CYBERSECURITY AND DATA PRIVACY LAW ALERT
October 23, 2025
By: Leora F. Ardizzone, Esq.

RMF
RuskinMoscouFaltischek P.C.
Smart Counsel. Straight Talk.

Risk Analysis: An Ounce of Prevention

On January 6, 2025, a Notice of Proposed Rulemaking was published that would have changed the HIPAA Security Rule, to include among other things, more specific requirements for conducting a risk analysis. See here. In its current iteration, the risk analysis requirement was not intended to be a one size fits all rule, and there were certain minimum requirements based on recommendations of the National Institute of Standards and technology. The Risk Analysis Standard under the Security Rule (45 CFR 164.308(a)(1)) required organizations to conduct a thorough and accurate assessment of potential risks and vulnerability to the confidentiality, integrity and availability of electronic protected health information (ePHI) held by a covered entity or business associate. In guidance published by the Health and Human Services Department, Office of Civil Rights (OCR), regulated entities are advised to periodically identify where all ePHI is maintained, transmitted and received; identify and document threats and vulnerabilities unique to its environment; the likelihood of a threat occurring and the potential impact of such an occurrence; assess and document the organization's security measures in effect to safeguard ePHI; determine the risk levels of any threats or vulnerabilities identified during the risk analysis and corrective actions to mitigate those risks. See here.

In the Notice of Proposed Rule Making, the OCR noted that many regulated entities failed to invest adequate resources in cybersecurity and only between 14-17% of regulated entities are "substantially fulfilling their regulatory responsibility to safeguard ePHI they [held] through risk analysis activities." As a result of the failure of regulated entities to perform risk analyses despite the regulation and published guidance, the Proposed Rule seeks to convert the published guidance into law and require that every regulated entity conduct a risk analysis not less than once every 12 months and in response to a change in the regulated entity's environment. The public comment period to the proposed rule closed in March 2025, but in February 2025, the College of Healthcare Information Management Executives, America's Essential Hospitals, American Health Care Association, Association of American Medical Colleges, Federal of American Hospitals, Health Innovation Alliance, Medical Group Management Association and National Center for Assisted Living sent a letter to President Trump objecting to the Proposed Rule changes and requesting that the Proposed Rules be rescinded immediately. See here. Among the reasons for their objections is that the financial burdens of compliance would adversely impact health care delivery, stifle innovation and would not improve cybersecurity. The authors of the letter propose that instead of imposing costly mandates, the federal government should provide more support and resources to healthcare providers, especially to those who are targeted by foreign bad actors.

As of the date of this article, a final rule has not been published but even before the Notice of Proposed Rule Making was published, the OCR announced its "Risk Analysis Initiative" in a press release announcing a resolution agreement with Bryan County Ambulance Authority, and since then it has been engaged in enforcement actions. See here. In 2025 alone, the OCR announced a number of settlements of enforcement actions where a key issue was the failure to perform a comprehensive risk analysis. The following represents a few examples of those settlements:

In March 2025 the OCR announced a settlement with Health Fitness Corporation, (HFC) a business associate providing wellness plans to clients across the country. See here. The settlement was made after HFC made four reports to OCR of breach on behalf of multiple covered entities between October 2018 and January 2019 when it discovered a software misconfiguration on the server housing ePHI affecting 4,304 patients. After concluding its investigation, OCR found that HFC failed to conduct an accurate and thorough risk analysis. As part of its settlement, HFC agreed to conduct a thorough risk analysis and to develop and implement a risk management plan, to being monitored by OCR for two years and pay a fine of $277,816 to OCR.

In April 2025, the OCR announced a settlement with Northeast Radiology, P.C., (NERAD) a radiology practice, after a report of breach of NERAD's Picture Archiving and Communications System was made in 2020 affecting close to 300,000 patients. See here. After concluding its investigation, OCR found that NERAD failed to conduct a comprehensive risk analysis. As part of its settlement, NERAD agreed to conduct a thorough risk analysis and to develop and implement a risk management plan, to being monitored by OCR for two years and pay a fine of $350,000 to OCR.

In July 2025, the OCR announced a settlement with Deer Oaks, a behavioral health provider after receiving a complaint that Deer Oaks impermissibly disclosed ePHI. See here. During the investigation, Deer Oaks claimed that the ePHI was exposed as a result of a coding error in a discontinued online patient portal from December 2021 through May 2023.The investigation also found that Deer Oaks experienced a breach in August 2023 when a threat actor claimed to have exfiltrated patient data and demanded payment to prevent posting the data on the dark web. OCR concluded that Deer Oaks failed to conduct an accurate and thorough risk analysis, and as part of its settlement, Deer Oaks agreed to conduct a thorough risk analysis and to develop and implement a risk management plan, to being monitored by OCR for two years and pay a fine of $225,000 to OCR.

In August 2025, the OCR announced a settlement with BST & Co. CPAs, LLP, (BST) an accounting firm, after receiving a breach report that BST filed in February 2020 following a ransomware attack impacting PHI of its covered entity client. See here. After concluding its investigation, OCR found that BST failed to conduct an accurate and thorough risk analysis. As part of its settlement, BST agreed to conduct a thorough risk analysis and to develop and implement a risk management plan, to being monitored by OCR for two years and pay a fine of $175,000 to OCR.

It may still take some time before the Final Rule is issued, if it ever is. Regardless, the law still requires that regulated entities conduct risk analyses and the OCR has made clear, with its Risk Analysis Initiative, that the failure to conduct a comprehensive, accurate and thorough risk analysis will result in the imposition of fines and corrective action. Don't wait until your patient's ePHI is compromised. Take action now and make sure to conduct annual risk analyses that include at minimum, the following:

1. Identify and document where ePHI may be created, received, maintained, or transmitted.
2. Identify reasonably anticipated threats to ePHI.
3. Identify potential vulnerabilities and risks to ePHI, including but not limited to risks associated with business associate arrangements.
4. Assess and document security measures protecting ePHI.
5. Determine the likelihood that a threat will exploit vulnerabilities.
6. Determine the potential impact that a threat will successfully exploit vulnerabilities.
7. Assess the risk level for each threat and vulnerability.

Failure to comply with existing risk analysis requirements and published guidance could result in significant monetary penalties and reputational damage following exposure of ePHI under your control. For more information or any other cybersecurity related issues, or if you have experienced a data breach, please contact:

Leora F. Ardizzone
(516) 663-6538
lardizzone@rmfpc.com