CASE STUDY: BENEFITS OF A HIPAA GAP ASSESSMENT

Situation

With the Office of Civil Rights (OCR) promising to increase Health Insurance Portability and Accountability Act (HIPAA) audits of covered entities (CEs), organizations have a pressing need to evaluate their compliance and remediate gaps. OCR is tasked with enforcing HIPAA, and their current audit list may include any CE or business associate (BA). Penalties for noncompliance can include massive fines or even criminal charges.

To avoid these penalties and prepare for an audit, organizations need a clear picture of their current state of compliance. RSM was recently approached by an organization that knew there were gaps in its compliance program but was struggling to determine the right course of action to remediate this risk. To meet this need, we performed a HIPAA gap assessment to identify missing controls and develop a prioritized approach to achieving and maintaining compliance.

Solution

RSM's HIPAA gap assessment evaluated the organization against HIPAA's security and privacy standards. For this client, the process involved interviewing key individuals, reviewing documentation and supplementing these reviews with vulnerability and penetration testing. This provided detailed insight into whether the organization's programs, policies, procedures and controls were supporting or undermining efforts to achieve HIPAA compliance.

RSM determined the organization to be only 51 percent compliant with relevant HIPAA regulations. Because implementing the significant number of missing controls can be a daunting task for any organization, a prioritized approach was needed. Instead of simply identifying control gaps, we developed a workable strategy for achieving and maintaining compliance, along with expected costs for implementing the plan.

Performing the HIPAA gap assessment highlighted both compliance shortfalls and also security gaps. The organization lacked several basic information security practices, which contributed to their struggles in achieving compliance. To move the organization toward compliance and improved security, we developed the following program-level goals and a detailed three-year road map.

Program-level goals:

- Information security program: A formal information security program helps build a culture where security is a core value of the organization. As part of the program, policies and procedures should define how the organization protects sensitive data. Regular training should reinforce employees' responsibilities in protecting this data.
- Risk management: The organization needed to implement a formal risk management program that could incorporate processes for determining what could cause significant harm to the organization in the event of a breach.
- Vulnerability management: To properly secure the network, the organization needed a strong vulnerability management program. This would entail processes for developing secure baselines, hardening devices, patching systems, monitoring systems and testing the network.
- Compliance: Compliance with the HIPAA rules would require coordination among several business units. The organization needed to assign an owner to the compliance program to establish accountability and effective management of compliance initiatives.

Three-year road map

To meet these program-level goals, we also created a three-year road map with yearly milestones. This way, the organization could demonstrate progress in reaching compliance and security objectives.

Year one: During year one, the focus was to establish a foundational security program and develop a compliance strategy. This strategy involved tasks such as technical hardening, establishing incident response procedures, formalizing policies and implementing a security steering committee to provide ongoing oversight and guidance.

Year two: Year two's focus was to enhance and maintain the security program through ongoing governance, training, testing and remediation. This consisted of enhancements to security awareness training, vulnerability management and security controls testing.

Year three: Year three's milestones including addressing risks and vulnerabilities through optimization of current programs. This involved maturing the risk management program, automating incident response procedures and improving application security.

Results

The HIPAA gap assessment was the first step in helping this organization build a defensible security program and reduce the risks associated with noncompliance. By providing insight into HIPAA requirements, the organization was better prepared to implement these requirements. The HIPAA gap assessment established the client's current state of compliance, allowing RSM to develop a road map that prioritized both tactical and strategic actions to remediate gaps in the most efficient way possible.

Additionally, the HIPAA gap assessment gave the organization a sense of how an OCR audit might occur and what evidence and documentation the auditor might request, should the situation arise. Moreover, the HIPAA gap assessment provided the impetus the organization needed for finally prioritizing security. If organizations recognize how compliance and security initiatives can complement one another, they can build a cost-effective, sustainable program for fulfilling both responsibilities.

+1 800 274 3978
rsmus.com