Complying with California's New Medical Information Breach Regulations

CAHF 2021 Annual Convention & Expo

Anderson Health Information Systems, Inc.

Hooper, Lundy & Bookman, PC

Rhonda Anderson, RHIA, QCP

President & Founder, AHIS Consulting

- Administrative, Health Information & Quality Management consulting expertise in post-acute care, ICF-ID, Psychiatric & Dialysis
- Past President CHIA
- Served on many national and state AHIMA, CHIA & CAHF committees; CAHF Speaker
- 37 years with AHIS Consulting

Today's Presenters

Barbara Phillips, RHIT, QCP, RAC-CT

Senior Consultant, AHIS Consulting

- Expertise in regulatory & legal compliance
- HIPAA Privacy and Security Compliance knowledge
- CAHF speaker
- 25 years of experience in post-acute care
- 15 years with AHIS Consulting

Today's Presenter

Andrea Frey, JD, MPH

Associate Attorney, Hooper, Lundy & Bookman, PC

- Co-chair of the firm's Digital Health Task Force
- Practice focuses on transactional and health care regulatory matters, with an emphasis on health privacy, digital health, licensure and certification, scope of practice, and medical staff issues

Disclaimer

- This webinar was developed as a general educational offering and reference for long-term care professionals and is not intended as legal advice nor should it be a substitute for professional advice in any specific situation
- To the best of our knowledge, it reflects current state and federal regulations and practices. The examples used do not represent the employer of the presenter or any preferred electronic health record system or health information technology

Objectives

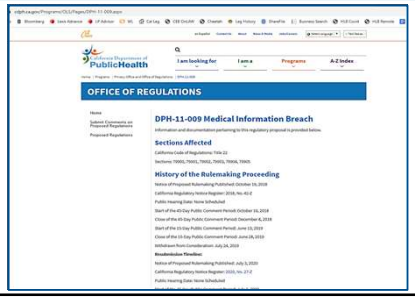
Participants will identify:

- New medical breach regulations and what they require of licensed health care facilities
- What's changed under the new regulations and how they are different from federal requirements
- Practical considerations and takeaways around revising policies and procedures to promote compliance

Abbreviations and Acronyms

• BA	Business Associate
• CE	Covered Entity
• CDPH	California Department of Public Health
• HIPAA	Health Information Portability and Accountability Act
• HHS	Dept of. Health & Human Services
• IIHI	Individually Identifiable Health Information
• OCR	Office for Civil Rights
• OHCA	Organized Health Care Arrangement
• PHI	Protected Health Information

CDPH Breach Regs Effective July 1, 2021



7

The Three Questions

WHETHER TO REPORT?

WHEN AND HOW TO REPORT ?

WHAT HAPPENS NEXT?

8

Whether to report: Is there a breach?

HIPAA	CA H&S Code § 1280.15 / 22 CCR § 79900
• Unauthorized acquisition, access, use or disclosure • Involves "**unsecured**"** "**protected health information**"	• "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

9

Exclusions from Breach Under HIPAA

- ***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***

10

Exclusions from Breach Under CDPH Regulations

		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"	"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"

11

Suspected/Confirmed Breach Documentation

- Perform preliminary fact finding to determine
  - Nature of breach
  - Verification of resident(s) impacted
- Initiate a Breach Log for a <u>suspected or confirmed breach</u> including:
  - Type of breach
  - Risk assessed
  - Steps to mitigate
  - Notifications

12

Breach Log

- Example, not full form

Breach Log & Risk Assessment

Name of Facility: _____

Person Completing Breach Information: _____ Date: _____

Breach Date: _____ Discovery Date: _____

Individual Affected: _____ Type of Breach: _____

Hacking Incident: [ ] Improper Disposal [ ] Loss [ ] Theft
[ ] Unauthorized Access/Disclosure

Location of Breach: [ ] Electronic Medical Records [ ] Email [ ] Laptop
[ ] Network Server [ ] Other Portable Electronic Device
[ ] Paper/Film [ ] Other

Type of Protected Health [ ] Clinical [ ] Demographic
Information Involved in Breach: [ ] Financial [ ] Other

Brief Description _____

Safeguards in Place Prior to Breach: [ ] None
[ ] Privacy Rule Safeguards (Training, Policies/Procedures, etc.)
[ ] Security Rule Administrative Safeguards (Risk Analysis, Risk Management, etc.)
[ ] Security Rule Physical Safeguards (Facility Access Controls, Workstation Security, etc.)
[ ] Security Rule Technical Safeguards (Access Controls, Transmission Security, etc.)

