Published on *The National Law Review* https://natlawreview.com

California Attorney General Issues Guidance on Health Data Privacy Issues

Article By:

Elliot Golding

Kristin L. Bryan

Amber Mulcare

Citing "multiple unreported ramsomware attacks" targeting the healthcare sector, last month the California Attorney General (CA AG) issued guidance reminding healthcare entities of their requirements under state and federal health data privacy laws to implement adequate security measures and comply with breach notification requirements. Although the document does not provide any "new" guidance, it signals that the California AG is prioritizing breaches in the health care sector and serves as a reminder that entities subject to HIPAA are not exempt from California's more stringent breach notification requirements.

In particular, the AG's bulletin reminds Covered Entities under HIPAA that California state law imposes additional requirements, such as notice to the Attorney General when a breach impacts more than 500 people. Although the generally applicable California data breach law exempts entities subject to HIPAA from California's requirements regarding the ***content*** of breach notification letters, that law does not exempt Covered Entities or Business Associates from the AG notice provisions. California also has other breach reporting requirements that are stricter than HIPAA, such as the California Department of Public Health's 15-day deadline for "healthcare facilities" to report "medical information breaches" experienced by the facility or its business associates.

The AG's bulletin recommends entities implement the following minimum preventive measures:

- 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.

- Other security safeguards required under other laws (such as HIPAA) and recommended in government publications (such as data security best practices available in the CISA Cyber Resource Hub).

National Law Review, Volume XI, Number 292