KROKIDAS & BLUESTEIN LLP

CLIENT ALERT

HHS AND OCR RECOMMENDATIONS TO PREVENT AND MITIGATE CYBERSECURITY BREACHES

Department of Health and Human Services ("HHS") data has revealed that roughly 50 million Americans across 49 states had their health information breached in 2021, a threefold increase from 2018. The same data shows that as the health care industry grows more digitized, cybercriminals are becoming increasingly aggressive. Last year, hackers were responsible for 74% of all health data breaches, more than twice the share of such breaches caused by hackers in 2016. The geopolitical conflict in Eastern Europe has increased cyberattacks by state actors who target health care organizations. A joint cybersecurity advisory from the U.S. Cybersecurity and Infrastructure Security Agency (CISA) and other international cybersecurity authorities has cited intelligence that Russian state actors and cybercrime groups are exploring options for cyberattacks against critical infrastructure beyond the boundaries of Europe.

To reduce the threat of cyberattacks against protected health information, the HHS Office for Civil Rights ("OCR") has recently recommended that covered entities and business associates take additional preventative steps to implement HIPAA-compliant cybersecurity safeguards.

OCR-Recommended Safeguards

In its first quarter cybersecurity newsletter of 2022, OCR reminds all covered entities and business associates that the most common cyberattacks – phishing, known vulnerabilities, and weak authentication protocols – can be mitigated by implementing requirements under the HIPAA Security Rule. OCR recommends several safeguards, including:

- Ongoing training and simulated phishing emails to test personnel security awareness and prevent ransomware attacks;
- System risk analyses and subscriptions to NIST, CISA, and HC3 agency alerts in order to identify known vulnerabilities;
- Continuous security upgrades to address known vulnerabilities; and
- Multi-factor authentication, strong passwords, and access management processes to protect privileged accounts.

Potential Mitigation of HIPAA Fines and Penalties under the HIPAA Safe Harbors Act

Protecting sensitive health information has been and continues to be the most important reason for health care organizations to take preventative steps against cyberattacks. However, the 2021 "HIPAA Safe Harbors Act" (effective January 5, 2021) now provides the added incentive of the

possible mitigation of fines and penalties by OCR for organizations that adopted recognized cybersecurity practices before experiencing a security breach.

The new Act requires OCR to consider whether a covered entity or business associate had demonstrated HIPAA-compliant security practices for the previous 12 months when determining penalties for HIPAA violations. The Act also grants covered entities and business associates the flexibility to choose the recognized security practices that are appropriate for the size, complexity, and capabilities of the organization, as consistent with the HIPAA Security Rule. Organizations are not required to implement recognized security practices, nor will they face higher penalties for choosing not to implement them. However, an adequate demonstration of recognized security practices may reduce the likelihood or impact of a future security breach while reducing the risk of punitive measures imposed by OCR should a breach occur.

Although only preventative measures are eligible to be rewarded under the HIPAA Safe Harbors Act, swift corrective responses by organizations that have experienced a health data breach may be looked upon favorably, particularly if significant time passes before OCR investigates. For this and the other reasons discussed above, we strongly recommend that organizations that have experienced a health data breach implement recognized security practices if they have not done so already.

Covered entities and businesses looking to adopt recognized security practices may start by consulting the resources shared by the HHS 405(d) Program and Task Group, OCR Security Rule Guidance Materials, and the NIST *Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, along with other HHS and NIST resources.

If you have questions about HIPAA compliance, please contact Jennifer Gallop (jgallop@kb-law.com); Anthony Cichello (acichello@kb-law.com); and Emily Kretchmer (ekretchmer@kb-law.com).