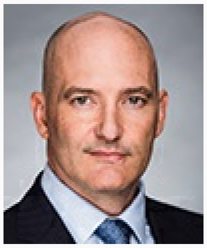
COSMOS
Navigate the Compliance Universe

Compliance Today - May 2022
A proactive approach to cybersecurity: Adopting best practices is critical

By Jon Moore, MS, JD, HCISPP

Jon Moore (jon.moore@clearwatercompliance.com) is Senior Vice President and Chief Risk Officer, Clearwater, Nashville, TN.



Jon Moore

For far too long, many healthcare organizations viewed cybersecurity as a problem exclusively for their IT departments. Leaders at these organizations failed to appreciate how a single cyber incident could have lasting—and potentially devastating—consequences for the organization as a whole, its patients, and partners.

Unfortunately, many healthcare executives and their boards are now learning the hard way that data privacy and security are no longer just technical issues for the IT team that are hidden behind complicated jargon.

In 2021, the Office for Civil Rights (OCR) investigated a record number of breaches. Its breach portal shows 714 reported breaches of protected health information affecting records of 500 or more individuals for that year.[1] This represents a 7.7% increase over the previous year. Ten of those incidents exposed a million or more records each. As of March 10, there have been an additional 102 reported breaches of 500 or more records and another million-plus record breach.

These breaches are costing healthcare a record-breaking amount of money. IBM's*Cost of a Breach Report 2021*[2] cites healthcare again at the top of the list—for 11th consecutive year—as the industry with the highest average cost of a breach. In 2021 that average cost reached $9.23 million, compared to $7.13 million in 2020. With the number of successful breaches last year—reflective of what we've seen since the onset of the pandemic—it wouldn't be surprising, when the numbers are tallied for the 2022 report, to see it continuing to rise.

That's why it's becoming ever more apparent that healthcare organizations can no longer approach cybersecurity reactively and as simply an IT problem.

Today, the most successful healthcare organizations take a more proactive and holistic approach to their cybersecurity and risk management programs. They understand that now is the time to adopt best practices and better prepare themselves for the increasing likelihood of attacks and incidents.

The good news is that there are now many incentives to take action, and with proper guidance and support, your organization can be well on its way to reducing your cyber risks today and in the future.

New incentives, new motivations

While there are many practical reasons to invest time and resources to implement more robust cybersecurity practices, some healthcare organizations might not be aware of a new law that provides even more incentive to do so—HR 7898.[3]

HR 7898 became law last year. It's an amendment to the Health Information Technology for Economic and

Clinical Health (HITECH) Act that encourages healthcare-covered entities and their business associates to adopt recognized cybersecurity practices. How? Because if you experience a breach or other security incident and get on the U.S. Department of Health & Human Services' radar, demonstrating your healthcare organization has recognized cybersecurity practices in place must be taken into consideration when the agency reviews your case.

While it's not a safe harbor and won't protect you from fines, penalties, or other measures, it may affect how long an audit lasts, what its outcome might be, and could potentially influence the amount of fines and other penalties you face.

The law specifies: "*Nothing in this section shall be construed to limit the Secretary's authority to enforce the HIPAA Security rule (part 160 of title 45 Code of Federal Regulations and subparts A and C of part 164 of such title), or to supersede or conflict with an entity or business associate's obligations under the HIPAA Security Rule.*"[4]

But the law does instruct OCR to consider whether, if the healthcare organization has demonstrated that for the preceding 12 months, it has recognized cybersecurity practices in place.[5]

In simplest terms, OCR may still impose fines and penalties. Still, healthcare organizations that have adopted recognized practices may experience far less scrutiny and reduced monetary penalties. As a healthcare covered entity or business associate, the incentive here is if you do face an audit or have a security incident that prompts an investigation, you may experience a range of advantages you'd otherwise miss out on.