Tool: Sample Report Comparing State/Federal Privacy Breach Regulations

San Diego-based Martha Ann (Marty) Knutson, attorney and counselor at law, developed the following table that outlines federal and California requirements for protected health information (PHI) privacy breaches. Knutson's table could be used as a template for other states. "Every state hospital association could commission a review of its laws and compare them to the HITECH breach reporting requirements," she says. Legal counsel should assist in that review, of course.

Medical privacy laws are catalogued at the website of Georgetown University's Center on Medical Record Rights and Privacy. According to the National Conference of State Legislatures (NCSL), 46 states have a security breach notification requirement. (Alabama, Kentucky, New Mexico, and South Dakota apparently do not.) The state laws are listed at the NCSL website, and they typically cover breaches of various types of personal information, whether health-related or not.

Source: Martha Ann (Marty) Knutson is an attorney and counselor at law, San Diego (mak@mknutsonlaw.com).

Reporting Obligations for Medical Record Privacy Breaches in California

Authority	Who Must Report	What Must Be Reported	To	How Quickly	Possible Consequences
CMIA	Licensed Health Facilities, Clinics, Home Care Agencies and Hospices in California (*reporting requirement does not include individual licensed providers*)	"unlawful" or "unauthorized" access to, use or disclosure of patient medical information (see page 2)	CDPH and Patient	5 business days from "detection" (unless law enforcement requests a delay)	• Investigation of intentional or large breaches by CDPH / DHHS • Corrective Action Plan costs • Civil fines or misdemeanor conviction for underlying act (access, use, disclosure) • Fines for delays in reporting • "Resolution Agreement" costs, including independent monitoring • CDPH may refer breaches involving licensed individuals to OHII and licensing boards • Reputational harm • Civil suits • Enforcement action by state AG (HIPAA and CMIA), DAs, city attorneys, etc. (CMIA only)
HITECH	HIPAA "covered entities" (CE) – *including individual licensed providers, health plans, and health care clearinghouses*	"Breaches" = violations of the HIPAA privacy rule that involve "unsecured"** information and carry a significant risk of financial, reputational or other harm to the individual (*based on a documented risk assessment – see page 3*) ** "unsecured" = not encrypted or destroyed	Patient and DHHS Media (maybe)	To patient - "without unreasonable delay", but no later than 60 days from time the CE knew or should have known of the breach (unless law enforcement requests a delay) To DHHS Secretary (> 500 individuals = same time frame as patient; (< 500 individuals = annual report no later than February 29) To Media –if > 500 patients single state or jurisdiction = same time frame as patient;	

CMIA = Confidentiality of Medical Information Act, Cal. Civ. Code §§ 56.05-56.37 and Cal. H. & S. Code § 1280.15
CPDH = California Department of Public Health
DHHS = U.S. Department of Health and Human Services
HITECH = Health Information Technology for Economic and Clinical Health Act (included in the February 2009 stimulus bill, Pub. L. 111–5)
OHII = California Office of Health Information Integrity

Reporting Obligations for Medical Record Privacy Breaches in California

California Reporting

Health and Safety Code Section 1280.15

All Facilities letters:
7/29/2009
11/19/2009

Cal. Admin. Code Title 22, § 70707

Must report:

- Use, access or disclosure that is - "**unlawful**" (no definition) or "**unauthorized**" = "inappropriate access, review, or viewing of patient medical information without a direct need for medical diagnosis, treatment, or other lawful use"
- **Other "lawful" uses and disclosures** without execution of an "authorization" by the patient **do not need to be reported.** *These include*: mandated reporting to public agencies, obtaining payment, pursuant to court orders, search warrants and subpoenas, utilization and quality review, organ donation, to family directly involved in the patient's care, providing directory information**.**
- **Inadvertent misdirection** "within the same facility or health care system within the course of coordinating care or delivering services" is not reportable.

Format:

Patient report – no set requirements except directing to last known address. (*But see federal requirements on p.3*)

CDPH Report should include:

- Date and time of reported incident
- Facility name
- Facility address/location
- Facility contact person
- Name of patient(s)
- Name of the alleged violator(s)
- General information about the circumstances surrounding the breach
- Any other information needed to make the determination for an onsite investigation

"In assessing penalties, "the department shall consider the [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."

