

OCR's Risk Analysis Initiative: Lessons from the BST Settlement



Meghan O'Connor is a partner at Quarles & Brady LLP, where she provides strategic counsel in the areas of data privacy and cybersecurity, regulatory compliance, information governance, and commercial contracting and transactions. She is also co-chair of the firm's Data Privacy & Security Industry Team and the Artificial Intelligence Team.



Sarah Erdmann is a partner at Quarles & Brady LLP. Ms. Erdmann guides clients on a variety of data privacy and security compliance matters for health and non-health clients.



Simone Colgan Dunlap is a partner at Quarles & Brady LLP and advises clients on regulatory compliance and related risk management and corporate/contracting matters. She is also the firm's National Vice Chair for the Health & Life Science Practice Group.

Meghan O'Connor / Sarah Erdmann / Simone Colgan Dunlap

In August 2025, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced a settlement with a New York-based accounting and advisory firm, BST & Co. CPAs, LLP (BST), that serves as both a clear enforcement signal for OCR under the Trump administration and a valuable case study in the evolving landscape of security requirements under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

The underlying investigation concerned a potential violation of the HIPAA Security Rule; specifically, the failure to conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information (ePHI), and resulted in a settlement under which BST was required to pay \$175,000 to OCR and implement a corrective action plan to be monitored by OCR for two years.¹

OCR's investigation of BST stemmed from a breach notification report BST filed in February 2020 regarding BST's 2019 ransomware attack that affected the ePHI of BST's covered entity client.² This settlement is evidence of the increase in enforcement actions brought about by the OCR's Risk Analysis Initiative (Initiative), which was created to investigate compliance with the HIPAA Security Rule risk analysis provision.

Based on the continued enforcement actions under the Initiative, HIPAA-covered entities and business associates that have not completed a risk analysis recently should plan to timely undertake one, set a regular cadence for risk analyses, and be prepared to update timelines as necessary to address changes in IT systems or architecture, organizational changes, or in response to a new threat or incident.

UNDERSTANDING THE ENFORCEMENT LANDSCAPE

OCR launched the Initiative in the fall of 2024, during the Biden administration, in response to a 264% increase in breaches involving ransomware attacks since 2018.³ OCR audits found that 86% of covered entities and 83%

of business associates audited were not substantially implementing the risk assessment requirements of the Security Rule.⁴

Through the Initiative, OCR has been sending a clear message that compliance with HIPAA risk analyses is an enforcement priority. That message is reinforced by OCR's recent settlement with BST, which marks OCR's 15th ransomware enforcement action and 10th overall settlement under the Initiative.

“A HIPAA risk analysis is essential for identifying where ePHI is stored and what security measures are needed to protect it,” OCR Director Paula M. Stannard said in a press release. “Completing an accurate and thorough risk analysis that informs a risk management plan is a foundational step to mitigate or prevent cyberattacks and breaches.”⁵

Per the terms of the resolution agreement BST entered into, BST agreed to:

- Conduct an accurate and thorough risk analysis to determine the potential risks and vulnerabilities to the confidentiality, integrity, and availability of its ePHI;
- Create and implement a risk management plan to address and mitigate security risks and vulnerabilities identified in its risk analysis;
- Develop and maintain written policies and procedures to comply with the HIPAA Privacy and Security Rules (and update them as needed); and
- Enhance its existing HIPAA and security training program and provide annual training for all workforce members to whom the HIPAA policies and procedures apply, including workforce members with access to PHI.⁶

The inclusion of additional steps beyond completion of a risk analysis highlights OCR's stance that entities subject to HIPAA must also take action to mitigate

those risks and vulnerabilities to ePHI that are identified in the risk analysis to ensure compliance with the HIPAA Security Rule.

REGULATED ENTITY IMPLICATIONS

The BST case provides critical insights into OCR's current enforcement philosophy.

1. *Risk Analysis Remains an Enforcement Priority Across Administrations.* The Initiative was launched under the Biden administration, and there have been a number of changes to HHS priorities and staff since the Trump administration took office. The first enforcement actions under the Initiative were handled by the Biden OCR, so it was unclear how the Trump OCR would proceed. The BST settlement continues the theme of other Initiative investigations — i.e., stakeholders should expect to see continued interest in risk analysis compliance and should treat regular risk analyses as the cornerstone of HIPAA Security Rule Compliance.
2. *OCR Expects Compliance from All Regulated Entities.* The HIPAA Security Rule was originally designed to be flexible, scalable, and technology-neutral. The aim was to allow entities to comply with Security Rule safeguards as appropriate for the entity, with differential impact based on an organization's size, needs, and sophistication. It bears stressing that BST is a public accounting, business advisory, and management consulting firm, and its status as a business associate did not exempt it from scrutiny. This settlement signals that HHS expects all HIPAA-regulated entities — from large, sophisticated providers to smaller consultants that may occasionally support the health care industry — to take risk analysis compliance requirements seriously. It will be increasingly difficult for entities to avoid regulatory enforcement with arguments that they did not have sufficient knowledge of those requirements

or resources to support compliant risk analysis efforts.

