COSMOS
Navigate the Compliance Universe

Report on Patient Privacy Volume 22, Number 11. November 10, 2022 Security Checklist: OCR Advice on Preparing, Responding to Incidents

By Jane Anderson

A "timely response" to a cybersecurity incident is one of the best ways to prevent, mitigate and recover from cyberattacks, according to HHS Office for Civil Rights (OCR). In addition, reporting any breach must occur "without reasonable delay," OCR reminded HIPAA-regulated entities.

In its October 2022 OCR Cybersecurity Newsletter, OCR explained that "security incidents will almost inevitably occur during the lifetime of a regulated entity" and spelled out recommended procedures for HIPAA-covered health care entities to follow.[1] "Having a plan established and documented is essential to being able to detect security incidents quickly in order to respond to and recover from security incidents effectively," OCR said.

Cybersecurity incidents and data breaches have continued to increase across all industries, including health care, OCR said, noting that a 2022 report noticed a 42% increase in cyberattacks for the first half of 2022 compared to 2021 and a 69% increase in cyberattacks targeting the health care sector.

"The number of data breaches occurring in the health care sector also continue to rise," OCR wrote. "Breaches of unsecured protected health information (PHI), including [electronic] ePHI, reported to ...OCR affecting 500 or more individuals increased from 663 in 2020 to 714 in 2021. Seventy-four percent (74%) of the breaches reported to OCR in 2021 involved hacking/IT incidents. In the health care sector, hacking is now the greatest threat to the privacy and security of PHI."

Form an Incident Response Team

In preparing their security incident response process, regulated entities should consider forming an incident response team that is organized and trained to effectively respond to security incidents, OCR said. The agency recommended utilizing the National Institute of Standards and Technology (NIST) guide to handling computer security incidents.[2] That guide covers:

- Selecting a team structure and staffing
- Establishing relationships and lines of communication between the security incident response team and other internal and external groups
- Identifying internal groups that may need to participate in incident handling, such as management, information technology support, legal, public affairs and communications, human resources, business continuity/disaster recovery, physical security and facilities management
- Identifying points of contact at external groups that may be helpful to include in the event of an incident, such as network service providers, software and hardware vendors, local and federal law enforcement, incident handling teams of business partners and customers
- Determining what services the incident response team should provide, such as intrusion detection,

advisory distribution, education and awareness and information sharing

"Once formed, the security incident response team should conduct regular testing of security incident procedures," OCR said. "This could involve conducting tests involving different types of potential security incident scenarios, for example, a malicious insider exfiltrating sensitive information, a cyber-criminal's infiltration and deployment of ransomware, or a distributed denial of service (DDoS) attack that interrupts system operations. Security incident procedures should be updated with lessons learned from testing as well as from actual security incidents to improve the team's response and effectiveness."

OCR added that "having audit logs in place and regularly reviewing such logs are actions that regulated entities are required to take and greatly improve their ability to identify security incidents early." For instance, log files may help identify when and how a cybercriminal entered an information system and what activities occurred, OCR said. "By recording information system events, alerts, user actions, and other activities in appropriate logs and conducting regular reviews of such logs, regulated entities will have mechanisms and procedures in place to record and review information system activity and be able to identify and respond to security incidents quickly."