HHS-OCR Risk Analysis Enforcement Initiative Continues Under New Administration

Author: Brian H. Myers and Mendel Epstein

In April 2025, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR)[1] announced a settlement marking its eighth enforcement action in its Risk Analysis Initiative.[2] Since its introduction in October 2024, the initiative already has resulted in combined settlement payments of nearly $900,000 from eight different health care organizations.

When announcing the initiative in October 2024, the OCR Director stated that "failure to conduct a HIPAA Security Rule risk analysis leaves health care entities vulnerable to cyberattacks, such as ransomware. Knowing where your ePHI is held and the security measures in place to protect that information is essential for compliance with HIPAA."[3] The Director expressed that OCR created the initiative to "highlight the need for more attention and better compliance with this Security Rule requirement."

The initiative follows a compliance audit conducted by OCR in 2016–2017, from which OCR concluded that only 14 percent of covered entities were substantially fulfilling their regulatory responsibilities to safeguard ePHI through risk analysis activities.[4]

Notably, the two most recent settlements under the risk analysis initiative were obtained in February 2025 and announced in April 2025, indicating that the Trump Administration is continuing to pursue the initiative first announced by the Biden Administration. The ongoing enforcement initiative underscores the importance of health care organizations understanding the Security Rule's requirements and conducting a proper risk analysis.

What Exactly Is a Risk Analysis?

HIPAA's Security Rule requires organizations to conduct a "risk analysis" that includes "an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by a covered entity or business associate."[5]

According to HHS,[6] conducting a risk analysis is the "first step" and a "foundational element" in an organization's Security Rule compliance.[7] However, the Security Rule does not specify a precise methodology for conducting a risk analysis.[8] According to HHS, "there are numerous methods of performing [a] risk analysis and there is no single method or 'best practice' that guarantees compliance with the Security Rule."[9] While this grants organizations some flexibility, it also creates uncertainty as to precisely what constitutes compliance with the risk analysis requirement.

To reduce some of this uncertainty, HHS issued guidance on "several elements a risk analysis must incorporate, regardless of the method employed."[10] Those elements include the following:

- **Document where ePHI is stored and transmitted (data inventory and mapping).** The scope of the risk analysis must include all ePHI in all forms of electronic media. Examples include portable devices such as thumb drives, laptops, and mobile phones as well as

individual desktops, email accounts, fax machines, printers, network storage devices such as file servers and backup servers, cloud storage servers, and electronic medical record (EMR) servers. Other examples may be specific to an organization's practice, such as a medication dispensing system or imaging devices, if they store or transmit ePHI. The risk analysis should include an inventory that identifies and documents all places where ePHI is stored or transmitted and map how data flows to, from, and within the organization.

- **Document Potential Threats and Vulnerabilities.** For each place where ePHI is stored or transmitted, the organization must identify and document reasonably anticipated threats and vulnerabilities to ePHI in each location. For example, if ePHI is stored and transmitted in email accounts, one vulnerability is a compromise of the credentials for the email account. If ePHI is stored and transmitted on the local hard drives of portable devices such as laptops or smartphones, another vulnerability is unauthorized access to the data on the device, should it be lost or stolen.
- **Document Current Security Measures.** For each place where ePHI is stored or transmitted, the organization must document its current security measures protecting that location from threats and vulnerabilities. Using the example of portable devices, the organization may encrypt locally stored data at the hardware level or implement remote access tools that administrators can use to delete the device's contents.
- **Determine the Level of Risk.** While the Security Rule does not specifically define "risk," HHS guidance defines risk as a function of (1) the probability that a particular threat will trigger or exploit a particular vulnerability and (2) the impact to the organization should this occur. HHS recognizes that this process could be quantitative or qualitative. For example, an organization could quantify risk on a scale of 1 to 10. Alternatively, an organization could characterize risk as low, medium, or high.
- **Document Risk Analysis.** The organization must document the results of its risk analysis, including each step of the process outlined above. A short summary report will likely not be sufficient to demonstrate that the risk analysis was "accurate and thorough." Documenting the risk analysis is especially important when an organization is being audited by OCR after experiencing a data breach, as OCR often requests copies of all risk analysis reports going back as far as six years.
- **Repeat Analysis.** HHS recognizes that the Security Rule does not specify how frequently an organization must perform a risk analysis. HHS guidance states that organizations should conduct risk analysis annually, biennially, or every three years. However, the department's recent Notice of Proposed Rulemaking would require organizations to conduct a risk analysis at least annually.[11] HHS guidance also maintains that organizations should conduct a risk analysis whenever an organization makes a material change to its operations. HHS provides examples of situations that might require an updated risk analysis, including a security incident, a change in ownership, turnover in key staff or management, or the incorporation of new technology.

Common Deficiencies

The HHS Senior Advisor for Cybersecurity presented a webinar in October 2023 that elaborated on the risk analysis requirements.[12] During the webinar, the presenter emphasized that a risk analysis must be "accurate and thorough," noting that a common deficiency in risk analyses is the failure to conduct an inventory of all systems that store or transmit ePHI. The presenter also acknowledged that organizations often conflate a HIPAA compliance gap assessment with a risk analysis, which are two different things.

Other common deficiencies include the use of template forms or generic tools in conducting a security risk analysis. OCR has specified that the risk analysis must pertain to the specific operations of the organization. Template forms and generic tools may fail to account for the unique aspects of an organization's network and fail to identify specific risks posed to that environment.

Where to Begin

Again, the Security Rule allows organizations flexibility in how they conduct their risk analysis. HHS points to NIST Special Publication 800-30 as one example of a guide for conducting a risk analysis.[13] In addition, the Office of the National Coordinator for Health Information Technology (ONC), in collaboration with OCR, developed a Security Risk Assessment Tool (SRA Tool). The SRA Tool is a computer application designed to walk health care organizations through the steps of a risk analysis.[14]

While the SRA Tool may be helpful as a starting point, HHS maintains that it is provided for informational purposes only.[15] HIPAA does not require its use, and its use does not guarantee compliance with HIPAA.[16] Fundamentally, the SRA Tool still requires organizations to make their own judgments regarding the probability, impact, and risk posed by any particular threat or vulnerability.

For support in identifying threats and vulnerabilities, making judgments about risk, and developing risk management plans, organizations often engage subject matter experts such as cybersecurity firms and law firms to help conduct a risk analysis. In light of OCR's ongoing enforcement initiative and the risks posed by cybersecurity incidents, health care organizations will benefit from conducting a thorough risk analysis at their earliest opportunity.

---

[1] The OCR within HHS is the primary enforcement agency for HIPAA. They conduct investigations, compliance reviews, and take enforcement actions against covered entities that violate the Privacy or Security Rules.

[2] U.S. Dept. of Health and Human Services, "HHS Office for Civil Rights Settles HIPAA Ransomware Cybersecurity Investigation with Neurology Practice" (April 25, 2025) available at https://www.hhs.gov/press-room/ocr-hipaa-racap-np.html (last accessed May 14, 2025).

[4] 90 FR 915

[5] 45 C.F.R. § 164.308(a)(1)(ii)(A).

[6] As the arbiter of HIPAA regulations, HHS is also charged with providing guidance to medical providers as to interpreting and implementing the requirements set forth by the regulations.

[10] *Id.* Notably, OCR issued a Notice of Proposed Rule Making in January 2025, seeking to amend the Security Rule's risk analysis requirement to explicitly incorporate these elements. 90 FR 898.