3. *Evolving Standards Demand Proactive Approaches.* While the HIPAA Security Rule currently allows for significant flexibility and scalability in implementation, the December 2024 Notice of Proposed Rulemaking to modify the HIPAA Security Rule⁷ (issued by the Biden administration) proposed new, express risk analysis requirements that, if finalized, would eliminate some of the current flexibility in conducting risk analyses. The proposed rule included specific, prescriptive risk analysis compliance requirements like a data map and technology asset inventory.
4. *Your Risk Analysis Will Be Reviewed – Make Sure It's Robust.* Regulated entities should expect HHS to request the organization's most recent risk analyses as part of any compliance assessment. Such analyses must accurately and thoroughly assess potential risks and vulnerabilities. HHS, NIST, and other well-regarded industry groups have a variety of guidance materials demonstrating the scope of an appropriate HIPAA-compliant risk analysis. Put bluntly, the ostrich approach – burying your head in the sand and acting surprised when HHS expects a fulsome risk analysis – is not going to be a successful strategy.
5. *The Real Cost of Inadequate Risk Analysis Goes Beyond Fines.* Last but not least, conducting a fulsome risk analysis that complies with the HIPAA Security Rule is not just about crossing t's and dotting i's for regulators. This settlement highlights the growth in the number and size of breaches and the marked increase of sophisticated cyberattacks using hacking and ransomware. In this context, it's imperative that organizations conduct a security risk analysis to mitigate potential harm resulting from such incidents.

RECOMMENDED STEPS FOR COMPLIANCE

Organizations subject to HIPAA should review the following practical steps to conduct a risk analysis and use the results of that risk analysis to mitigate the risks and vulnerabilities to ePHI identified.

- *Conduct a comprehensive risk analysis.* Ideally, this should include an inventory of technology assets, documentation of how ePHI moves through information systems, and identification of the locations within its information systems where ePHI may be created, received, maintained, or transmitted. If you need additional assistance with where to begin, you can start by reviewing OCR's Guidance on Risk Analysis on the HHS website. Also consider guidance from the National Institute of Standards and Technology (NIST). Only federal agencies are required to follow NIST guidelines, but because they represent the industry standard of ePHI security practices, OCR recommends them as a helpful starting place for developing compliance activities.⁸
- *Remember that there is no single approved method for conducting a risk analysis.* Formulaic approaches that lack specificity will not pass muster with OCR and are unlikely to meaningfully address risk. Note that in the proposed Security Rule, it was suggested that regulated entities perform risk analysis in a manner that conforms with guidance from NIST and CISA. Even if the Trump administration does not move forward with risk analysis-related updates like those in the proposed rule, regulated entities may consider taking steps to keep up with evolving regulatory expectations and best practices, such as:
 - Incorporating data maps, technology asset inventories, dark web scans, penetration tests, and other technical processes into their risk analysis processes
 - Using an objective methodology for categorizing threats, vulnerabilities, and the likelihood of exploitation

- Linking preparation of a gap analysis and risk mitigation plan with the risk analysis
- *Create a risk management plan that directly relates to the findings in the risk analysis.*
- *Maintain copies of your risk analysis and risk management plan.*
- *Understand that your risk analysis/risk management plans are not static.* Risk analysis and risk management plans should be updated at least annually. In the proposed Security Rule, OCR expressly noted that its expectations are that regulated entities would include the use of artificial intelligence tools in risk analyses and associated risk management activities.
- *Clarify your requirements.* Finally, if your organization is uncertain whether it is subject to HIPAA or any other privacy and security requirements, it's important to work with counsel to clarify your legal obligations and assess the quality of your compliance posture.

CONCLUSION

The BST settlement confirms that the Initiative remains a priority across administrations, and that OCR expects all regulated entities, no matter their size, to maintain robust, well-documented risk analysis programs. With more aggressive requirements potentially on the horizon, organizations cannot afford to treat risk analysis as a checkbox exercise. The stakes are too high,

both in terms of regulatory exposure and the very real threat of cyberattacks that compromise patient data. Regulated entities that treat security compliance as an ongoing commitment rather than a one-time project will be best positioned to protect both patients and their organizations from harm.

Endnotes

1. See Resolution Agreement at 2, 6, HHS OCR v. BST & Co. CPAs, LLC (2024), available at <https://www.hhs.gov/sites/default/files/hhs-ocr-bst-hipaa-settlement.pdf> (last visited Dec. 1, 2025).
2. *Id.*
3. See Press Release, HHS, HHS Office for Civil Rights Settles HIPAA Ransomware Cybersecurity Investigation for \$90,000, available at <https://web.archive.org/web/20241230230804/https://www.hhs.gov/about/news/2024/10/31/hhs-office-for-civil-rights-settles-hipaa-ransomware-cybersecurity-investigation-for-90000-dollars.html> (last visited Dec. 1, 2025).
4. See HHS OCR, 2016–2017 HIPAA Audits Industry Report, available at <https://www.hhs.gov/sites/default/files/hipaa-audits-industry-report.pdf> (last visited Dec. 1, 2025).
5. See Press Release, HHS, HHS' Office for Civil Rights Settles HIPAA Ransomware Security Rule Investigation with BST & Co. CPAs, LLP, available at <https://www.hhs.gov/press-room/hhs-ocr-bst-hipaa-settlement.html> (last visited Dec. 1, 2025).
6. See Resolution Agreement at 6–9.
7. HIPAA Security Rule to Strengthen the Cybersecurity of Electronic Protected Health Information, 90 Fed. Reg. 898 (proposed Jan. 6, 2025) (to be codified at 45 C.F.R. pts. 160, 164).
8. HHS OCR, Guidance on Risk Analysis, available at <https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html> (last visited Dec. 1, 2025).

Reprinted from Journal of Health Care Compliance, Volume 28, Number 1, January–February 2026, pages 15–18, with permission from CCH and Wolters Kluwer.
For permission to reprint, e-mail permissions@cch.com.
