OCR's Risk Analysis Initiative: Lessons From Recent HIPAA Enforcement Actions

JUNE 9, 2025

GAYLAND O. HETHCOAT II

Health care organizations are under pressure to shore up their cybersecurity response efforts. Much of this pressure is coming from the US Department of Health and Human Services Office for Civil Rights (OCR), which has made clear through recent enforcement actions that conducting a proper risk assessment under the Health Insurance Portability and Accountability Act (HIPAA) Security Rule is not optional.

These enforcement actions ratcheted up during the Biden Administration and have continued during the Trump Administration, signaling that risk analysis remains a top compliance priority for organizations charged with complying with HIPAA.

HIPAA's Risk Assessment Requirement and Why It Matters

Under the HIPAA Security Rule (as codified in 45 C.F.R. § 164.308), all HIPAA covered health care providers, health plans, health care clearinghouses (covered entities), and their business associates (collectively, regulated entities) must "[c]onduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information [ePHI] held by the covered entity or business associate." OCR has repeatedly described this assessment (also referred to as a risk analysis) as the "**foundation for**

effective cybersecurity practices and the protection of ePHI." Without a proper assessment, regulated entities may not know where their information is stored and how (if at all) it is protected, undermining their ability to implement the Security Rule's safeguards to protect ePHI.

OCR considers risk analysis especially critical given today's threat landscape. Ransomware — a type of malicious software that encrypts data, rendering it inaccessible, and demands a ransom for its release — and other hacking incidents have surged in health care, with a 264% increase in large breaches involving ransomware since 2018. Major cyberattacks often succeed because security gaps are unidentified or unaddressed. A risk assessment compels regulated entities to evaluate these gaps — from unencrypted devices and open ports to outdated software and lax access controls — before a breach occurs.

OCR Launches "Risk Analysis Initiative"

In October 2024, OCR announced that it was launching a "Risk Analysis Initiative" focused on enforcing the Security Rule's risk analysis requirement. The agency made the announcement in a **press release** about a settlement with Bryan County Ambulance Authority (BCAA) in Oklahoma, following a ransomware attack that encrypted the ePHI of 14,273 patients. According to OCR, BCAA violated the Security Rule by failing to conduct a compliant assessment to determine the potential risks and vulnerabilities to ePHI in BCAA's systems. Under the terms of a resolution agreement, BCAA agreed to pay $90,000 and implement a corrective action plan.

The findings in the BCAA case, however, were not an anomaly. As OCR noted in a **2024 report to Congress** about reported breaches from 2022, the agency identified "numerous instances" where regulated entities' risk analyses were inadequate. "Specifically," the report stated, "the risk analyses, if conducted at all, were often based on incomplete inventories of where PHI is created, received, maintained or transmitted, resulting in an incomplete assessment of risks and vulnerabilities that is deficient in scope."

The Risk Analysis Initiative was OCR's answer to this problem — an enforcement project explicitly targeting noncompliance with the Security Rule's risk analysis requirement. In the BCAA press release, the agency explained that it would focus select investigations on whether regulated entities have performed a comprehensive risk assessment, with the goal of increasing completed enforcement cases and spotlighting the need for better compliance. In practical terms, this means that if a regulated entity reports a cyberattack-related breach or otherwise comes under OCR's scrutiny, one of the first questions the agency may ask is whether the entity has proof of an up-to-date, thorough risk analysis. Lacking such proof could lead to significant penalties.

Between the announcement of the BCAA settlement and President Trump taking office on January 25, OCR publicly reported three additional enforcement actions under the banner of the Risk Analysis Initiative, all of which included monetary payments and corrective action plans. On January 7, the agency announced parallel settlements with two business associates that were the targets of separate ransomware attacks. In one, an **electronic health records vendor** that experienced a breach of 31,248 individuals' ePHI agreed to pay $80,000 to resolve OCR's allegation that it failed to conduct an accurate and thorough risk assessment. In the other, OCR reached a **$90,000 settlement with a data hosting and cloud service provider** for similar alleged violations that the agency uncovered after ransomware encrypted the ePHI belonging to a dozen of the company's covered entity clients. In the **third enforcement action**, which OCR announced on January 15, the agency settled with a surgical group for $10,000 after a ransomware attack exposed the ePHI of 15,298 patients.

Risk Analysis Initiative Continues During Trump Administration

Since President Trump began his second term, OCR has announced five more enforcement actions as part of the Risk Analysis Initiative. While these cases were initiated during the Biden Administration (or during the first Trump Administration), their resolution and spotlight in OCR press releases this year underscores OCR's continued enforcement focus. Indeed, the current OCR leadership (now under an acting director) has explicitly reiterated the messaging during the Biden Administration, describing compliance with the risk analysis requirement as "**the first step**" to prevent or mitigate breaches of ePHI.

