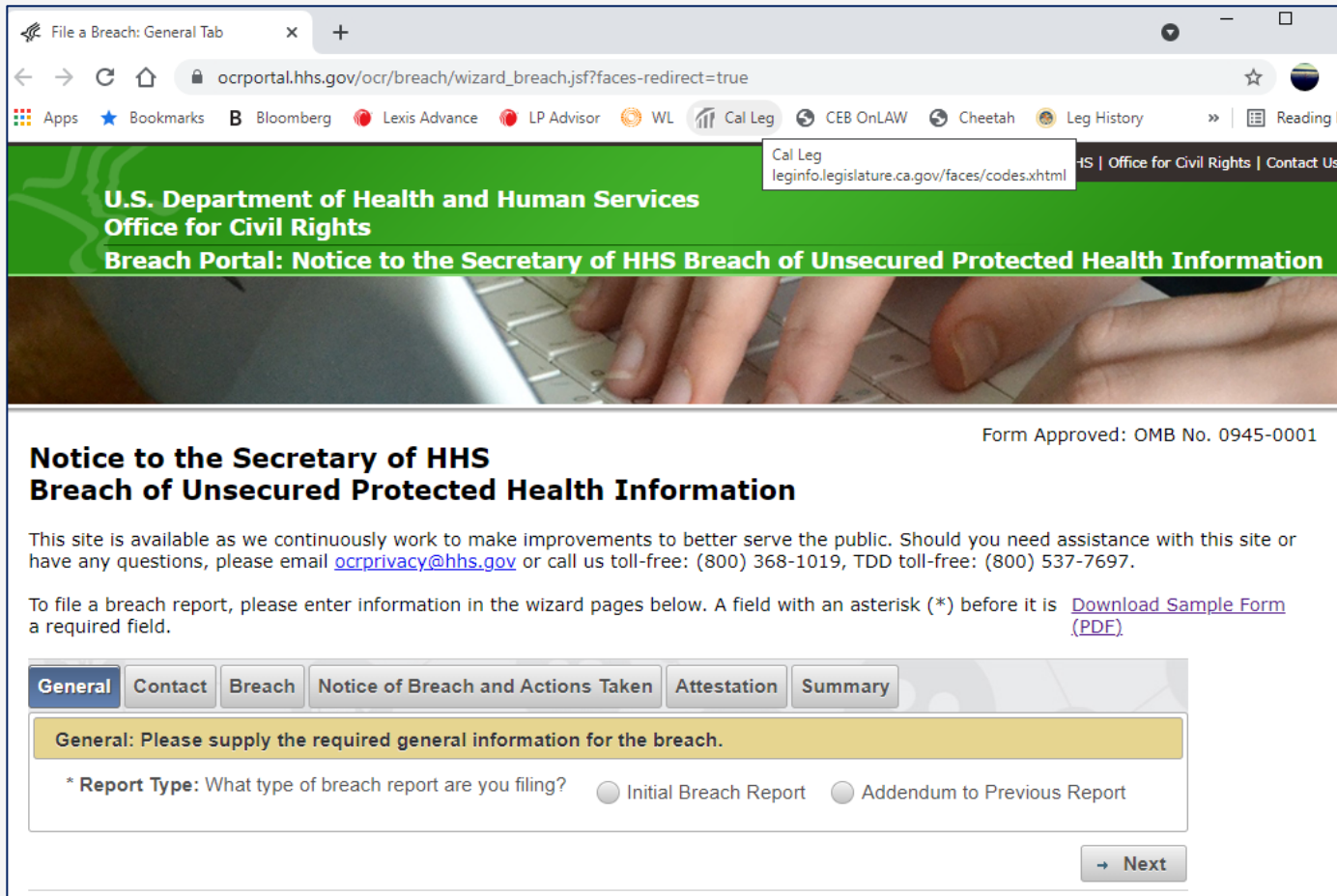
Click browse button to select file and then click upload to attach the file.

