Effective Immediately: California's New Health Facility Breach Reporting Regulations

Insights 07.09.21

PROFESSIONAL

STEPHEN K. PHILLIPS
Partner
San Francisco

PAUL T. SMITH
Of Counsel
San Francisco

ANDREA FREY
Partner
San Francisco
San Diego

The California Department of Public Health issued long-delayed regulations implementing the health facility medical information breach reporting regulations on July 1. The new regulations, which can be found under Title 22 California Code of Regulations sections 79900 – 79905 (and also available here), take effect immediately. Health facilities subject to the Department's breach reporting requirements should review and update their policies and procedures to accommodate the new rules.

The regulations implement Health and Safety Code section 1280.15, which requires a clinic, health facility, home health agency, or hospice licensed by the Department to prevent any unlawful or unauthorized access to, or use or disclosure of, a patient's medical information, and to report any unauthorized access, use or disclosure to the Department no later than 15 business days after it has been detected by the licensee. Like the HIPAA breach reporting regulations, the new regulations allow a health facility to avoid reporting if it determines, after a documented risk analysis, that there is a low probability that medical information has been compromised. The facility must also notify the patient of the breach within the same period, if notification to the Department is required. Failure to make a timely report to the affected patient or the Department carries a penalty of $100 per day. The regulations detail how the Department may penalize facilities for a breach, including factors by which the Department may increase or decrease penalties.

New Exceptions to the Notice Requirement. The statute already provides that internal paper records, electronic mail, or faxes inadvertently misdirected within the same facility or health care system within the course of coordinating care or delivering services does not constitute unauthorized access to, or use or disclosure of, a patient's medical information. However, there is no exception in the statute itself for misdirected communications outside the health care system – for example, a fax directed to the wrong physician, or a claim sent to the wrong health plan – or for other breaches that pose no risk to the patient. The new regulations retain the exception for inadvertent disclosures within the same facility or health care system, and create additional exceptions for:

i. Inadvertently misdirected communications sent to a HIPAA-covered entity within the course of coordinating care or delivering services.

ii. A disclosure of medical information in which a health care facility or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain the medical

information.

iii. Any access to, use, or disclosure of medical information permitted or required by state or federal law.

iv. Encrypted electronic data containing a patient's medical information, provided the encrypted data has not been unlawfully accessed, used or disclosed.

v. A disclosure for which a health care facility or business associate, as applicable, determines that there is a low probability that medical information has been compromised based on a risk assessment of at least the following factors:

– The nature and extent of the medical information involved, including the types of identifiers and the likelihood of re-identification;

– The unauthorized person who used the medical information or to whom the disclosure was made;

– Whether the medical information was actually acquired or viewed; and

– The extent to which the risk of access to the medical information has been mitigated.

These exceptions parallel those in the HIPAA breach reporting regulations (beginning at 45 CFR § 164.402). If anything, they are a little broader, because HIPAA does not contain an express exception for inadvertently misdirected communications sent to a HIPAA-covered entity within the course of coordinating care or delivering services – although a HIPAA risk analysis of a miscommunication of this kind might well result in a conclusion that the incident need not be reported because the probability that protected health information has been compromised was low.

The exception relating to the risk assessment is taken almost verbatim from the HIPAA rule, so a risk assessment should result in the same conclusion for purposes of both rules. The new regulation requires a facility that determines after a risk assessment that an incident does not constitute a reportable breach to maintain a centralized record of each such incident, along with all materials the health care facility relied upon in performing the risk assessment. The facility must maintain these records for a period of at least six years from the time of the incident, and make them available for inspection by the Department at all times. (This is consistent with the HIPAA rule, which requires covered entities to maintain documentation of risk assessments for six years.)

Reporting Requirements. Although the overall thrust of the regulations has been to harmonize the breach notification obligations of facilities with HIPAA, the reporting requirements of the new regulations are an exception. The regulations under Section 79901(f) define "detect" to mean:

"[T]he discovery of a breach, or the reasonable belief that a breach has occurred by a health care facility or business associate. A breach shall be treated as detected as of the first business day on which such breach is known to the health care facility or business associate, or by exercising reasonable diligence would have been known to the health care facility or business associate. A health care facility or business associate shall be deemed to have knowledge of a breach if such breach is known or by exercising reasonable diligence would have been known, to any person other than the person committing the breach, who is a workforce member or agent of the health care facility or a business associate."

The regulations include business associates in the definition of "health care facility." Read together, these provisions arguably now require a health care facility to report a breach by one of its business associates within 15 business days of detection *by the business associate*, regardless of the facility's actual knowledge of the breach, and regardless of whether the business associate notifies the facility in a timely manner. If this is the intent of the regulation, it is inconsistent with the HIPAA data breach reporting rule (which does not generally impute awareness of a breach on the part of a business associate to the covered entity), and it arguably exceeds the Department's statutory authority under Health and Safety Code section 1280.15, which requires reporting within 15 business days "after the unlawful or unauthorized access, use, or disclosure has been detected *by the clinic, health facility, home health agency, or hospice*." Nothing in the statutory language suggests that detection by a facility's vendor is imputed to the facility absent actual knowledge by the facility. Obviously, a requirement to

report a breach of which a facility is not aware and which it has no means of discovering would be problematic.

