STRATEGIC MANAGEMENT SERVICES

OCR Reports Increase in Large Settlements of Ransomware Breaches

Richard P. Kusserow | October 2024

Tips and steps to mitigate risks

The Office of Civil Rights (OCR) has reported a growing number of large ransomware breaches. The latest example of these breaches is the recent settlement of Cascade Eye and Skin Centers in the state of Washington for $250,000 to resolve a violation of the Health Insurance Portability and Accountability Act (HIPAA) Security Rule that resulted in a ransomware attack. The HIPAA Security Rule created national standards to protect electronic personal health information (ePHI) created, received, used, or maintained by covered entities. Appropriate administrative, physical, and technical safeguards are mandated to ensure the confidentiality, integrity, and security of ePHI. In the Cascade case, nearly 300,000 files containing ePHI were compromised by a ransomware attack. In their investigation, OCR found multiple violations of the HIPAA Security Rule, including failures to conduct a compliant risk analysis to determine the potential risks and vulnerabilities to ePHI in its systems and insufficient compliance monitoring of its health information systems. Cascade, under the two-year settlement, is required to implement a corrective action plan for protecting and securing the security of PHI, including:

- Conducting a thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Implementing a risk management plan to address and mitigate security risks and vulnerabilities identified in their risk analysis;
- Developing a written process to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports;
- Implementing policies and procedures for responding to an emergency or other occurrence that damages systems that contain ePHI;
- Developing written procedures to assign a unique name and/or number for identifying and tracking user identity in its systems that contain ePHI; and
- Reviewing and revising as necessary written policies and procedures to comply with the HIPAA Privacy and Security Rules.

All covered entities should include this as part of their compliance programs. OCR also calls for all HIPAA Privacy and Security Officers to take the following steps to prevent or mitigate cyber threats:

- Ensure BAAs with vendors and contractors address breach/security incident obligations.
- Integrate risk analysis and risk management into business processes.
- Conduct regular risk assessments when planning new technologies/business operations.
- Ensure audit controls are in place to record and examine information system activity.

- Implement regular reviews of information system activity.
- Utilize multi-factor authentication to ensure only authorized users are accessing ePHI.
- Encrypt ePHI to guard against unauthorized access to ePHI.
- Incorporate lessons learned from incidents into the overall security management process.
- Provide regular ongoing training specific to the organization and job responsibilities.
- Reinforce workforce personal obligations in protecting privacy and security.

You can keep up-to-date with Strategic Management Services by following us on **LinkedIn**.

About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.