akerman

Blog Post

OCR Will Focus on You if You Don't Focus on Cybersecurity

December 21, 2023
By Elizabeth F. Hodge

With a couple of "firsts," the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is signaling that it is cracking down on healthcare organizations that fail to identify and address cybersecurity vulnerabilities as required by the Health Insurance Portability and Accountability Act of 1996 (HIPAA Rules). On October 31, 2023, OCR issued its first settlement agreement under the HIPAA Rules related to a ransomware attack (the Ransomware Settlement) and on December 7, 2023, its first settlement under the HIPAA Rules arising from a phishing cyber-attack (the Phishing Settlement). In the press release for its first settlement agreement, OCR made clear that cybersecurity awareness is a top concern for OCR, with hacking accounting for 77 percent of the large breaches reported to OCR in 2023.

The Ransomware Settlement

In October 2023 (also Cybersecurity Awareness Month), OCR entered into the Ransomware Settlement with Doctors' Management Services (DMS), a medical management company that provides a variety of administrative services, such as medical billing and payor credentialing. DMS's network server was infected with ransomware, a software that denies a user access to their data, usually by encrypting the data so that it can only be viewed by the hacker until a ransom is paid.

Related People

Elizabeth F. Hodge

Related Work

Data Privacy and Security
Health Insurers and Managed Care Organizations
Healthcare

Related Offices

Miami
West Palm Beach

Health Law Rx

Akerman Perspectives on the Latest Developments in Healthcare Law

Read blog posts

According to OCR, the initial unauthorized access occurred on April 1, 2017, but DMS did not detect it until December 24, 2018, when ransomware was used to encrypt the practice's files. The electronic protected health information (ePHI) of approximately 206,695 individuals was affected. OCR investigated the matter and determined that, prior to the breach, DMS had failed to:

- Conduct a thorough risk analysis to determine the potential risks and vulnerabilities to ePHI across the organization;
- Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports; and
- Implement reasonable policies and procedures to comply with the standards, implementation specifications, and other requirements of the Security Rule.

As a result of OCR's investigation, DMS agreed to pay $100,000 to OCR and enter into a resolution agreement and corrective action plan, which will be monitored by OCR for three years. The key terms of the corrective action plan require DMS to:

- Review and update its risk analysis to identify potential risks and vulnerabilities to DMS's data to protect the confidentiality, integrity, and availability of ePHI. In addition, DMS must update its enterprise-wide risk management plan to address and mitigate any security risks and vulnerabilities found in the updated risk analysis.
- Review and revise, if necessary, its written policies and procedures to comply with the Privacy and Security Rules. Specifically, the policies and procedures shall include processes for the regular review of all records of information system activity collected by DMS and processes for evaluating when the collection of new or different records needs to be included in the review.

- Provide training to all staff members who have access to patients' PHI regarding the HIPAA policies and procedures.

The Phishing Settlement

Most recently, OCR entered into the Phishing Settlement with Lafourche Medical Group (LMG), a medical group specializing in emergency medicine, occupational medicine, and laboratory testing. LMG was the victim of a phishing attack, a type of cybersecurity attack wherein individuals are tricked to disclose sensitive information via electronic communication. Through the phishing attack, an unauthorized individual obtained access to the email account of one of LMG's owners. Because LMG was unable to determine which specific patients were affected, it notified all of its patients — approximately 34,862 individuals. OCR investigated the matter and determined that, prior to the breach, LMG had failed to:

- Conduct a Security Rule risk analysis to identify potential threats or vulnerabilities to ePHI across the organization as required by HIPAA; and
- Implement policies and procedures to regularly review information system activity to safeguard PHI against cyber-attacks.

As a result of OCR's investigation, LMG agreed to pay $480,000 to OCR and enter into a resolution agreement and corrective action plan, which will be monitored by OCR for two years. The key terms of the corrective action plan require LMG to:

- Establish and implement a risk management plan based on its December 2022 security risk assessment to reduce security risks and vulnerabilities to ePHI to keep patients' PHI secure, and annually conduct risk analyses of potential risks and vulnerabilities to its ePHI.
- Develop, maintain, and revise written policies and procedures as necessary to comply with the HIPAA Rules, including development of policies

and procedures for the regular review of all records of information system activity collected by LMG and processes for evaluating when the collection of new or different records needs to be included in the review. The policies and procedures should also identify which systems are being included in the review and a new and very specific requirement of a 14-day frequency to conduct such reviews.

- Provide training to all staff members who have access to patients' PHI regarding the HIPAA policies and procedures.

OCR Cybersecurity Resources

In recent years, OCR has published a number of resources to assist healthcare organizations in protecting themselves and their patients from cybersecurity incidents. There is an HHS webpage dedicated to providing helpful information to protect against cyberattacks and comply with the HIPAA Rules, including recent newsletters regarding defending against common cyberattacks, HIPAA and cybersecurity authentication, and how sanction policies can support HIPAA compliance.

Earlier this month HHS released a concept paper outlining its cybersecurity strategy for the healthcare sector. HHS's proposals are another signal that the agency intends to be more aggressive regarding cybersecurity compliance and include:

- establishing voluntary cybersecurity performance goals for the healthcare sector;
- providing resources to incentivize and implement the cybersecurity performance goals;
- implementing an HHS-wide strategy to support greater enforcement and accountability;
- a forthcoming proposal by the Centers for Medicare & Medicaid Services (CMS) for new cybersecurity requirements for hospitals through Medicare and Medicaid;

- OCR beginning an update to the HIPAA Security Rule in spring 2024 to include new cybersecurity requirements; and
- HHS working with Congress to increase civil monetary penalties for HIPAA violations and increase resources for HHS to investigate potential HIPAA violations and conduct proactive audits.

Takeaways

In light of the LMG and DMS resolution agreements and the proposals in the HHS concept paper, healthcare organizations should take this opportunity to assess their cybersecurity compliance efforts by doing the following:

- Conduct periodic risk analyses of potential risks and vulnerabilities to the organization's ePHI.
- Develop and implement a risk management plan to minimize the risks to the organization identified by the risk analyses.
- Maintain, review, and revise, if necessary, written policies and procedures to ensure compliance with the HIPAA Rules, particularly the HIPAA Security Rule.
- Train (and re-train) workforce members on the organization's HIPAA policies and procedures.
- Review all vendor and contractor relationships to ensure business associate agreements address breach/security incident obligations.
- Ensure audit controls are in place to record and examine information system activity.
- Utilize multifactor authentication to ensure only authorized users are accessing ePHI.
- Encrypt ePHI at rest and in transit to guard against unauthorized access.
- Incorporate lessons learned from security incidents into the overall security management process.

Given the prevalence of cyberattacks against the healthcare sector and the number of individuals affected by such incidents, covered entities and business associates should expect that OCR will increase its scrutiny of cybersecurity events affecting the healthcare sector and prepare accordingly to protect themselves and their patients. Akerman's Health Law Rx blog will continue to post updates of OCR's enforcement activities related to cybersecurity.