13

Suspected/Confirmed Breach Documentation

- Facility or BA must demonstrate notifications
  - Breach Notification Checklist
- Complete Risk Assessment Checklist
  - Analyze and score elements of a possible breach
  - Use to determine **impact and severity** of risk of improper use or disclosure

14

Breach Notification Checklist

- Example, not full form

HIPAA BREACH NOTIFICATION CHECKLIST
CONFIDENTIAL

#	YES	NO	TYPE OF MEDIUM BREACHED
1.	☐	☐	Computerized data (includes emails, faxes)
2.	☐	☐	Encrypted
3.	☐	☐	Paper
4.	☐	☐	Oral

#	YES	NO	DATA ELEMENTS BREACHED
1.	☐	☐	Name of Individual(s)
2.			If "Yes, to #1", please enter the number of individuals
3.	☐	☐	Postal Address Information
4.	☐	☐	Zip Code(s)
5.	☐	☐	Date(s) of Birth
6.	☐	☐	Telephone Number(s)

15

Risk Assessment Scoring Checklist Example

Item	No	Yes, Likelihood	Impact	Risk Assessment Score = Likelihood × Impact
Nature and Extent				
Patient identifiers were used or disclosed? Describe: _____				
Does the PHI used or disclosed contain a diagnosis?				
Does the amount of PHI used or disclosed increase the risk? ☐ Small and not identifiable, ☐ identifies individual				
Does the PHI used or disclosed include sufficient indirect patient identifiers that could make re-identification of the individuals possible?				
Unauthorized Person				
Does the unauthorized recipient have obligations to protect the privacy and security of the disclosed information such as a BA or another CE?				
Is the recipient a member of your internal workforce or a BA such that you can assure that the PHI will not be further used or disclosed?				

(not full form)

16

Risk Assessment Scoring Likelihood x Impact

***Likelihood**
- **1.0 = High**: More than likely could be impermissibly used or disclosed
- **0.5 = Medium**: May be impermissibly used or disclosed
- **0.1 = Low**: Minimal, rare, or seldom probability of being impermissibly used or disclosed

✖

****Impact**
- **100 = Severe**: Easily identifies patient / could be impermissibly used or disclosed
- **50 = Moderate**: Has potential of identifying the patient / probability of improper use or disclosure is uncertain
- **10 = Minimal**: May or may not identify the patient /satisfactory assurances obtained information will not be impermissibly used or disclosed

17

Risk Assessment Scoring Checklist

- Total Risk Assessment Score determines level of risk.
- A score of 10 or below indicates low risk
  - Incident may not need to be reported

18

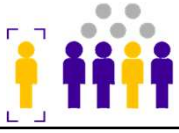
Breach Risk Assessment

- Use a Checklist/Tool to assess each of these areas
  - Nature and extent of PHI disclosed
  - Use or disclosure by unauthorized person
  - Circumstances surrounding acquisition/viewing of PHI/IIHI
  - Extent risk has been mitigated/recommended mitigation actions

19

Nature and Extent of the Breach

- Assess resident identifiers used or disclosed
  - Sensitive diagnosis, like AIDS, or a mental illness?
  - Amount disclosed increases risk?
  - Information contains enough to re-identify a person
    - By reading or hearing could identify the person?
    - Person is well-known individual, i.e., celebrity or a business leader?



20

Access/Disclosure by Unauthorized Person

- Person who has an obligation to protect the PHI
  - Staff member or business associate
  - Determine if Information likely will not be further disclosed
- Person has a relationship with the individual whose information was disclosed
  - Likely to act in that individual's best interest?

21

Access/Disclosure by Unauthorized Person_2

- Assess possible motivation behind the person's use or viewing of information
  - Accessed in error, or intentional?
  - Malicious, self-serving, or harmful intent involved?
- Did the person who viewed the PHI deliberately seek it out?
- Is there any reason to believe there was an intent to use it for personal gain, or sell it?

