WHY SKIPPING SECURITY RISK ASSESSMENTS CAN COST MILLIONS

by Angele Tran

Angele Tran

(tran@fsainfo.org) is a Compliance Manager at Friends Services Alliance Compliance Collaborative in Blue Bell, PA.

Healthcare data breaches pose a serious threat to providers and systems, and the past few years have emphasized the growing cybersecurity challenges facing the industry.

While the percentage increase has declined over the past few years, in 2024, there was an 8.4% increase in data breaches reported to the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) from 2023 and a 9.3% increase from 2022, showing a slow, but still steady, increase year-over-year.[1]

Common targets for cyberattacks include hospitals and health systems, business associates, vendors, and partners, such as cloud storage providers and billing firms. Small to midsize providers are particularly vulnerable due to their limited cybersecurity infrastructure.

The impacts of these attacks can be catastrophic, compromising protected health information (PHI), personally identifiable information, financial and billing data, as well as clinical records and imaging. Safeguarding against these attacks becomes more challenging as ransomware attacks become more sophisticated, often targeting backup systems and exploiting vulnerabilities in third-party vendors.

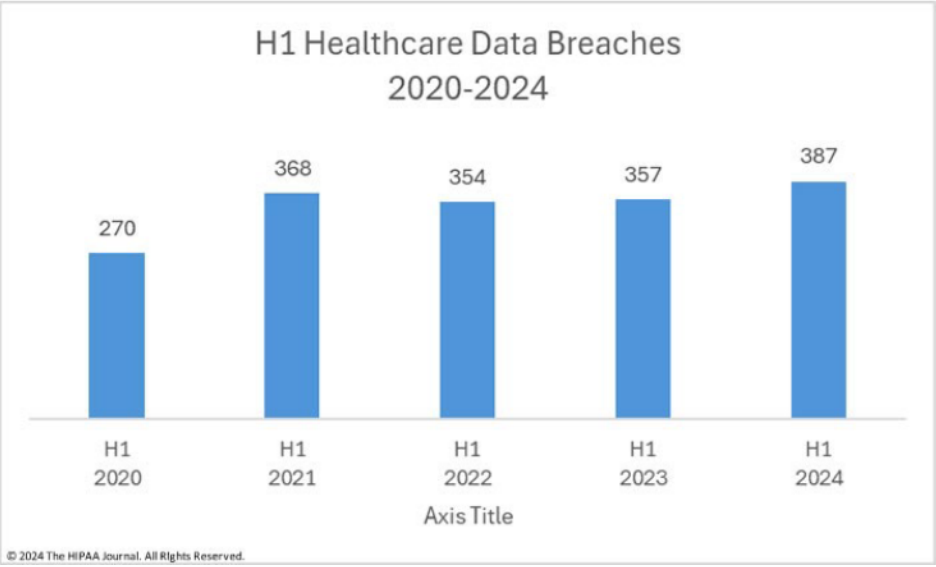
These impacts are also why Title 45 of the Code of Federal Regulations (CFR) requires certain administrative safeguards "to prevent, detect, contain, and correct security violations."[2]

Healthcare providers and their third-party vendors are required under HIPAA to perform regular risk analyses, including conducting a security risk assessment (SRA), which is the foundational step in evaluating and strengthening security practices. Although it's just one component of a comprehensive risk management strategy, the SRA lays the groundwork by identifying existing and potential vulnerabilities. After all, you can't mitigate risks unless you first know where they are.

Background on SRAs

Currently, under the HIPAA Security Rule, it is required that "covered entities and its business associates conduct a risk assessment of their healthcare organization."[3] An SRA allows healthcare providers and third-party providers to identify system

Figure 1



risk areas, informs entities on ways to prepare for cyberattacks, and builds into a larger risk management strategy.

While SRAs are not the only protection against cyberattacks, they are a healthcare organization's most important defense tactic. However, SRAs should not be considered an item to check off a to-do list but an essential part of performing annual maintenance on an IT infrastructure.