Add a new file

No file chosen

[More information](#)

Notice to HHS Secretary - HIPAA



The screenshot shows a web browser window with the URL ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf?faces-redirect=true. The page header includes the U.S. Department of Health and Human Services, Office for Civil Rights, and the title "Breach Portal: Notice to the Secretary of HHS Breach of Unsecured Protected Health Information". The form is titled "Notice to the Secretary of HHS Breach of Unsecured Protected Health Information" and includes a "Form Approved: OMB No. 0945-0001" label. A disclaimer states: "This site is available as we continuously work to make improvements to better serve the public. Should you need assistance with this site or have any questions, please email ocrprivacy@hhs.gov or call us toll-free: (800) 368-1019, TDD toll-free: (800) 537-7697." Instructions for filing a breach report are provided, including a link to "Download Sample Form (PDF)". The form has tabs for "General", "Contact", "Breach", "Notice of Breach and Actions Taken", "Attestation", and "Summary". The "General" tab is active, showing a yellow box with the instruction: "General: Please supply the required general information for the breach." Below this, there is a field for "* Report Type: What type of breach report are you filing?" with two radio button options: "Initial Breach Report" and "Addendum to Previous Report". A "Next" button is located at the bottom right of the form.

- General info;
- Contact info;
- Description of breach;
- Type of PHI involved;
- Existing safeguards;
- Notice of breach and actions taken in response; and
- An attestation

Notice to CDPH by Facility (excluding a BA) – HSC 1280.15 & Section 79902(a)(1)

- Description of what happened, including: name and address of facility, date and time breach occurred and was detected, and events surrounding the breach;
- A description of medical information involved in the breach;
- **Names of *all* affected patients;**
- Names and contact information of the individuals who performed the breach, any witnesses to the breach and any unauthorized persons who used the medical information or to whom it was disclosed;
- The dates of patient notice and a copy of the same;
- The contact information of a health care facility representative who the Department can contact for additional information;
- Description of any corrective or mitigating action taken by the facility;
- **Any other instances of a reported event that includes a breach of the same patients' medical information by the facility within the last six years;** and
- **Any audit reports, written statements, or other documents that the health care facility relied upon in determining that a breach occurred.**

What caused the breach:	What OCR and CDPH likely looking for:
Employee / contractor(s) doesn't follow procedure	Counseling / peer review / other sanction Supervision failure? Review of procedure's adequacy – new controls? Checklist? Process change? Retraining Employee acknowledgement forms Monitoring process
Insider intentionally accesses or discloses data for gain / personal use	They're out of there ... Law enforcement involved Retrain whoever is left
Theft of stationary device / stored data	Better physical security measures – relocation, cameras, alarms, biometrics, steel doors; off-site back-up; a better grade of lock; encryption
Theft / loss of mobile device	Encryption
Theft / loss of paper	Better physical security provisions; take the process electronic

Civil Code Section 1798.82 – Notice to California Attorney General

- Sample notice to affected individuals and date(s) provided;
- Certain info for “law enforcement purposes”;
- Date(s) of breach (if known) and discovery of breach;
- Type of personal info involved in breach;
- Brief description of breach; and
- Contact information



HIPAA (45 CFR Section 164.404) & Section 79902(b)(1)

- Brief description of what happened, including the facility's name, date of breach and date of discovery;
- A description of medical information involved in the breach;
- Any steps the patient should take to protect himself or herself from potential harm resulting from the breach;
- A brief description of what the facility is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches;
- Contact information (a toll-free telephone number, an e-mail address, internet website address, or postal address); and
- In plain language



HIPAA (45 CFR Section 164.404) & Section 79902(b)(1)

Notice may be delegated to business associate depending on which entity is in the “best position to provide notice to the individual”



Civil Code Section 1798.82 – Notice to Affected CA Residents

- Titled “Notice of Data Breach,” and use following headings, both of which should be “clearly and conspicuously displayed”:
 1. “What Happened” (including date of breach),
 2. “What Information Was Involved,”
 3. “What We Are Doing,”
 4. “What You Can Do,” and
 5. “For More Information”
- Written in plain language and no smaller than 10-pt type;
- Toll-free telephone numbers and addresses of the major credit reporting agencies if SSN or driver’s license # involved;
- With SSN, driver’s license # involved also need “an offer to provide appropriate identity theft prevention and mitigation services”



<https://oag.ca.gov/privacy/databreach/list>



- ✓ Provide the notice as soon as possible
- ✓ Draft carefully to ensure notice content requirements are met and to avoid potential civil liability exposure under the CMIA
- ✓ Be sincere
- ✓ “High Up” signer
- ✓ Make it easy to raise questions / concerns



What Happens Next?

