CLIENT ALERTS & INSIGHTS

Annual Report to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance

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. In accordance with the Health Information Technology for Economic and Clinical Health (HITECH) Act, OCR is tasked with annually reporting to Congress on HIPAA Privacy, Security, and Breach Notification Rule Compliance. This authority includes detailing the volume of complaints received, the resolution methods, compliance reviews initiated, outcomes of these reviews, audits conducted, summaries of audit findings, the issuance of subpoenas or inquiries, and planned compliance and enforcement initiatives.

Impact and Enforcement

The Report demonstrated a marked rise in HIPAA complaints (17% increase from 2018 to 2022) and significant breaches reported (107% increase from 2018 to 2022). Despite this increase, OCR conducted no audits and issued no subpoenas in 2022 due to purported financial constraints. In April of 2019, a significant reduction in the maximum annual cap for three of the four penalty tiers was introduced due to a Notification of Enforcement Discretion Regarding HIPAA Civil Money Penalties by HHS. Additionally, the 2021 HITECH Amendment requires OCR to assess whether entities have maintained recognized security practices for the preceding twelve months when determining fines or other remedies in resolving potential HIPAA Security Rule violations.

In 2022, OCR received 30,435 new complaints alleging HIPAA violations, resolving 32,250 complaints in various manners. Most of these complaints were resolved before initiating an investigation (87%), with a minor fraction resulting in corrective action following an investigation (2%), and some resolved with resolution agreements and monetary settlements totaling $802,500. Additionally, OCR completed 846 compliance reviews, with a significant number of cases necessitating corrective action or resulting in civil money penalties.

The Report highlights numerous outreach activities conducted by OCR for the purpose of educating the healthcare industry about implementing recognized security practices as well as the process for demonstrating such practices to OCR in the event of an investigation or audit. OCR outreach activities include regular updates to HIPAA web content, informational videos and webinars targeted at healthcare professionals and practices, and numerous guidance documents related to HIPAA compliance in various settings and applications (e.g. reproductive healthcare data; cell phone or tablet considerations; telehealth and cyberattack risk; etc.)

Recommendations and Next Steps

Notwithstanding the challenges faced by OCR in enforcing HIPAA compliance amidst rising cybersecurity threats and increasing regulatory responsibilities, the Report provides valuable insight into the OCR investigation process. The significant increase in patient complaints and steeper penalties resulting from failure to maintain recognized security practices should serve as a cautionary tale to covered entities and business associates. Based on the findings highlighted in the Report, here are the top 10 recommendations for entities regulated by HIPAA to improve compliance and enhance data protection efforts:

1. Strengthen Security Practices: Implement and maintain recognized security practices as outlined in the 2021 HITECH Amendment, including adopting standards and guidelines developed under the National Institute of Standards and Technology Act and the National Cybersecurity Protection Act.
2. Enhance Risk Assessments: Regularly conduct comprehensive risk assessments to identify vulnerabilities within electronic health record systems and implement necessary security measures to mitigate these risks.
3. Invest in Cybersecurity: Allocate sufficient resources towards cybersecurity infrastructure and personnel training to keep pace with evolving threats and maintain compliance with the HIPAA Security Rule requirements.
4. Report Breaches Promptly: Ensure timely reporting of any breaches as required by the HIPAA Breach Notification Rule to avoid penalties and maintain transparency with affected individuals and regulatory bodies.
5. Seek Technical Assistance When Needed: Take advantage of the technical assistance offered by OCR to resolve potential non-compliance issues before they escalate into formal investigations or require corrective actions.
6. Educate Workforce Regularly: Conduct ongoing training programs for all workforce members on HIPAA privacy and security policies, emphasizing the importance of protecting patient information and understanding the legal obligations.
7. Monitor and Audit Compliance: Implement regular monitoring and auditing mechanisms to ensure continuous compliance with the HIPAA regulations and to detect potential violations or security breaches early.
8. Engage with Business Associates: Ensure that all business associates and subcontractors are fully compliant with HIPAA regulations, including executing business associate agreements that clearly outline responsibilities and expectations for protecting protected health information (PHI).
9. Prepare for Compliance Reviews: Develop and maintain an organized and comprehensive documentation process for HIPAA compliance efforts to facilitate OCR's compliance reviews and demonstrate adherence to regulatory requirements.
10.

Stay Informed About Regulatory Changes: Keep abreast of any changes or updates to the HIPAA regulations, including regular review of guidance documents and web programming published by HHS and OCR.

Implementing these recommendations can help regulated entities not only comply with HIPAA and HITECH Act requirements but also strengthen the protection of PHI. This will ultimately foster patient trust 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.