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?
- ☐ Patients(s) notified?
- ☐ What happened to involved staff / physicians / contractors?
- ☐ New training material to attach?

Reporting Obligations for Medical Record Privacy Breaches in California

Federal Reporting

HITECH Interim Final Regulation, Breach Notification 74 **Fed. Reg.** 42740 (2009), codified at 45 **C.F.R.** §164.400 et seq.

OMB Memorandum M–07–16 (2007)

Must report:

- Access, uses and disclosures that "pose a **significant risk of financial, reputational or other harm to the individual**"
- A "**documented risk assessment**" is required if the CE decides the risk is not "significant" enough to report

Notice Requirements:

Individual notices (and media, if required) must contain:

- **what happened**, included dates of breach and discovery, if known;
- **types of information involved** (name, address, SSN, DOB, diagnosis codes, etc.);
- **what individuals should do** to protect themselves;
- **what the CE is doing** to investigate, mitigate harm and protect against further breaches;
- **Contact procedures for questions / further information** (must include 800 number, email, website or postal address)

Substitute notice - "Conspicuous notice" on the homepage of CE's website or to "major" media with an 800 number is required if insufficient or out of date contact info for >10 patients

DHHS Notification forms – online at www.hhs.gov/ocr/privacy/hipaa/administrative/breachnotificationrule

"Breach" Exceptions - need not report:
(1) unintentional access, use by workforce member without further distribution; (2) mistaken / accidental disclosure between similarly situated individuals that routinely handle PHI; (3) disclosure where the unauthorized person "could not reasonably retain the information"

Risk Assessment Criteria:

1. What elements were in the breached data?
2. Is it likely that the information is accessible or usable to others?
3. Did the context of the disclosure create greater risk of harm? (e.g. revealing a diagnosis)
4. Do the recipient(s) have any duty not to further disclose the data?
5. Does the information have potential value – i.e. use or sale to others?
6. Is it likely that the disclosure will cause:
    a. Identity theft
    b. Blackmail
    c. Humiliation
    d. Fear
    e. Discrimination, prejudice, harassment
    f. Other reputational harm
7. Is there / was there any mitigation of the potential harm?

Reporting Obligations for Medical Record Privacy Breaches in California

Examples of reported violations	
	California penalties assessed*
Intentional "curiosity" access	$100,000 (17 employees / 33 patient records) $250,000 (21 employees, two physicians / 1 patient) $250,000 (1 employee, 204 patient records) $130,000 (Physician staff, physician, contractors, employee / 1 patient) $95,000 (2 employees, 2 contractors / 1 patient)(second incident)
Intentional access / disclosure for criminal purpose	$125,000 (4 face sheets taken, used for identity theft) $225,000 (9 patient records accessed, used for identity theft)
Intentional access / disclosure to co-worker, relative	$60,000 (Access and disclosure of child's record to relative) $60,000 (Access and disclosure to patient's mother and sister) $25,000 (Access and disclosure of child's record to mother)
Intentional disclosure outside facility	$42,500 (Cellphone discussion and "Myspace" posting) <penalty pending> (5 employees took and distributed pictures of trauma patient) <penalty pending> (2 employees took and distributed pictures of amputated leg)
Unintentional loss / disclosure	$250,000 (records relating to 596 patients missing from unlocked "storage locker") $75,000 (visitor allowed access to restricted area, overheard two patient registration interviews) $25,000 (patient 2's lab results misfiled in patient 1's record which was subpoenaed) <penalty pending> (Backpack containing paper assignment sheets stolen / 100 patients) * More details, including plans of correction submitted by the facilities, are available on the CDPH website.
	Federal Penalty in California
Repeated "curiosity" access	$865,500 + Resolution Agreement + 3 year monitored Corrective Action Plan
	More than fifty CA "covered entities" have reported breaches affecting >500 patients

For more Information Privacy and Security resources go to - **http://compliance-toolbox.wikispaces.com**

MKnutsonLaw.com (858) 705-6633