California

CDPH follow-up

- Information requests
- Onsite investigation
- 2567 (Public document)
- Fine(s)
- Appeal

Patient – civil suit for nominal and actual damages

Other civil suit (AG etc.)

The Feds

OCR follow-up

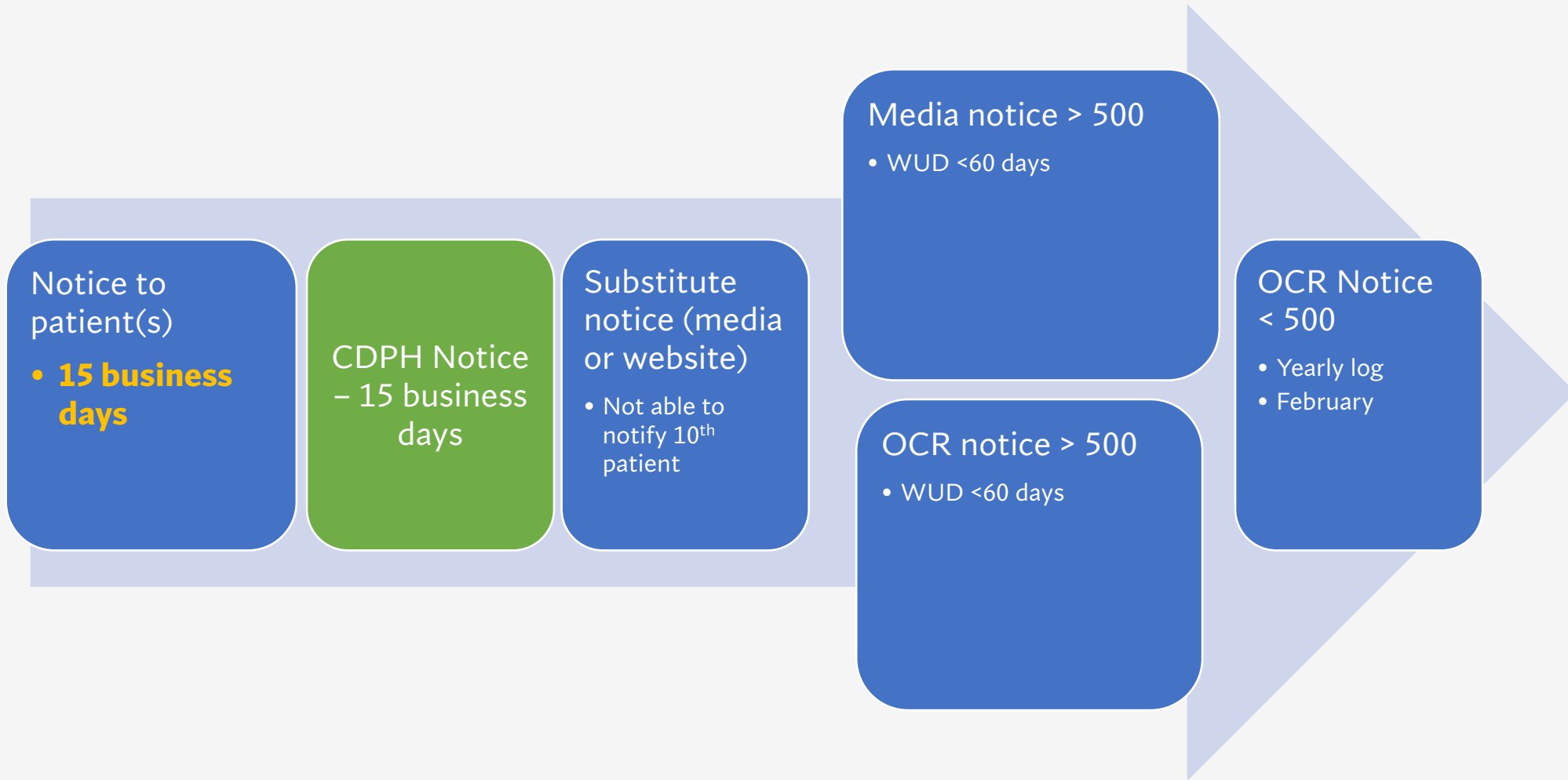
- > 500
- Particularly egregious facts

Corrective Action

Fine + Resolution Agreement

No private right of action

- Lawyerly creativity



What were the pre-breach compliance efforts?

- Plan for monitoring / auditing of access
- Role based access
- Role based training / competency validated
- Training updated based on lessons learned
- Employee “acknowledgement” forms
- Well advertised Hotline - available to public
- Walk around “rounds” of the facility

“Reasonable and appropriate corrective action after the release”

- Remove lost device's access to server
- Written assurance of deletion / return / destruction
- Call Center – sufficient staffing
- Forensic confirmation
- Prospective auditing of involved accounts
- Counseling

“Preventative Action” Checklist



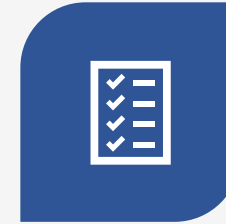
**PROCESS CHANGE(S)
MADE? IN WRITING?**



**STAFF IN-SERVICED?
WHO, WHAT, HOW?
CHECK FOR
EFFECTIVENESS /
COMPETENCY?**



**“LESSON” SHARED AND
/ OR APPLIED
ELSEWHERE IN THE
FACILITY?**



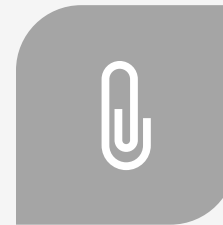
**MONITORING OR
AUDITING THE NEW
PROCESS? WHERE IS
THIS REPORTED?**



PATIENT(S) NOTIFIED?



**WHAT HAPPENED TO
INVOLVED STAFF /
PHYSICIANS /
CONTRACTORS?**



**NEW POLICY OR
TRAINING MATERIAL TO
ATTACH?**



- Mis-steppers and their supervisors reprimanded / counseled
- Intentional snoopers - terminated
