Ransomware, HIPAA, and a $175K Lesson in Compliance

In August 2025, the U.S. Department of Health and Human Services (HHS) announced that its Office for Civil Rights (OCR) had resolved with BST & Co. CPAs, LLP ("BST") regarding a HIPAA Security Rule violation tied to a ransomware incident (HHS, 2025). This settlement highlights the importance of conducting a thorough HIPAA risk analysis—and the risks associated with inadequate or incomplete compliance programs.

The Incident and Findings

BST was acting as a HIPAA business associate for a covered entity, handling financial data that also included protected health information (PHI). In December 2019, BST detected a ransomware infiltration into parts of its network that impacted its covered entity client (HHS, 2025). BST reported the breach in early 2020, triggering an investigation by the OCR.

OCR's findings were clear: BST had neglected to conduct an accurate and thorough risk analysis to assess vulnerabilities to the confidentiality, integrity, and availability of its electronic PHI (ePHI). Without that foundational assessment, BST lacked the insight to implement sufficient safeguards (HHS, 2025). Due to this deficiency, BST effectively left gaping vulnerabilities unaddressed.

Terms of the Settlement and Corrective Requirements

Under the terms of the resolution agreement, BST agreed to a multi-year corrective action plan and a monetary payment of $175,000 to OCR (HHS, 2025). The corrective action plan is to be monitored for two years, and steps BST must take include:

- Conducting an accurate, comprehensive risk analysis
- Developing and implementing a risk management plan to mitigate identified risks
- Establishing, maintaining, and updating written policies and procedures to adhere to the HIPAA Privacy and Security Rules
- Enhancing its HIPAA/security training programs and ensuring annual workforce training for all staff with access to PHI (HHS, 2025)

OCR also published recommended best practices for covered entities and business associates, including:

- Locating and mapping where ePHI resides, how it enters, flows through, and exits the systems
- Periodically updating risk analyses and applying risk mitigation measures

- Ensuring audit controls and activity review mechanisms are in place
- Implementing user authentication and encrypting ePHI both in transit and at rest
- Using lessons learned from prior incidents to continually strengthen security
- Tailoring workforce HIPAA training to respective roles and responsibilities (HHS, 2025)

Takeaways for Practices and Business Associates in the Health Space

This settlement serves as a sobering reminder: a risk analysis is not just a compliance checkbox—it's the linchpin of a defensible, security-minded HIPAA program. Organizations that fail to understand where their ePHI resides, how it can be compromised, or what controls are necessary, are far more vulnerable to ransomware, breaches, and enforcement exposure.

Here are a few lessons every health provider, partner, or business associate should internalize:

1. **Risk analysis must be comprehensive and repeated to ensure accuracy.** It is not a one-and-done task. As systems, workflows, and threats change, so must your assessments.
2. **Translate findings into action.** Identifying risks without mitigating them is just an intellectual exercise. The plan to manage those risks must be concrete and enforced.
3. **Documentation is essential.** Written policies, procedures, and logs help demonstrate that your organization took compliance seriously—and can be key in an enforcement review.
4. **Workforce training tailored to roles is non-negotiable.** People are often the weakest link; role-based training prevents "one size fits all" approaches.
5. **Don't wait for a breach to test your program.** Using lessons from other incidents (internal or external) helps you proactively harden your defenses.

Final Word & Action Step

The HHS/BST settlement marks OCR's 15th ransomware enforcement and its 10th under OCR's "Risk Analysis Initiative" (HHS, 2025). If a well-resourced accounting firm with specialized expertise can fall short, so too could any practice or vendor that doesn't rigorously test its compliance program.

Is your compliance program truly robust—or are you vulnerable to the same exposure? If you aren't confident in your risk analysis, documentation, or security posture, now is the time to act. **Make sure your compliance program is not falling short. Get your free Gap Analysis from ChiroArmor today.** Visit: https://chiroarmor.com/gap/

Reference

HHS. (2025, August 18). *HHS' Office for Civil Rights settles HIPAA ransomware security rule investigation with BST & Co. CPAs, LLP*. U.S. Department of Health & Human Services. https://www.hhs.gov/press-room/hhs-ocr-bst-hipaa-settlement.html

—

Dr. Ray Foxworth, DC, FICC, is the visionary behind ChiroHealthUSA, serving as its esteemed founder and CEO. With over 39 years of dedicated service in chiropractic care, Dr. Foxworth has navigated the complexities of billing, coding, documentation, and compliance firsthand. His rich experience includes roles as the former Staff Chiropractor at the G.V. Sonny Montgomery VA Medical Center and past chairman of the Chiropractic Summit and Mississippi Department of Health.

Dr. Foxworth is deeply committed to advancing the chiropractic profession, which is evident through his leadership roles. He is an at-large board member of the Chiropractic Future Strategic Plan and holds an executive board position with the Foundation for Chiropractic Progress.