Blogs
September 10, 2021

On August 24, 2021, the office of the California Attorney General (AG) Rob Bonta issued a press release notifying the public of healthcare data privacy guidance that AG Bonta sent to stakeholder organizations, including the California Hospital Association, the California Medical Association, and the California Dental Association, that day. According to the press release, the guidance was sent to stakeholders as a bulletin that, in part, reminded the entities of their obligation to notify the California Department of Justice (DOJ) when the health data of more than 500 California residents has been breached. The press release quotes Attorney General Bonta, stating, "California law mandates that data breaches impacting more than 500 of our residents be reported to the California Department of Justice. In addition, I implore all entities that house confidential health related information to be vigilant and take steps now to protect patient data, before a potential cyberattack." California

law requires entities that have suffered a data breach, including a health data breach, affecting more than 500 California residents to submit a breach report to the Office of the Attorney General.[1] When healthcare providers notify the AG of these breaches, the DOJ advises the public of the breach through the AG's website.[2] Last year, the U.S. Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, and the U.S. Department of Health and Human Services released a joint report that stated the agencies had "credible information of an increased and imminent cybercrime threat to U.S. hospitals and healthcare providers." The AG's press release cited this report and emphasized the importance of data security for California residents, stating, "[w]hen the breaches of data involve Social Security numbers, health records, or other sensitive information, they threaten the privacy, security, and economic wellbeing of impacted Californians. They also disrupt the ability of providers to provide care and erode patient trust." The press release also highlights certain steps healthcare entities should take "at a minimum" to protect patient data from ransomware attacks:

- Keep all operating systems and software housing health data current with the latest security patches;
- Install and maintain virus protection software;
- Provide regular data security training for staff members that includes education on not clicking on suspicious web links and guarding against phishing emails;
- Restrict users from downloading, installing, and running unapproved software; and
- Maintain and regularly test a data backup and recovery plan for all critical information to limit the impact of data or system loss in the event of a data security incident.

A copy of the bulletin is available here. [1] CA Civil Code section 1798.82. [2] https://oag.ca.gov/privacy/databreach/list

Authors

Elizabeth Smith

Associate
ElizabethSmith@perkinscoie.com 737.256.6124

Explore more in

Privacy & Security
Blog series

Perkins on Privacy

Perkins on Privacy keeps you informed about the latest developments in privacy and data security law. Our insights are provided by Perkins Coie's Privacy & Security practice, recognized by Chambers as a leading firm in the field. Subscribe ?

View the blog