The California AG recently reminded companies in the healthcare industry of potential data breach notification obligations beyond HIPAA. As ransomware attacks continue to rise, particularly in healthcare, companies should keep in mind the patchwork of state and federal health data privacy laws that may apply.

Companies may have obligations under both federal and state laws to protect information. In the healthcare space, this means that entities subject to HIPAA either as a covered entity or business associate may also be subject to other more stringent state medical information laws or other general data security laws – in addition to the HIPAA Security Rule. Some (but not all) of these state general data security laws include certain exemptions for HIPAA-regulated entities, or for information subject to or protected under HIPAA. However, these laws may still apply to health or medical information that is not subject to HIPAA. Similar to OCR’s recent reminder about ransomware, the California AG similarly called for
entities collecting and storing health-related information to take preventative measures against these attacks. This includes, at minimum:

- keeping systems and software up-to-date,
- installing and maintaining virus protection
- providing regular data security training, including education about phishing
- restrict users from downloading and installing unapproved software; and
- maintain and test regularly data backup and recovery plan.

In addition to obligations to protect information, federal and state laws have specific breach reporting requirements. While some requirements may overlap, the state obligations may trigger notice to additional regulatory authorities. For example, in California, entities subject to HIPAA must also report security breaches of more than 500 California residents to the California’s AG’s office.

**Putting it into Practice:** The California AG’s bulletin provides insight into what the agency might expect companies to be doing to prevent cyberattacks. It also serves as a reminder of potential state breach reporting obligations for HIPAA-regulated entities. States other than California have similar requirements. It also suggests that AG will likely be keeping a close watch on breaches reported under HIPAA (either through media notices or the OCR breach portal) that go unreported to the office. The AG also signaled in the bulletin that this area will likely be an increasing enforcement priority by noting its authority to bring civil actions for violations of HIPAA.

Copyright © 2021, Sheppard Mullin Richter & Hampton LLP.

National Law Review, Volume XI, Number 239