PUBLICATION

What You Should Know About California's New Health Facility Breach Reporting Regulations

July 12, 2021

On July 1, 2021, the California Department of Public Health (the Department) issued regulations governing health facility medical information breach requirements. Specifically, the new regulations specify the reporting requirements health care facilities must follow for medical information breaches and further clarify how administrative penalties for violations of medical information breaches will be assessed. The regulations implement California's 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 – as well as to the affected patient(s) – no later than 15 business days after the breach has been detected by the facility (unless a documented exception to this time delay is permitted by law). The new regulations are effective as of July 1, 2021.

Breach Exceptions

Aside from adhering to proper notification and reporting requirements, understanding what does and does not constitute a breach of medical information is paramount in complying with the new regulations. A breach is defined as "each individual instance of unlawful or unauthorized access to, use, or disclosure of a specific patient's medical information." There are several noted exceptions which should be helpful to facilities:

- any internal paper record, electronic mail or facsimile transmission outside the same health care facility or health care system sent to a HIPAA-covered entity that has been inadvertently misdirected within the course of coordinating care or delivering services;
- 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;
- any access to, use, or disclosure of medical information permitted or required by state or federal law;
- any lost or stolen encrypted electronic data containing a patient's medical information that is in any way created, kept, or maintained by a health care facility where the encrypted electronic data has not been accessed, used, or disclosed in an unauthorized way;
- encrypted electronic data containing a patient's medical information, provided the encrypted data has not been unlawfully accessed, used, or disclosed; and
- disclosure for which a health care facility or business associate, as applicable, determines there is a low probability medical information has been compromised based on a risk assessment of at least the following factors:

    - nature and extent of medical information involved, including types of identifiers and likelihood of reidentification;
    - the unauthorized person who used the medical information or to whom disclosure was made;
    - whether medical information was actually acquired or viewed; and
    - extent to which risk of access to medical information has been mitigated.

In the event a health care facility has performed a risk assessment in accordance with the above-listed factors and has determined that an incident does not constitute a breach, the regulations require that facility to maintain a centralized record of each non-breach incident, along with all materials relied upon in performing the risk assessment, and to make those records available for inspection by the Department at all times. These records must be kept for at least six years from the time of incident. These exceptions largely parallel the breach exceptions set forth in the HIPAA regulations (45 CFR §164.402), with the addition of specifying inadvertent misdirection of communications sent outside the same health care facility or health care system to a HIPAA-covered entity within the course of coordinating care or delivering services.

Notice Requirements

The health care facility must report to the Department a breach of a patient's medical information, or a breach reasonably believed to have occurred, no later than 15 business days after the breach has been detected. The report, must be in writing, signed by a representative of the health care facility, and submitted in accordance with the regulation, must contain the following elements:

- name and address of the health care facility where the breach occurred;
- date and time each breach occurred;
- date and time each breach was detected;
- name of patient(s) affected;
- description of medical information that was breached, including the nature and extent of the medical information involved, including types of individually identifiable information and likelihood of reidentification;
- description of events surrounding the breach;
- name(s) and contact information of the individual(s) who performed the breach, any witness(es) to the breach, and any unauthorized person(s) who used the medical information or to whom the disclosure was made, to the extent known;
- date patient or patient's representative was notified, was attempted to be notified, or will be notified of breach;
- contact information of a health care facility representative whom the Department may contact for additional information;
- description of any corrective or mitigating action taken by the health care facility;
- any other instances of a reported event that includes a breach of that patient's medical information by the health care facility in the previous six years;
- a copy of the notification sent to the patient or patient's representative and any additional information provided;
- any audit reports, witness statements, or other documents that the health care facility relied upon in determining that a breach occurred.

With regard to the patient notification, the regulation requires that it be made in writing no later than 15 business days after the breach has been detected by the health care facility. The patient notification must contain the following elements (which must be stated in plain English):

- brief description of what happened, including the health care facility name and address, date of the breach and date of discovery of the breach, if known;
- description of the types 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 health care facility involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and
- contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, internet website address, or postal address.

The health care facility has a continuing obligation beyond the statutory 15 days to supply the Department, as well as the patient, with any additional related information as it becomes available. If a health care facility fails to report in accordance with the above requirements, or is unreasonably delayed, the Department may assess a penalty in the amount of $100 for each day that the breach is not reported to the Department, with total combined penalties not to exceed $250,000 per reported event. In assessing whether delay is unreasonable, the Department will consider factors including:

- size of the affected population;
- lack of sufficient information in the reporting of an incident to make a determination of compliance;
- time passed between the time of an incident and its discovery;
- whether the cause of an incident was a business associate or workforce member; and
- availability of staff to respond to an incident.

Reporting Requirements

Notice requirements are triggered by "detection" of the breach. The regulations define "detect" as:

[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. (Emphasis supplied).

Health care facilities should be aware the regulation suggests a health care facility is required to report a breach by one of its business associates within 15 business days of detection by the business associate, even if the facility has no knowledge of same and whether or not the business associate notifies the facility of the breach in enough time to comply with the statutory time delay. While this is similar to the interpretation of the HIPAA regulations with respect to the "discovery" of a breach, there have been concerns that the regulations exceed the authority set forth in Health and Safety Code Section 1280.15, which does not include "business associates" in the list of entities associated with the detection of a breach that then triggers the statutory time delays. While this discrepancy will likely create interpretation and enforcement complications during this initial implementation period, health care facilities must be cognizant of the seeming imputation of knowledge of the breach and take reasonable measures to mitigate against running afoul of the notice and reporting requirements set forth above.

Administrative Penalties

The regulations allow the Department to impose administrative penalties if it determines that a health care facility has experienced a breach. When the Department has determined that an administrative penalty for a breach of a patient's medical information is warranted, the base penalty amount is $15,000 for each violation, which can be adjusted after consideration of certain factors.

- The health care facility's history of compliance with Section 1280.15 and other related state and federal law for the past three calendar years;
- 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);
- 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;
- any other factors applicable to the specific circumstances surrounding the breach, as identified by the Department.

The maximum total combined amount that can be assessed is $250,000 per reported event. The Department may reduce a final penalty amount if the Department determines that the administrative penalty is unduly burdensome or excessive. Notably, there are no indicators as to what would fall within this residual reduction option; however, the Department is authorized to have "full discretion" to consider "all factors" in assessing an administrative penalty. The regulation specifically allows for reductions for small and rural hospitals, primary care clinics, and skilled nursing facilities. It is important to note health care providers are required to "establish and implement appropriate administrative, technical, and physical safeguards to protect the privacy of a patient's medical information" and "reasonably safeguard confidential medical information from any unauthorized access or unlawful access, use, or disclosure." As such, it is reasonable for health care facilities to expect that the safeguards put in place to protect the privacy and security of a patient's medical information will factor into the Department's assessment.

As breach notification and related health information privacy and security laws and regulations affecting the U.S. health care industry evolve, Baker Donelson stands ready to support you. If you have any questions about this or any other aspect of your health information, privacy, and security practices, please contact any member of Baker Donelson's Health Information Technology or Data Protection, Privacy, and Cybersecurity Practice Teams.