The latest enforcement actions involve settlements ranging from $25,000 to $350,000 and breaches affecting between 4,304 and 585,621 individuals' ePHI. Notably, unlike the prior Risk Analysis Initiative cases that were publicized during the Biden Administration, which all stemmed from ransomware attacks, these more recent cases reflect a broader range of security failures. For example, OCR's settlement with a company that provides wellness plans to covered entities arose from ePHI becoming discoverable on the internet and being exposed to automated search devices (web crawlers) due to a software misconfiguration on the server housing the ePHI. In a **settlement with a radiology group**, unauthorized individuals had accessed radiology images stored on the group's Picture Archiving and Communication System (PACS) server. The common thread across all these actions, regardless of the breach type, was the regulated entity's alleged failure to conduct a sufficient risk analysis.

The chart below summarizes key details from all nine of the Risk Analysis Initiative settlements to date.

OCR's Risk Analysis Initiative Settlements (Through June)

Name	Entity Type	Settlement Amount	Individuals Affected	Type of Breach	Year Breach Was Reported
Bryan County Ambulance Authority	Covered Entity	$90,000	14,273	Ransomware	2022
Elgon Information Systems	Business Associate	$80,000	31,248	Ransomware	2023
Virtual Private Network Solutions, LLC	Business Associate	$90,000	6,400	Ransomware	2021
Northeast Surgical Group, P.C.	Covered Entity	$10,000	15,298	Ransomware	2023
Health Fitness Corporation	Business Associate	$227,816	4,304	Server software misconfiguration	2018

Northeast Radiology, P.C.	Covered Entity	$350,000	298,532	Unauthorized access to PACS server	2020
Guam Memorial Hospital Authority	Covered Entity	$25,000	5,000	Ransomware	2019
Comprehensive Neurology, PC	Covered Entity	$25,000	6,800	Ransomware	2020
Comstar, LLC	Business Associate	$75,000	585,621	Ransomware	2022

In addition to those cases formally designated as part of the Risk Analysis Initiative, OCR continues to take enforcement actions in which violations of the Security Rule's risk analysis requirement play a central role, even if the settlement is not explicitly categorized under the initiative. These cases often involve multiple alleged deficiencies in HIPAA compliance. For example, on April 23, OCR announced a **$600,000 settlement with a California health care network** that experienced a phishing attack impacting 45 of its employees' email accounts, resulting in the breach of 189,763 individuals' ePHI. OCR alleged that its investigation revealed multiple potential HIPAA violations, including failure to conduct a comprehensive risk analysis. The case illustrates that risk assessment shortcomings continue to be a common thread in enforcement activity, whether or not they are labeled as part of a focused initiative.

Key Takeaways

OCR's recent enforcement actions demonstrate that the HIPAA Security Rule risk analysis requirement is not a mere paperwork exercise but a strategic compliance imperative with direct implications for cybersecurity readiness. The Risk Analysis Initiative has persisted across Administrations, reflecting a commitment to enforcing this cornerstone of security compliance, and the rising volume and breadth of settlements show that OCR is holding covered entities and business associates of all types and sizes accountable for thorough risk assessments. Regulated entities should therefore treat risk analysis as an urgent compliance priority integrated into their cybersecurity strategy. By doing so, and by seeking experienced legal guidance to navigate regulatory expectations and minimize liability risks, organizations can better fortify their defenses and withstand OCR's heightened scrutiny.

Contacts

Gayland O. Hethcoat II
COUNSEL

Related Industries

Health Care

— Health Privacy, Security & HIPAA

Continue Reading

HEALTH CARE COUNSEL BLOG

FDA Launches National Sweep of Deceptive Drug Advertisements

SEPTEMBER 30, 2025 | STEPHANIE TRUNK, SHOSHANA GOLDEN, EMILY COWLEY LEONGINI

HEALTH CARE COUNSEL BLOG

‘Ghost Network’ ERISA Class Action Lawsuit Settled: Key

Takeaways for Health Care Providers

SEPTEMBER 25, 2025 | MOLLY J. WILTSHIRE, KATIE HEILMAN, ALISON LIMA ANDERSEN

All Insights from Health Care Counsel Blog

HEALTH CARE COUNSEL BLOG

HHS Signals Heightened Information Blocking Enforcement

SEPTEMBER 16, 2025 | GAYLAND O. HETHCOAT II