Skadden

Cybersecurity and Data Privacy Update

April 3, 2024

If you have any questions regarding the matters discussed in this memorandum, please contact the attorneys on the next page or call your regular Skadden contact.

One Manhattan West
New York, NY 10001
212.735.3000

1440 New York Avenue, N.W.
Washington, D.C. 20005
202.371.7000

155 N. Wacker Drive
Chicago, IL 60606
312.407.0700

HHS Office for Civil Rights Reaches Second Health Care Ransomware Settlement

The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) recently announced its second settlement in four months growing out of a ransomware attack on a health care business. Maryland-based Green Ridge Behavioral Health agreed to pay $40,000 and implement a corrective action plan after an investigation found potential violations of the Health Insurance Portability and Accountability Act (HIPAA) privacy and security rules.

The settlement comes as ransomware has emerged as a critical threat to health care organizations, and regulators have prioritized enforcing cybersecurity standards, underscored by the announcement in October 2023 of a $100,000 settlement involving an attack on a medical billing company and OCR's recent investigation into the cyberattack on Change Healthcare, a clearing house for medical claims.

Background

Green Ridge is a behavioral health clinic that provides psychiatric evaluations, medication management and psychotherapy. In February 2019, Green Ridge notified OCR that its network server had been infected with ransomware resulting in the encryption of patient health records and company files. OCR launched an investigation into Green Ridge's HIPAA compliance and found evidence that Green Ridge failed to conduct a proper risk assessment, implement appropriate security measures or sufficiently monitor its IT systems to protect against a cyberattack.

In addition to the fine and implementation of the corrective plan, Green Ridge agreed that the plan would be monitored by OCR for three years. Corrective steps identified in the settlement announcement include:

- "Conducting a comprehensive and thorough analysis of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information;
- Designing a Risk Management Plan to address and mitigate security risks and vulnerabilities found in the Risk Analysis;
- Reviewing, and as necessary, developing, or revising its written policies and procedures to comply with the HIPAA Rules;
- Providing workforce training on HIPAA policies and procedures;
- Conducting an audit of all third-party arrangements to ensure appropriate business associate agreements are in place, where applicable; and
- Reporting to OCR when workforce members fail to comply with HIPAA."

HHS Office for Civil Rights Reaches Second Health Care Ransomware Settlement

The settlement highlights the growing focus on cybersecurity and HIPAA compliance in the wake of ransomware attacks. As explained by OCR Director Melanie Fontes Rainer in the press release about the Green Ridge settlement:

> Ransomware is growing to be one of the most common cyber-attacks and leaves patients extremely vulnerable. These attacks cause distress for patients who will not have access to their medical records, therefore they may not be able to make the most accurate decisions concerning their health and well-being. Health care providers need to understand the seriousness of these attacks and must have practices in place to ensure patients' protected health information is not subjected to cyber-attacks such as ransomware.

The White House has also acknowledged the severity of this threat and, in coordination with HHS, is exploring potential legislation and mandatory cybersecurity standards for health care providers.

In December 2023, HHS released a concept paper detailing the department's ongoing and planned steps to improve cyber resiliency in the health care sector. The paper outlines plans to publish voluntary security goals for providers, develop financial supports and incentives for hospitals to improve cybersecurity, and increase accountability through new enforceable cybersecurity standards. In the announcement of the paper, Deputy National Security Advisor for Cyber and Emerging Technologies Anne Neuberger said the administration "is establishing strong cybersecurity standards for health care organizations and enhancing resources to improve cyber resiliency across the health sector, including working with Congress to provide financial support for hospitals."

In light of this evolving landscape, health care providers must be vigilant in fortifying their cybersecurity programs. Staying informed about the latest threats, implementing robust data security protocols and developing a comprehensive incident response plan are all crucial steps. By taking proactive measures, they can protect their patients and potentially avoid fines under stricter regulations.

Key Points

- **Increasing focus on ransomware**: This marked the second settlement focused on ransomware breaches in health care, highlighting a growing concern for HHS.
- **HIPAA compliance is critical**: The settlement underscores the importance of implementing and maintaining a robust HIPAA compliance program. This includes conducting regular risk assessments, ensuring safeguards are in place to protect patient data and providing staff training on HIPAA policies.
- **Enforcement actions for non-compliance**: HHS is actively investigating and enforcing HIPAA violations. Providers found to be non-compliant may face financial penalties and corrective action plans.

Recommendations

- Review your HIPAA compliance program to ensure it addresses current security threats, including ransomware.
- Review all vendor and contractor relationships to ensure appropriate business associate agreements are in place and address breach/security incident obligations.
- Conduct a thorough risk assessment to identify vulnerabilities in your IT systems.
- Implement appropriate safeguards to protect patient data, such as encryption and multi-factor authentication.
- Ensure audit controls are in place to record and examine information system activity.
- Regularly monitor your systems for suspicions activity.
- Train your staff on HIPAA policies and procedures, including how to identify and report potential breaches.

Contacts

William E. Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Joshua Silverstein
Counsel / Washington, D.C.
202.371.7148
joshua.silverstein@skadden.com

Seve Gonzales
Associate / Chicago
312.407.0543
seve.gonzales@skadden.com

Lisa V. Zivkovic
Associate / New York
212.735.2887
lisa.zivkovic@skadden.com