March 2023 Update to

Cybersecurity Framework Guide

The Administration for Strategic Preparedness & Response (ASPR) recently issued an update to the Health Sector Cybersecurity Framework Implementation Guide (March 2023). Today's climate of increasingly sophisticated cyberattacks have many healthcare organizations feeling vulnerable and ill-prepared to address the daily threats and ongoing compliance requirements.

The U.S. Office for Civil Rights (OCR) notes that many, if not most, healthcare organizations struggle with managing cybersecurity effectively. The OCR reports that organizational failure to conduct an accurate and thorough risk analysis is one of the most frequent violations of the HIPAA Security Rule (*based on fines and resolution agreements*).

In addition to risk analysis, the update highlights the importance of a broader, more collaborative approach to risk analysis that will enhance the ability to effectively identify and manage organizational risk, safeguard patient privacy, and protect business value. Staff can provide excellent perspectives regarding cybersecurity risk at the point of care.

Brian Williams, Vice President of Compliance at MedTrainer recognizes the complexity of HIPAA compliance and the overwhelming need for improving cybersecurity preparedness, as there is not a one-size-fits-all solution. He suggests that organizations start by conducting security risk assessments to reveal the improvements urgently needed in order to enhance cybersecurity and staff awareness.

To learn more about how to conduct a HIPAA Security Risk Analysis click here. Next month, we will discuss how to interpret the results of the SRA and strategies to improve HIPAA compliance and preparedness for what appears to be inevitable cybersecurity attacks on healthcare organizations of all sizes.

Source: Health Care & Public Health Sector Cybersecurity Framework Implementation Guide Version 2, March 2023