CLIENT ALERTS & INSIGHTS

Annual Report to Congress on Breaches of Unsecured Protected Health Information

APRIL 3, 2024

Authors: Kathrin “Kat” Zaki, Christina Hultsch, W. Clifford Mull

Background

The U.S. Department of Health and Human Services (HHS), Office for Civil Rights (OCR) recently published an executive summary (Report) outlining key enforcement activities of the Health Insurance Portability and Accountability Act (HIPAA) in 2022 related to breaches of unsecured protected health information (PHI). OCR received a total of 626 notifications of breaches affecting 500 or more individuals, marking a 3% increase from 2021. These breaches impacted approximately 41.7 million individuals and were predominately caused by hacking and other cyberattacks. Additionally, OCR dealt with 63,966 reports of smaller breaches affecting fewer than 500 individuals, mainly due to unauthorized access or disclosure.

Impact and Enforcement

OCR launched investigations into all significant breaches as well as a selection of smaller breaches, initiating a total of 799 investigations. These investigations were completed through either the provision of technical assistance, voluntary compliance through corrective action, resolution agreements and corrective action plans. Resolution agreements are typically reserved for OCR findings of noncompliance due to willful neglect or other good cause to warrant additional enforcement action. Notably, three OCR breach investigations were settled with resolution agreements and monetary payments totaling $2,425,640.

The Report emphasizes the necessity for regulated entities to enhance their compliance with HIPAA regulations, especially concerning the Security Rule standards related to risk analysis, management, and audit controls. Hacking incidents were highlighted as the leading cause of large breaches, accounting for 74% of the cases in 2022, and affected the most individuals. In contrast, breaches impacting fewer than 500 or more individuals were caused mainly by unauthorized access or disclosure and predominantly impacted paper records as opposed to network servers.

Recommendations and Action Items

There is a high risk of data breaches in the healthcare system and the risk continues to grow as hackers become more sophisticated and as healthcare systems continue to digitize and electronically store sensitive patient data. The recent Change Healthcare outage has demonstrated the serious financial consequences a cyberattack may have. However, the cost of noncompliance may not necessarily be limited to financial harm. Reputational harm due to poor data security infrastructure can become too severe for some healthcare entities to absorb. Additionally, the Change Healthcare outage has shown that cyberattacks can also have a negative impact on patient

safety and healthcare outcomes due to significant disruptions in the timely administration of healthcare. As a result, legislative efforts are underway to encourage healthcare provider compliance with cybersecurity standards by tying payments under federal healthcare programs to the healthcare providers meeting such cybersecurity standards.

To address these issues, we recommend that all entities regulated by HIPAA consider the following top 10 recommendations to mitigate the risk of a data breach and improve their protections against a cyberattack:

1. Risk Analysis and Mitigation: Conduct a thorough risk analysis to identify and mitigate potential security vulnerabilities, including implementation of robust risk management practices to prevent unauthorized access or disclosure.
2. Asses Cyber Insurance Needs: Procure a cyber insurance policy that matches the level of sophistication of your company, with minimum coverage limits of at least one million in the aggregate for smaller entities, and at least five million for larger entities.
3. Security Incident Response: Regularly review system activity to detect and respond to security incidents promptly.
4. Monitor and Record: Enhance audit controls to monitor and record security-related events effectively.
5. Response and Reporting: Strengthen response and reporting mechanisms to address security breaches efficiently.
6. User Authentication Process: Improve authentication processes to verify the identity of persons or entities accessing protected health information.
7. Encryption and Secured Communications: Encrypt sensitive data to render it unusable, unreadable, or indecipherable to unauthorized individuals.
8. Minimum Necessary Data: Ensure proper destruction of protected health information when it is no longer needed and at all times use the minimum necessary data to accomplish goals.
9. Education and Training: Educate workforce members and business associates about their obligations under HIPAA and the importance of safeguarding health information.
10. Compliance Culture: Foster a culture of compliance and security awareness within the organization to prevent breaches and ensure the highest possible protection of PHI.

Implementing these recommendations can help regulated entities not only comply with HIPAA and HITECH Act requirements but also strengthen the protection of PHI and reduce the risk of potential legal, financial, and reputational repercussions.

For additional information, please contact:

Kathrin Zaki at kzaki@beneschlaw.com or 646.777.0040.

Christina Hultsch at chultsch@beneschlaw.com or 614.223.9381.

W. Clifford Mull at cmull@beneschlaw.com or 216.363.4198.