22

Access/Disclosure by Unauthorized Person_3

- Attitude of the person who saw or used the PHI – did person:
  - Report it?
  - Show willingness to work with the facility, speak openly, and show concern?
  - Show reluctance to discuss
  - Seem to use the occurrence as leverage to get something they wanted?

23

Unauthorize Acquisition/ Viewing of PHI

- Possible to demonstrate PHI was never actually accessed, viewed, or acquired?
- Electronic format: can a computer analyst show that the information was accessed, viewed, transmitted, or compromised, e.g., by a hacker?

24

Mitigation

- If individual who accessed PHI was a direct employee or Business Associate
  - Can they confirm verbally information was subsequently destroyed?
  - If not, will person who accessed information submit written confirmation PHI was destroyed?
  - If paper-based, were documents containing PHI returned to the facility timely and completely?

25

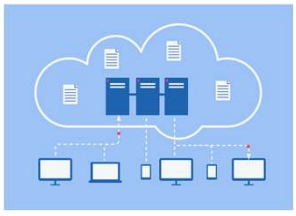
Risk Assessment Outcome

- Determination that probability of compromise is low
  - Incident may not need to be reported **however** have on file Assurance
    - Destruction by the unauthorized accessor
    - PHI will not be further used or disclosed
- Higher level of risk is reportable
- Doubt? – REPORT/NOTIFY

26

Risk Assessment Outcome

- Document all notifications/reports
  - If risk assessment is not completed -Low probability cannot be demonstrated
- Maintain risk assessment and all materials NEW!
  - Six years
  - **Including** those where the incident does not constitute a reportable breach



27

How and When to Report

HIPAA

- 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
- Media notice may be required in certain instances

CDPH

- 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 →

28

How and When to Report

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."
- Notice to AG for 500+ CA residents

29

CDPH Reporting Requirements

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!

30

HHS Reporting Requirements: OCR Notice & Contents

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

https://ocrportal.hhs.gov/ocr/breach/wizard_breach.jsf

31

CDPH Reporting Requirements: Department Notice & Contents

- Description of:
  - What happened, including: name and address of facility, date and time breach occurred and was detected, and events surrounding the breach;
  - Medical information involved in the breach;
- **Names of *all* affected patients;**
- Names and contact information of 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;
- Dates of patient notice and a copy of the same;

NEW

32

CDPH Reporting Requirements: Department Notice & Contents_2

- 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.**

NEW

33

Breach Reporting Form Example

BREACH INCIDENT REPORT FORM

All medical information breaches shall be reported to the department no later than 15 business days after the breach has been detected (per HSC 1280.15 (b)(1)). Please complete and submit this form to your local District Office. For a list of our District Offices, visit our website at: https://www.cdph.ca.gov/Programs/CHCQ/LCP/Pages/DistrictOffices.aspx. You may also fill out a report using CalHEART online at https://healthcarereportal.cdph.ca.gov.

Facility Information

Facility Name:*

Facility Address:* Street Address ____ Suite/Unit# ____

City ____ State ____ Zip Code ____

Contact Person:* Last Name ____ First Name ____

Primary Phone:* ____ Alternate Phone: ____

Email Address:* ____

Date of Reports:* ____

(not full form)

34

HHS & CDPH Reporting Requirements: Patient Notice & Contents

- Brief description (*in plain language*) of:
  - What happened, including the facility's name, date of breach and date of discovery;
  - Medical information involved in the breach;
  - Steps the patient should take to protect himself or herself from potential harm resulting from the breach; and
  - 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)

35

What happens next? Mitigation Efforts

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 (misstepper, those in similar position) 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

What happens next? Penalties & Potential Liability

HIPAA	H&S Code Section 1280.15, 22 CCR Section 79905	Civil/B&P Codes
• 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	• 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	• 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?

37

What happens next? CDPH Administrative Penalties

The regulations 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"

+ Penalty adjustments for SNFs

- Department may issue the higher of a penalty under H&S Code Section 1280.15 or Section 1417, but not both

38

What happens next? CDPH Administrative Penalties

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."

39

Note on Services via Telehealth

Current compliance & enforcement flexibilities under HIPAA and CA law

- Allow use of electronic platforms like FaceTime and Zoom
- Relaxed enforcement of sanctions TEMPORARY during Public Health Emergency

*But still important to do breach risk assessment and report if anything other than low risk

40

Thank You for Attending!