Updates
September 09, 2021

California Issues New Regulations on Notification Obligations for Medical Information Breaches

Certain California-licensed healthcare facilities are now subject to additional breach reporting obligations pursuant to regulations (Regulations)[1] issued by the California Department of Public Health (Department) on July 1, 2021. These Regulations modify California Health and Safety Code section 1280.15 (section 1280.15) and impose requirements on healthcare facilities (as defined below) regarding what information must be submitted in a breach report, explain exceptions to the requirements, and further align section 1280.15 with the breach notification obligations under the Health Insurance Portability and Accountability Act of 1996, as amended (HIPAA). The Regulations also clarify potential penalties for violations of the new provisions.

Background

Section 1280.15, which has been in effect for years, currently requires a clinic, health facility, home health agency, or hospice licensed by the Department (collectively, a "healthcare facility") to "prevent unlawful or unauthorized access to, and use or disclosure of" a patient's medical information, and to report any unauthorized access, use, or disclosure of a patient's medical information to the Department no later than 15 business days after it has been detected by the licensee. However, section 1280.15 lacks detail on the reporting requirements for such breaches and a framework by which administrative penalties can be assessed in a fair and consistent manner.

The Regulations are intended to provide additional details on reporting requirements, increase vigilance by healthcare facilities to protect patient medical information, and improve patient experiences for the people of California. The Regulations also more closely align breach reporting obligations under section 1280.15 with federal reporting requirements under HIPAA.

Details

Additional Requirements on the Type of Information Submitted

Under the Regulations, healthcare facilities are still required to notify patients no later than 15 business days after the "unlawful or unauthorized access, use or disclosure has been detected by the clinic health facility," as required under the original Section 1280.15. However, the Regulations now specify the form and content of such notifications, which was missing from the text of the statute itself.

Exceptions to the Breach Notification Reporting Requirement

Section 1280.15 contains a single exception to the breach notification reporting requirement (for internal paper records, electronic mail, or facsimile transmissions inadvertently misdirected within the same facility or healthcare system within the course of coordinating care or delivering services). The Regulations expand the exceptions by carving out various types of access, use, and disclosure from the definition of a "breach," including:

- Any paper record, electronic mail, or facsimile sent to a HIPAA-covered entity that is inadvertently misdirected within the course of coordinating care or delivering services;
- A disclosure where the healthcare facility has a good-faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such medical information;
- Access, use, or disclosure of a patient's medical information permitted or required by state or federal law;
- Lost or stolen encrypted electronic data where the encrypted electronic data has not been accessed, used, or disclosed in an unlawful or unauthorized manner; and
- A disclosure where the healthcare facility determines there is only a low probability of compromise in accordance with HIPAA's four-factor analysis, taking into account the following facts at a minimum: (1) the nature and extent of the medical information involved; (2) the unauthorized user or recipient of the medical information; (3) whether the medical information involved was actually acquired or viewed; and (4) the extent to which the risk of access to the medical information has been mitigated.

Penalties

Under the Regulations, the base penalty amount is $15,000 for each violation. The maximum total per reported event is $250,000. The base penalty is subject to certain adjustments of up to $10,000, that include the healthcare facility's history of compliance with section 1280.15 and other related state and federal laws for the preceding three calendar years, the extent to which the healthcare facility detected violations and took preventative action, factors outside the control of the healthcare facility, and any other applicable factors as determined by the Department. Small and rural hospitals, primary care clinics, and skilled nursing facilities are also subject to reduced penalties for breaches under the Regulations under specified conditions. The Department also has discretion to reduce the final penalty if it is "unduly burdensome or excessive," which is not defined under the Regulations.

Relationship to Other Breach Notification Laws

Relationship to HIPAA

Coexisting with the Regulations are federal laws relating to healthcare facilities, including HIPAA. As a federal law, HIPAA is meant to be a "floor" for patient protection standards, but states may enact their own laws and regulations relating to the privacy and security of protected health information to provide more stringent requirements. The Regulations align California's data breach notification laws relating to healthcare facilities with HIPAA and, in some cases, apply an even broader standard. This section discusses some of the similarities and differences between the Regulations and HIPAA.

Under the Regulations, a business associate's (a vendor, contractor, or other service provider of a healthcare facility) liability for breach notification is different than the standard applied under HIPAA. Under HIPAA, business associates are directly liable for compliance with certain requirements of the HIPAA rules, whereas under the Regulations, business associates are not directly liable for reporting breaches to healthcare facilities or to the Department. In the legislative history of the Regulations, the Department indicates that healthcare facilities are responsible for the actions of their business associates, and any breach detected by a business associate is imputed to the healthcare facility. Section 79902(a) also specifically excludes reporting obligations on the part of the business associate ("A health care facility, *excluding* a business associate, shall report […]" (emphasis added)).

The Regulations and HIPAA's breach notification requirements now are more closely, but not identically, aligned. For example, the Regulations allow for an exception to the breach notification requirements where a

healthcare facility has determined that there is only a low probability of compromise in accordance with the HIPAA four-factor analysis described above. The Regulations allow for another exception, however, that is not currently permitted by HIPAA with respect to inadvertently misdirected communications to a HIPAA-covered entity within the course of coordinating care or delivering services. Arguably this exception would render the Regulations, in this respect, to be broader than federal law.

While the Regulations may be similar to HIPAA with respect to the form and content of breach notifications, the Regulations require notice to be given to the Department within 15 business days of detection of a defined breach, whereas under HIPAA, covered entities or business associates are only required to notify regulators, within 60 days, for breaches affecting more than 500 patients.

Relationship to Other Breach Notification Laws, Including California's Breach Notification Law (Cal. Civ. Code § 1798.29; 1798.82 et seq.)

While a detailed comparison between the breach notification obligations under the Regulations and other breach notifications laws is outside the scope of this update, healthcare facilities should be aware that a breach of a patient's medical information may be subject to several potentially overlapping breach notification laws at both the state and federal level. For example, California's breach notification law applies to "security breaches" of "medical information" which may not have the same meaning as the definitions of "Breach" and "Medical Information" under the Regulations.

Takeaways

Healthcare facilities subject to the Regulations should prepare for more active oversight and investigations by the Department. While the Regulations should reduce the overall number of data breach reports submitted due to the greater number of notification exceptions and the heightened standards for notification submission, the Department is likely to focus more closely on the reports submitted. Further, business associates should expect healthcare facilities to request amendments to existing contracts to account for updates to the required content for breach notifications. Healthcare facilities are also encouraged to review and revise their compliance policies and procedures to fortify their protection of patient medical information in order to minimize their chance of investigation, potentially reduce possible penalties in the event of a breach, and to properly respond to any regulatory inquiries.

Endnotes

[1] Title 22 California Code of Regulations, sections 79900 - 79905

Authors

April A. Goff

Partner
AGoff@perkinscoie.com 214.259.4954

Explore more in

Privacy & Security Life Sciences & Healthcare

Related insights

Update

Employers and Immigration Under Trump: What You Need To Know

Update

'Tis the Season… for Cybercriminals: A Holiday Reminder for Retailers