- Involvement of medical staff in process / policy changes
- Increased auditing – reported regularly somewhere meaningful
- Reports to governing body

HIPAA

- CMPs for violations determined on a tiered structure
- HHS Secretary determines amount “based on the nature and extent of the violation and the nature and extent of the harm resulting from the violation”
 - Currently between \$119 to \$59,522 per violation with yearly cap
- Penalties may not be imposed (except in cases of willful neglect) if violation corrected within 30 days
- Criminal penalties available; no private right of action

H&S Code Section 1280.15, 22 CCR Section 79905

- CDPH authorized to assess up to \$25,000 per patient, and up to \$17,500 per subsequent occurrence, even if no delay in reporting
- **Regs set base penalty at \$15,000 for initial violation, and 70% of that amount for subsequent violations**
- \$100 may be assessed for each day a facility fails to report the breach to the Department or to a patient
- Total penalty asserted may not exceed \$250,000
- No private right of action

Civil/B&P Codes

- Private right of action by consumers under CMIA (nominal damages of \$1000 per violation) and 1798.84
- Civil penalties, ranging from \$2,500 for negligent disclosures of medical information in violation of CMIA to \$250,000 for knowing and willful disclosures for the purpose of financial gain and under the CMIA
- Potential criminal liability exposure under CMIA
- Civil penalties under CA Unfair Practices Act?

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

Press Release / Attorney General Becerra Announces Landmark Settlement Again...



