PUBLICATION

HIPAA Updates: The Obligations Continue to Unfold

Authors: Alisa L. Chestler, Layna S. Cook Rush
February 19, 2024

There has been a notable emphasis on proactive enforcement of the privacy and security of protected health information in recent weeks as evidenced by multiple developments regarding compliance with the Health Insurance Portability and Accountability Act (HIPAA). Recent developments include launching the HIPAA Audit Review Survey aimed at evaluating the effectiveness of past audits and gathering feedback – potentially foreshadowing the return of the audit program. The Department of Health and Human Services (HHS) introduced Healthcare and Public Health Cybersecurity Performance Goals (HPH CPGs) to bolster cybersecurity practices, particularly for small- and medium-sized health care organizations. Additionally, the National Institute of Standards and Technology (NIST) finalized the updated Cybersecurity Resource Guide, while HHS, through Substance Abuse and Mental Health Services Administration (SAMHSA) and Office for Civil Rights (OCR), issued a Final Rule aligning Part 2 regulations with HIPAA rules. In response, HIPAA-covered entities and their business associates should thoroughly assess their privacy and security programs, ensuring compliance with HIPAA rules and the implementation of industry-standard security controls.

OCR Audit Program

OCR, the agency within HHS tasked with HIPAA enforcement, announced a HIPAA Audit Review Survey in a notice published in the Federal Register on February 12, 2024. The 207 covered entities and business associates that participated in the 2016 – 2017 OCR HIPAA Audits will receive this online survey consisting of 39 questions. OCR specifically asks for information regarding subsequent HIPAA compliance actions taken by the survey recipients as a result of the previous audits to evaluate the effectiveness of the audits and the counseling the organizations obtained from OCR in response to the audits. The surveys allow covered entities "to give feedback on the Audit and its features, such as the helpfulness of HHS' guidance materials and communications, the utility of the online submission portal, whether the Audit helped improve entity compliance, and the entities' responses to the Audit-report findings and recommendations." Furthermore, the survey asks for information regarding the burden the audits place on entities – specifically regarding the collection of necessary documents and audit-related requests – and how the audit program impacts day-to-day business operations.

The HIPAA compliance audit program officially started in 2011 after the Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 required OCR to conduct the audits. Covered entities and business associates were able to use the OCR audit protocol to determine their compliance with the HIPAA rules. The audit program ceased in 2017. Presumably the information gathered will inform an updated audit program in the future. However, it is still unknown when the next phase of the program would begin.

We recommend organizations that have not utilized the OCR audit protocol to consider such a review in anticipation of OCR resuming the program.

Cyber Performance: Small and Medium Organizations

HHS recently launched the new Healthcare and Public Health Cybersecurity Performance Goals (HPH CPGs). As HHS explains, the CPGs are meant to provide health care delivery organizations with practices that will "strengthen cyber preparedness, improve cyber resiliency, and ultimately protect patient health information and safety." The goal of the HPH CPGs is to help small- and medium-sized health care organizations to strengthen their cybersecurity practices given the proliferation of ransomware and other cybersecurity concerns within the industry. The HPH CPGs serve as baseline methods to secure patient information and are not a replacement for a comprehensive HIPAA compliance program. They are designed to help entities meet certain requirements and should be considered a minimum threshold for small and medium organizations to reduce the risks associated with some of the more common cyber incidents. The HPH CPGs serve as a tool for understanding the many facets of the steps needed for a minimum level of cybersecurity controls.

NIST Security Guide Update

On February 14, 2024, NIST finalized the update to, "Implementing the HIPAA Security Rule: A Cybersecurity Resource Guide," the resource guide for implementing the HIPAA Security Rule. The NIST Guide was originally published in 2005, updated in 2008, and then again in 2022 with a draft update. NIST has adopted some of the comments made to the 2022 draft in the most recent release. The updated version serves as a key resource for information technology, security, and compliance personnel in ensuring the risks of the organization have been evaluated, documented, updated, and remediated as required.

Confidentiality of Substance Use Disorder Patient Records

As detailed in a recent Baker Donelson alert, HHS, through SAMHSA and OCR, recently issued a Final Rule modifying the Confidentiality of Substance Use Disorder (SUD) Patient Records regulations, 42 CFR Part 2 (Part 2). The modifications serve to align Part 2 with HIPAA and HITECH in areas where Part 2 previously differed on the requirements for protecting confidential patient medical records. While the Final Rule is expected to become effective on April 16, 2024, SUD providers have until February 16, 2026, to come into compliance.

The recent publication of guidance by government agencies and the indications that OCR may revive the audit program should motivate health care entities to scrutinize their privacy and security programs to ensure they are, at a minimum, in compliance with the HIPAA rules and that they are implementing industry-standard security controls. HIPAA-covered entities and their business associates should regularly conduct risk analysis, update mitigation plans, and review and revise compliance programs.

Our HIPAA Compliance Team is available to assist entities with review of their compliance programs and offer guidance on implementing additional controls. For more information, contact Alisa L. Chestler, CIPP/US, QTE, Layna Cook Rush, CIPP/US, CIPP/C, or the Baker Donelson HIPAA attorney with whom you regularly work.