Typically, SRAs include components such as:

- Assessment of storage regarding all electronic PHI (ePHI)
- Identification of where ePHI is stored, received, maintained, or transmitted
- Documentation of any anticipated threats to ePHI unique to their entity
- Evaluation of current security measures, whether in-house or with a third-party provider
- Detailed consideration of consequences if a data breach occurs
- Identification of risk levels for threats that an entity has identified during an SRA
- Documentation of the steps of an SRA
- Determination of a process for reviewing and updating the entity's risk assessment[4]

Importantly, the HHS Office of Inspector General (OIG) considers routine risk assessments, such as SRAs, a critical component of a compliance program. Failing to conduct one may be seen as willful neglect, which could lead to civil monetary penalties if a breach occurs.[5]

Often, the challenge for organizations comes in the ambiguity of OCR's requirements. The lack of a standardized approach to confirm compliance and an absence of requirements for the timing of risk assessments can unintentionally cause the process to go by the wayside if organizations are undereducated on what risks their organization can mean or if it's not in the current budget.

OIG's approach to cybersecurity

OIG recognizes the significance of improving the HHS approach to cybersecurity and safeguarding against breaches in the healthcare system. In addressing this challenge, OIG has created a cybersecurity team that combats threats within HHS and the larger healthcare industry.[6]

In the 2024 OIG report, *Top Management & Performance Challenges Facing HHS*, improving cybersecurity was cited as one of the top five challenges for HHS. Like many healthcare entities and third-party vendors, it has been determined that "HHS must adapt as risks expand to include social engineering threats, data breaches, and increasingly sophisticated cyberattacks."[7]

This focus of attacks goes beyond the department and seeps into the industries and entities they oversee. The healthcare industry, year-over-year, has remained an area threatened by cyberattacks.

No organization is beyond the reach of OIG audits

In another 2024 report, *Review of the Department of Health and Human Services' Compliance With the Federal Information Security Modernization Act of 2014 for Fiscal Year 2024*, OIG details a performance audit of the HHS security program.[8] This report makes it clear to all healthcare organizations that no covered entity, not even a government agency, is beyond the reach of OIG audits, and each is held to the same standards of compliance and accountability.

This report was a result of HHS compliance with an annual independent evaluation of their entities' information security programs and practices to determine their effectiveness. For the second year in a row, the department was found to be "not effective," underscoring the significance of these annual audits and the changes needed from even the largest entities.

One of the independent auditor's top recommendations to HHS was to finish implementing its cybersecurity risk management strategy to identify and respond to potential risks.

All covered entities are subject to audits and enforcement actions

There are general rules and requirements that all covered entities must comply with when it comes to security standards. In addition to safeguarding the materials and integrity of all ePHI, entities are also required to be aware of and mitigate against any potential threats.

There is some flexibility in how entities implement security measures, which consider the size, complexity, technical infrastructure, costs of security measures, and other elements of the entity. But every organization is required to take reasonable and appropriate action to protect ePHI and record security measures they are taking.[9]

OCR is required under the Health Information Technology for Economic and Clinical Health Act of 2009 to conduct periodic audits of entities' compliance with HIPAA. In the current 2024–2025 HIPAA audits, 50 covered entities and business associates will be reviewed.[10]

The framework: Utilizing the SRA Tool

OIG strongly supports the requirement for healthcare organizations to conduct SRAs as part of a robust compliance and privacy/security program. Just as regular, thorough risk assessments indicate a strong compliance program, OIG would consider failing to conduct one as willful neglect.

Therefore, it's critical that healthcare organizations conduct SRAs and do them well, which for large organizations almost always includes the employment of a third-party consultant. However, the Office of the National Coordinator for Health Information Technology and OCR created an SRA Tool to help small and medium-sized healthcare organizations conduct an SRA.[11] This tool—available for download to a desktop computer—walks through the process of conducting an SRA through a self-guided approach, providing references throughout and reporting upon completion.