Thursday, September 17, 2020

Contact: (916) 210-6000, agpressooffice@doj.ca.gov

SACRAMENTO – California Attorney General Xavier Becerra today announced a landmark settlement against Glow, Inc. (Glow), a technology company that operates a fertility-tracking mobile app that stores personal and medical information. The settlement, which is subject to court approval, resolves the Attorney General’s investigation of Glow’s app for serious privacy and basic security failures that put women’s highly-sensitive personal and medical information at risk. In addition to a \$250,000 civil penalty, the settlement includes injunctive terms that require Glow to comply with state consumer protection and privacy laws, and a first-ever injunctive term that requires Glow to consider how privacy or security lapses may uniquely impact women.

“When you meet with your doctor or healthcare provider in person, you know that your sensitive information is protected. It should be no different when you use healthcare apps over the internet,” **said Attorney General Becerra**. “Mobile apps, like Glow, that make it their business to collect sensitive medical information know they must ensure your privacy and security. Excuses are not an option. A digital disclosure of your private medical records is instantaneously and eternally available to the world. Today’s settlement is a wake up call not just for Glow, Inc., but for every app maker that handles sensitive private data.”

The Attorney General’s complaint alleges the Glow app:

H&S Code Section 1280.15 states that:

- The Department, in investigating a breach and assessing a penalty, consider the health facility’s “history of compliance with this section and other related state and federal statutes and regulations, the extent to which the facility detected violations and took preventative action to immediately correct and prevent past violations from recurring, and factors outside its control that restricted the facility’s ability to comply with this section,” and permits the Department to consider any other factors in its full discretion.

The regulations under Section 79904 allow the base penalty to be increased or decreased by up to \$10,000 based on:



- The health care facility’s compliance history of compliance for the past three years;
- The extent to which the health care facility detected violations and took preventative action to immediately correct and prevent past violations from recurring;
- Factors “**outside the control of the health care facility**” as defined by Section 79901(i);
- Any other factors applicable to the specific circumstances surrounding the breach, as identified by the Department; or
- If the Department determines that the penalty is somehow “unduly burdensome or excessive”

What constitute “factors outside the control of the health care facility” under Section 79901(i)?

Includes, for example:

- Fires
- Explosions
- Natural disasters and severe weather events
- Civil unrest
- War
- Invasion
- Terrorism
- Utility or infrastructure failure

... BUT explicitly does not include:

“The acts of the health care facility, business associate, or their respective workforce members.”



Penalty Adjustments Available For:

- **Small and Rural Hospitals**
 - Hospital must submit its written request for penalty modification to the Department within 10 calendar days after the issuance of an administrative penalty describing the specific circumstances showing financial hardship to the hospital and the potential adverse effects on access to quality care in the hospital
- **Primary Care Clinics**
 - To protect access to quality care in those facilities
- **Skilled Nursing Facilities**
 - Department may issue the higher of a penalty under H&S Code Section 1280.15 or Section 1417, but not both





Ready for a Checklist Now?

HIPAA vs HIPPA

	HIPAA	HIPPA
Name	Health Insurance Portability and Accountability Act	Health Information Privacy Protection Act
Protects health coverage for people who change jobs.	✓	✗
Requires medical providers to give patients access to their personal health information	✓	✗
Requires medical providers to protect the privacy of health information	✓	✓
Prohibits stores and restaurants from asking for proof of vaccination	✗	✓
Prohibits stores and restaurants from requiring you to wear a mask	✗	✓
Prohibits anyone from asking you for any health information for any reason	✗	✓
History	Passed by Congress and signed into law by President Bill Clinton in 1996.	Invented by people on the internet during the COVID-19 pandemic.
Is it a real law?	✓	✗

Submit your questions through the Q & A box. (Usually located at the bottom of your screen.)

Andrea L. Frey

Hooper, Lundy & Bookman, P.C.

afrey@health-law.com

Martha Ann (Marty) Knutson

Riverside County

MKnutson@rivco.org

Lois Richardson

California Hospital Association

lrichardson@calhospital.org

Thank You

Thank you for participating in today's webinar.

You will receive an evaluation shortly. Full attendance and completion of the online evaluation and attestation of attendance are required to receive CEs

A recording of the program will be sent to each attendee.

For education questions, contact:

education@calhospital.org



California
Hospital
Association

1215 K Street, Suite 700

Sacramento, CA 95814

(916) 443-7401

www.calhospital.org

© California Hospital Association 2021