Health Information Compliance Alert

HIPAA: OCR Recommends Focus on Cybersecurity in 2022

After 2021 cyberattack spikes, feds urge CEs to better mitigate threats.

Even before the pandemic began, cybersecurity was a thorny subject for the healthcare industry. But, the feds suggest that last year was a particularly challenging year for HIPAA covered entities (CEs) and their business associates (BAs) - and healthcare as a whole needs a reset.

Background: Both big and small providers have suffered at the hands of hackers over the past few years, and it's taken both a professional and financial toll on many CEs and BAs. However, 2021 saw a huge increase in data security incidents in healthcare, with millions of individuals' protected health information (PHI) hijacked. "For healthcare, this year was even more turbulent as cybercriminals took advantage of hospitals and healthcare systems responding to the COVID-19 pandemic," said **Lisa J. Pino,** HHS Office for Civil Rights (OCR) director, in a blog post. "More than one health care provider was forced to cancel surgeries, radiology exams, and other services, because their systems, software, and/or networks had been disabled," she lamented.

Statistics: According to the OCR breach portal, 2021 was a banner year for HIPAA breaches. There were 714 incidents reported to OCR with 500 or more individuals' PHI exposed. In fact, more than 45.7 million individuals were impacted last year, the breach tool shows. Hacking and IT incidents dominated the landscape with the majority of the PHI outages attributed to issues related to network servers, email, desktop computers, and mobile devices.

In December, experts warned healthcare organizations about vulnerability issues related to patching fails for the Java-based software Apache Log4j, which is often used in applications on medical devices. Pino pointed to these "security flaws" as well as other systemic problems to "underscore why it is so important for healthcare to be vigilant in their approach to cybersecurity." She urged CEs and BAs to bolster their "cyber posture in 2022."

Heed This Expert Advice

In an investigative report of 2020 breaches - the most recent year that the feds have compiled data available to study - OCR offered a window into some of the top problems they feel that CEs and BAs should be homing in on, specifically risk analysis and management.

Reminder: Prioritizing the safety of electronic PHI (ePHI) is the central theme of the HIPAA Security Rule, but OCR finds that many CEs don't go beyond a cursory risk analysis of their EHR systems, Pino indicated. An enterprise-wide risk analysis that offers comprehensive protections and includes the organization's scale and scope are what the agency expects.

"The HIPAA Security Rule requires that organizations implement 'reasonable and appropriate' security controls based on their assessment of risk," explains **Adam Kehler,** director of RSP Healthcare Services at Online Business Systems. Additionally, "the sheer volume of data and number of systems in healthcare are increasing, thereby increasing the attack surface," he warns.

The investigations show that healthcare organizations fall short on the HIPAA Security Rule, and that's why this sector is vulnerable to attack and violations crop up more often than in other industries. "These reports highlight the continued

need for regulated entities to improve compliance with the HIPAA Security Rule standards, in particular the implementation specifications of risk analysis and risk management, information system activity review, audit controls, security awareness and training, and authentication," Pino advised.

Consider these OCR-inspired recommendations to jumpstart your 2022 HIPAA Security Rule compliance:

- Ensure you are up to date on patches and legacy system changes.
- Back up your data and store encrypted copies offline.
- Educate your staff on both the HIPAA regulations and common cybersecurity concerns like phishing and ransomware.
- Monitor your systems and keep a log of any unusual cyber activity.
- Conduct "regular scans to identify and address vulnerabilities, especially those on internet-facing devices, to limit the attack surface."

Resource: Find the blog post with links to other cyber hygiene hot topics as well as the 2020 breach reports at www.hhs.gov/blog/2022/02/28/improving-cybersecurity-posture-healthcare-2022.html.