Utilizing a tabletop exercise

A good way to test your HIPAA security plan is to periodically conduct tabletop exercises. A tabletop exercise is a simulated scenario where key team members discuss their roles and responses during a cyber incident. Think of it as a fire drill for cybersecurity.

Benefits of a tabletop exercise include:

- Testing the organization's response plan in a low-stakes environment.
- Clarifying roles and responsibilities among clinical, IT, administrative, and compliance teams.
- Identifying delays or bottlenecks in emergency workflows.
- Reinforcing communication plans internally and with families, regulators, and vendors.

Tabletop exercises should include scenarios such as ransomware attacks and vendor-related outages. After the scenarios are played out, your team should debrief after each session and update your response plans accordingly.

The Cybersecurity and Infrastructure Security Agency provides customizable, free, and available resources to organizations looking to conduct these types of exercises.[12]

The cost of not doing an SRA

In 2024, OIG called out OCR for weaknesses in certain auditing and HIPAA enforcement actions, which signals increased focus on OCR enforcement in response to the steady rise in cyberattacks.

In the past year, OCR has centered its enforcement of ransomware security incidents on entities' failure to conduct a compliant risk analysis. The repercussions will include settlements or civil money penalties. While OCR recognizes its part in educating HIPAA-regulated entities in what marks compliant processes, it noted in its October 2024 cybersecurity conference that it will "not consider a checklist or cookie-cutter form of assessment as compliant and notes during the conference that its own security risk assessment template is just a starting point and alone is not sufficient."[13]

The following incidents involving Anthem Inc. and Premera Blue Cross offer two recent and stark insights into what happens when organizations fail to conduct SRAs and are left open to unnecessary vulnerabilities and delayed responses.

Premera Blue Cross

On March 17, 2015, Premera reported a cyberattack that began on May 5, 2014, which exposed the ePHI of over 10.4 million individuals.[14] The breach, caused by a phishing email that installed malware, went undetected for nearly nine months. A federal investigation found potential violations of HIPAA regulations, including failure to conduct a proper risk assessment, insufficient security measures, inadequate system activity monitoring, and failure to prevent unauthorized access to ePHI.

In addition to a corrective action plan, Premera was ordered to pay HHS a "resolution amount" of $6,850,000 on April 30, 2020. Notably, in its corrective action obligation, Premera is now required to conduct an accurate and thorough risk analysis, identifying risks and vulnerabilities related to ePHI.

Anthem Inc.

On February 13, 2015, HHS opened a compliance review against Anthem based on reports that Anthem had experienced a significant cyberattack. On March 13, 2015, Anthem disclosed that cyberattacks had resulted in impermissible access to the ePHI of over 78 million people.[15] HHS's investigation determined that Anthem had failed to conduct a thorough and accurate risk analysis and failed to implement sufficient procedures to regularly review records of information system activity.

In addition to a corrective action plan, Anthem was required to pay HHS $16,000,000. Anthem's corrective action requirement mirrors that of Premera in that both are obligated to carry out a comprehensive evaluation of their systems to uncover potential threats and weaknesses affecting ePHI.

No longer just best practice

While an SRA isn't the only component of a strong HIPAA compliance program, it is the foundation. You can't mitigate vulnerabilities if you haven't first identified them.

It's crucial to note that this isn't just a best practice; it's a legal requirement under HIPAA, as outlined in the CFR. Yet, despite the mandate, many healthcare organizations struggle to execute SRAs effectively. Some attempt to manage assessments in-house, and while that can be sufficient in theory, the reality is that many lack the expertise or resources to do it well and only realize this after a breach or enforcement action.

Organizations that lack internal subject matter experts should strongly consider working with a qualified third-party consultant.