Section 79902(b) permits a health facility to discharge its patient reporting obligations by having its business associate provide the patient notices (which HIPAA also allows). Notice to the Department, however, must be made by the facility and not its business associate.

Health and Safety Code section 1280.15 does not specify the form or content of the required notification. The regulations provide this detail. Specifically, notice to the patient under Section 79902(b) must now have the same elements as patient notice under 45 CFR Section 164.404 of the HIPAA Breach Notification Rule:

i. A brief description of what happened, including the facility's name, date of breach and date of discovery, [1] if known;

ii. A description of the types of medical information involved;

iii. Steps patients should take to protect themselves;

iv. A brief description of the facility's mitigation efforts;

v. Contact procedures for questions and additional information; and

vi. The foregoing all in plain English.

The HIPAA Breach Notification Rule requires notice to HHS with the same detail at year end for breaches affecting fewer than 500 patient residents of a state and within 60 days of calendar year-end for other breaches. Section 79902(a) of the new regulations, however, requires notice within 15 business days to the Department in all cases. In addition to the information contained in the patient notices, the notice to the Department must include:

i. The names of *all* affected patients;

ii. The 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;

iii. The dates of patient notice;

iv. The contact information of a health care facility representative who the Department can contact for additional information;

v. 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

vi. Any audit reports, written statements, or other documents that the health care facility relied upon in determining that a breach occurred.

The Departmental reporting requirements that are additional to those under HIPAA promise to make any breach investigation and reporting more challenging for providers and may invite stricter Department scrutiny of provider breach investigations. Providers will also now need to provide a much more detailed roadmap of their breach investigations to the Department than exists under Section 1280.15 and HIPAA, and will need to record and compile individual patient breach histories so that all breaches affecting a patient within six years can be reported.

Administrative Penalties. Finally, the regulations deal with the administrative penalties the Department may impose if it determines that a facility has committed a breach of a patient's medical information in violation of Health and Safety code section 1280.15.

By law, the Department is authorized to assess an administrative penalty on a health care facility for a violation of up to $25,000 per patient whose medical information was unlawfully accessed, used, or disclosed, and up to $17,500 per

subsequent occurrence, even if there is no delay in reporting. In addition the Department can assess a penalty of $100 for each day that the facility fails to report the breach to the Department or an affected patient, though the total penalty asserted against a facility may not exceed $250,000. Section 1280.15(a) also requires 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 establish a *base penalty* amount at $15,000 for any initial violation, and provide that for any subsequent occurrence, the Department may assess "an amount equal to 70% of the initial violation amount," subject to the penalty adjustment factors under Section 79904. (Section 79903.) The regulations under Section 79904(a) allow the base penalty to be increased or decreased by up to $10,000 based on the following:

i. The health care facility's history of compliance with Health and Safety Code section 1280.15 and other related state and federal law for the past three calendar years;

ii. The extent to which the health care facility detected violations and took preventative action to immediately correct and prevent past violations from recurring;

iii. Factors outside the control of the health care facility as defined by section 79901(i). There is no penalty if the health care facility developed and maintained disaster and emergency policies and procedures that were appropriately implemented during a disaster or emergency, if factors outside the control of the health care facility as referenced in 79901(i) were the sole cause of a breach; or

iv. Any other factors applicable to the specific circumstances surrounding the breach, as identified by the Department.

The Department may also reduce a final penalty amount if it determines that "the administrative penalty is unduly burdensome or excessive," though how it makes this determination remains unspecified. Section 79904(b).

The Health and Safety Code does not require health facilities to prevent *all* unlawful or unauthorized access to patients' medical records. It instead requires health facilities to implement *reasonable safeguards* to prevent unlawful and unauthorized access – in effect, creating a negligence standard, rather than one of strict liability. Despite significant pushback from key stakeholders, the regulations do not make negligence a condition for the imposition of penalties. Insofar as the Department might seek to impose penalties under a standard of strict liability, it would arguably be exceeding its statutory authority.

Small and Rural Hospitals. Under Section 79905, the Department may agree to a penalty payment plan or penalty reduction for a small and rural hospital. The hospital must submit its written request for penalty modification to the Department within 10 calendar days after the issuance of an administrative penalty. The request must describe 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. The regulation allows the Department to adjust the penalties for primary care clinics in order to protect access to quality care in those facilities.

Skilled Nursing Facilities. The regulations echo the statute by providing that the Department may issue the higher of a penalty under the health facility medical information breach law, or under the provisions of the Health and Safety Code governing quality of long-term health facilities (starting at Health and Safety Code Section 1417), but not both.

[1] Although the regulations use the term "detect" where the HIPAA Breach Notification Rule uses the term "discovery," the regulations, either incidentally or purposefully, use the term discovery (without definition) here, instead of detection.

***

Hooper, Lundy & Bookman provides a range of legal services relating to health information privacy, security and technology, including assisting clients in responding to data breaches. For more information, please contact: Paul Smith, Steve Phillips or Andrea Frey in San Francisco, Amy Joseph in Boston, Alicia Macklin in Los Angeles, Bob Roth in Washington D.C., or your regular HLB contact.

RELATED CAPABILITIES

Digital Health and Other Health Technologies

Health Information Privacy and Security