STRATEGIC MANAGEMENT SERVICES

HIPAA Compliance in 2025: Key Survey Findings and Risk Mitigation Strategies

Richard P. Kusserow | February 2025

In 2024, near-record levels of fines for HIPAA violations underscored the ongoing compliance challenges faced by healthcare organizations. Findings from the 4th National HIPAA Compliance Survey, conducted by SAI360 in collaboration with Strategic Management Services, reveal that many organizations continue to face challenges with key HIPAA compliance areas, increasing their exposure to regulatory scrutiny and enforcement.

The survey provides a comprehensive assessment of how healthcare organizations are managing HIPAA compliance and identifies critical areas of risk. The results indicate gaps in compliance readiness, with less than half of all respondents selecting "very confident" when asked about their organization's ability to meet HIPAA regulatory requirements and fewer than 40% selecting "very prepared" when asked about their readiness for a HIPAA audit or Office of Civil Rights (OCR) investigation.

To further examine these findings, Strategic Management Services, in partnership with SAI360, hosted a webinar on January 23, 2025, featuring Robbi-Lynn Watnik and Natalie Lesnick. The webinar explored key vulnerabilities in HIPAA compliance identified in the survey; the areas organizations consider most critical for maintaining compliance in 2025; and strategic recommendations to mitigate these risks and improve compliance readiness.

Key Survey Insights: Identifying the Most Pressing Compliance Challenges

The survey gathered responses from more than 227 healthcare organizations to assess how HIPAA programs are structured and where organizations face the greatest challenges.

When asked about their top HIPAA compliance priorities for 2025, leaders identified:

- Incident response and reporting (54%)
- Reducing inappropriate/inadvertent disclosure of protected health information (PHI) by workforce (50%)
- Monitoring inappropriate access to PHI/snooping by workforce (45%)
- Breach notification management (40%)

- Monitoring business associate agreements and activity (38%)

While these responses represent diverse aspects of HIPAA compliance, they also point to four overarching challenges for healthcare organizations:

1. Development and adequacy of policies and procedures;
2. Workforce access to HIPAA policies and critical information;
3. Training and education on HIPAA requirements and monitoring of electronic health records access; and
4. Oversight and compliance management of business associates.

To address these risks, Mrs. Watnik and Ms. Lesnick shared key recommendations that organizations should consider implementing to improve their HIPAA compliance posture in 2025.

Mitigating Identified HIPAA Compliance Risks

1. **Strengthening Policies and Procedures**

The survey revealed that more than 50% of organizations have 16 or fewer HIPAA-related policies, raising concerns about whether these policies fully address regulatory requirements, particularly with 40% of organizations identifying breach notification management as a key priority for 2025. Additionally, the survey revealed that some organizations (e.g., smaller entities) attempt to consolidate multiple compliance topics into single policies for efficiency; however, this can lead to ambiguity, confusion, and gaps in compliance coverage.

To strengthen HIPAA compliance policies, organizations should:

- Ensure policies are specific, comprehensive, and aligned with regulatory best practices;
- Develop a clear breach notification policy that outlines reporting obligations and employee responsibilities;
- Regularly review and update policies to reflect changes in regulations; and
- Ensure policies are written in clear, actionable language that minimizes misinterpretation.

2. **Improving Workforce Access to HIPAA Policies**

Another central issue identified in the survey and discussed in the webinar was workforce accessibility to HIPAA policies and procedures. While 58% of organizations reportedly store HIPAA policies and procedures on an internal platform, such as a company intranet, many lack mechanisms to ensure that employees can easily access policies and remain informed of critical updates. Without proper access to HIPAA policies and critical updates, employees may inadvertently fail to follow established HIPAA privacy and security protocols, increasing the risk of noncompliance.

To strengthen workforce accessibility to HIPAA policies, organizations should consider:

- Establishing internal communication channels (e.g., newsletter, email correspondence) to alert employees to newly developed policies or critical updates to existing ones; and
- Incorporating key policies into training and education materials to reinforce HIPAA regulatory expectations and requirements.

3. **Enhancing Workforce Training and Monitoring to Reduce PHI Violations**

Workforce training and monitoring emerged as a significant finding in the survey, particularly in relation to preventing unauthorized access and disclosure of PHI. The survey found that 50% of organizations identified inappropriate or inadvertent disclosure of PHI by employees as a major compliance concern, while 45% reported concerns related to workforce snooping or unauthorized access to PHI. These findings suggest potential gaps in employee awareness and training on HIPAA security protocols and monitoring of HER access. Organizations can address these risks by:

- Providing scenario-based HIPAA training to reinforce PHI handling and security protocols;
- Implementing role-specific compliance training, ensuring employees understand HIPAA requirements relevant to their duties; and
- Deploying real-time PHI access monitoring to detect and prevent unauthorized data access.

4. **Strengthening Business Associate Oversight**

A final critical challenge identified in the survey was challenges in effective oversight of business associates. The survey revealed that 55% of organizations do not require HIPAA training for business associates, increasing exposure risks, as third-party vendors who lack HIPAA training may mishandle PHI, fail to follow security protocols, or introduce compliance vulnerabilities.

To improve business associate compliance, organizations should:

- Require all business associates to complete HIPAA training as part of contract agreements.
- Clearly define business associate responsibilities for PHI security, access controls, and breach notification.

For additional insights from this discussion, access the full webinar recording here. For more information on this topic contact Robbi-Lynn Watnik at rwatnik@strategicm.com or Natalie Lesnick at nlesnick@strategicm.com.

About the Author

Richard P. Kusserow established Strategic Management Services, LLC, after retiring from being the DHHS Inspector General, and has assisted over 2,000 health care organizations and entities in developing, implementing and assessing compliance programs.