It can be challenging to fit risk assessments into a budget or schedule, but failing to implement these safety measures will lead to far greater consequences if a breach occurs. To remain compliant and also be good stewards of resources, patient, and employee information, SRAs are the best first step in identifying areas of risk and building safeguards for your healthcare organization. CT

Endnotes

1. Steve Alder, "H1, 2024 Healthcare Data Breach Report," *The HIPAA Journal*, July 30, 2024, https://www.hipaajournal.com/h1-2024-healthcare-data-breach-report/.
2. 45 C.F.R. § 164.308(a)(1)(i).
3. Assistant Secretary for Technology Policy, "Security Risk Assessment Tool," accessed June 4, 2025, https://www.healthit.gov/topic/privacy-security-and-hipaa/security-risk-assessment-tool.
4. U.S. Department of Health and Human Services, Office for Civil Rights, "Guidance on Risk Analysis," content last reviewed July 22, 2019, https://www.hhs.gov/hipaa/for-professionals/security/guidance/guidance-risk-analysis/index.html.
5. 45 C.F.R. Part 164, https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164?toc=1
6. U.S. Department of Health and Human Services, Office of Inspector General, "Cybersecurity," video, last updated October 10, 2024, https://oig.hhs.gov/reports/featured/cybersecurity/.
7. U.S. Department of Health and Human Services, Office of Inspector General, *Top Management & Performance Challenges Facing HHS 2024*, https://oig.hhs.gov/documents/tmc/10057/2024%20Top%20Management%20and%20Performance%20Challenges%20Facing%20HHS.pdf.
8. U.S. Department of Health and Human Services, Office of Inspector General, "Review of the Department of Health and Human Services' Compliance with Federal Information Security Modernization Act of 2014 for Fiscal Year 2024, Report number: A-18-24-11200, issued November 15, 2024, https://oig.hhs.gov/reports/all/2024/review-of-the-department-of-health-and-human-services-compliance-with-the-federal-information-security-modernization-act-of-2014-for-fiscal-year-2024/#:~:text=Overall%2C%20through%20the%20evaluation%20of,program%20rating%20from%20FY%202023.
9. 45 C.F.R. § 164.306, https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.306
10. U.S. Department of Health and Human Services, Office for Civil Rights, "OCR's HIPAA Audit Program," content last reviewed December 31, 2024, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/audit/index.html.
11. Assistant Secretary for Technology Policy, "Security Risk Assessment Tool."
12. Cybersecurity & Infrastructure Security Agency, "CISA Tabletop Exercise Packages," accessed June 4, 2025, https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages.
13. Beth Neal Pitman, Shannon Britton Hartsfield, and Julia Hesse, "HIPAA Tidings: A Look at OCR's Recent Enforcement Actions," Holland & Knight, December 3, 2024, https://www.hklaw.com/en/insights/publications/2024/12/hipaa-tidings-a-look-at-ocrs-recent-enforcement-actions?utm_source=chatgpt.com.
14. U.S. Department of Health and Human Services, Office for Civil Rights, "Health Insurer Pays $6.85 Million to Settle Data Breach Affecting Over 10.4 Million People," content last reviewed September 25, 2020, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/premera/index.html.
15. U.S. Department of Health and Human Services, Office for Civil Rights, "Anthem pays OCR $16 Million in record HIPAA settlement following largest health data breach in history – October 15, 2018," content last reviewed October 15, 2018, https://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/anthem/index.html.

Takeaways

- A security risk assessment (SRA) is a critical first step in any healthcare organization's broader cybersecurity and risk management strategy.
- While SRAs require time and resources, high-profile breaches at organizations like Anthem and Premera demonstrate the far greater cost of neglecting them.
- Failing to conduct a compliant risk analysis remains the leading cause of healthcare data breaches.
- To support small and mid-sized organizations, the Office of the National Coordinator for Health Information Technology and the U.S. Department of Health and Human Services Office for Civil Rights developed a free HIPAA Security Risk Assessment Tool tailored to their needs.
- Many organizations struggle with confusing regulatory guidance, making it easy for risk assessments to fall through the cracks.