HealthManagement
Promoting Management and Leadership

Strengthening Healthcare Data Security: Managing Vendor Risks

As healthcare organisations increasingly depend on third-party vendors for crucial services—ranging from Electronic Health Records (EHR) software to medical device manufacturers—they also open themselves up to substantial cybersecurity risks. Over recent years, some of the largest data breaches in healthcare have stemmed from vulnerabilities within third-party vendors. One striking example is the 2024 breach of Change Healthcare, which affected many hospitals that didn't even realise their systems were compromised. With the rising sophistication of cyberattacks and the post-pandemic surge in digital healthcare investments, the need for proactive vendor risk management has never been more critical.

Growing Investments, Growing Risks

The healthcare sector is navigating two converging trends exacerbating the need for heightened vendor oversight. First, post-pandemic investments in digital health have soared, with venture capital pouring into areas such as telemedicine, digital health platforms, and health equity initiatives. In 2021, funding for U.S.-based digital health startups reached an unprecedented $29.1 billion. While these investments promise innovation and enhanced patient care, they also introduce new risk vectors. Many vendors, from wearables manufacturers to telemedicine platforms, require access to sensitive health data, increasing the potential for breaches.

Second, the threat from cybercriminals has grown more severe. Healthcare is one of the most targeted industries for cyberattacks due to its wealth of personal data. Attackers are becoming more adept at exploiting vendor network software vulnerabilities to access healthcare systems. With the advent of AI-driven tools, these attacks are faster, more sophisticated, and more complex to detect, creating a perfect storm for healthcare organisations unprepared for managing vendor-related risks.

Managing Vendor Risk: More Than Just Agreements

Many healthcare organisations assume a Business Associate Agreement (BAA) is sufficient to address vendor-related risks. However, a BAA alone is not enough to prevent or mitigate the consequences of a data breach. Often, the responsibility for vendor vetting is placed on a compliance officer who may only ensure that the BAA is signed without a comprehensive assessment of the vendor's security measures. IT departments must be involved in assessing the full extent of potential risks vendors introduce, from their network access points to their security protocols.

Healthcare organisations should adopt the same rigorous approach that insurers take, scanning vendors' networks and verifying their security measures before finalising contracts. Organisations can protect themselves from third-party vulnerabilities only through comprehensive evaluations, such as external network scans and security attestations. This scrutiny ensures that vendors are not just compliant on paper but are actively taking measures to protect the sensitive data they handle.

Contracting: The Critical Stage for Negotiating Liability

Addressing vendor-related risk doesn't stop at the technical level; it extends into the contracting phase. Too often, healthcare groups find themselves negotiating liability only after a breach has occurred. The average cost of a healthcare data breach, estimated at $10.1 million, means that even a minor lapse in vendor security can have devastating financial consequences. Thus, healthcare organisations must ensure that vendors carry adequate insurance and demonstrate robust security measures, such as antivirus protection and formal password policies.

Furthermore, contracts must clearly outline the liability division in case of a breach, specifying whose forensics will be used and how costs will be divided. Equally important is transparency about how vendors will use any patient data they access. Whether for research or operational purposes, healthcare organisations must ensure that any data use is properly disclosed and compliant with frameworks like SOC 2. This step is vital not only for protecting the organisation legally but also for maintaining trust with patients and regulatory bodies.

Continuous Vigilance: The Key to Long-Term Security

Even after contracts are signed and vendors are onboarded, managing vendor risk is far from over. In a rapidly evolving tech landscape, where new software and vendors are constantly introduced, healthcare organisations must remain vigilant. Regular audits, security patches, and compliance reporting are essential to maintaining data security over time. Longstanding vendors should not be excluded from this scrutiny, as they are equally vulnerable to cyberattacks.

Healthcare organisations should also consider adopting more advanced vendor management tools beyond the traditional BAA and Excel spreadsheet models. These tools can track vendor access points, security measures, and vulnerability flags in real time, allowing for more proactive risk management. In some cases, partnering with a cybersecurity vendor that offers round-the-clock monitoring and comprehensive assessments of all third-party relationships may be the best way to ensure long-term protection against data breaches.

In an era of digital healthcare expansion and increasing cyber threats, healthcare organisations must proactively manage vendor-related risks. The days of relying solely on Business Associate Agreements are over. Instead, organisations must thoroughly vet their vendors, negotiate liability upfront, and maintain continuous vigilance over their security protocols. By adopting more advanced risk management practices and technologies, healthcare organisations can better protect patient data and their own operational integrity in an increasingly interconnected world.

Source: HealthCareIT Today

Image Credit: iStock

Published on : Wed, 2 Oct 2024