# Integrating vendor management into cybersecurity strategies for healthcare



In a landscape where cyber threats increasingly target healthcare systems, the integration of vendor management into cybersecurity strategies is gaining critical importance, according to experts in the field. Speaking to HealthTech Magazine, cybersecurity specialist Rappl underscored the necessity for healthcare organisations to include third-party vendor management in their comprehensive cybersecurity protocols. She emphasised that while leveraging external vendor services is essential for growth, it also heightens the risk profile of these organisations due to a dependency on the vendors to safeguard sensitive data.

“You’re expanding your risk footprint because you’re relying on third-party services to protect your data,” Rappl stated, highlighting the need for robust independent audits of vendor processes. She further advocated for a thorough understanding of vendors’ application development processes, data storage protocols, and protective measures for the data they handle.

In conjunction with vendor management, the importance of usability when modernising health IT systems has also come to the fore. Stone, another expert in the field, pointed out that while creating highly secure applications is essential, they must also be user-friendly. “You can create the most secure application, but if it’s highly unusable, then people will find ways to circumvent the controls.” He added that overly complex password requirements can often hinder compliance rather than enhance it, particularly in a high-pressure healthcare environment.

Chaughtai shared insights from a recent experience with a healthcare organisation that successfully adopted a modern platform. This transition followed the discovery that their outdated legacy system was unwittingly exposing data. The rigid infrastructure of the old system made timely updates challenging, emphasising the pressing need for modernisation. Through the implementation of a more flexible “plug and play” model, the organisation has reportedly improved its security measures by gaining enhanced visibility and compliance. This upgrade allows IT teams to efficiently track data access in the event of a breach.

In addition to application usability and vendor management, building resilient architecture is essential to ensure rapid recovery following an attack. Stone referenced advancements such as Pure Storage’s SafeMode Snapshots, which are designed to create non-deletable copies of critical datasets, thereby providing a safety net against cybercriminals.

The ongoing evolution of cybercrime tactics means that healthcare organisations must remain vigilant. Chaughtai noted that employing application modernisation strategies alongside cybersecurity measures yields significant long-term benefits. “We need to consider the cost of data breaches holistically,” he remarked. This includes financial repercussions, the potential for diminished productivity, and perhaps most critically, the erosion of patient trust—a consequence that can have enduring implications.

As healthcare continues to digitise and embrace modern technological solutions, the interplay between cybersecurity and system usability will be pivotal in safeguarding data while supporting healthcare providers in their critical tasks.

Source: [Noah Wire Services](https://www.noahwire.com)

## Bibliography

1. <https://www.bitsight.com/blog/automating-healthcare-vendor-risk-management> - Corroborates the importance of vendor risk management in healthcare, highlighting the risks associated with third-party vendors and the need for continuous monitoring and robust security measures.
2. <https://www.upguard.com/blog/vrm-guide-for-healthcare> - Supports the necessity of a comprehensive vendor risk management program in healthcare, including ensuring vendor compliance with regulatory standards and managing ongoing vendor relationships.
3. <https://blog.charlesit.com/vendor-management-in-healthcare-navigating-security-risks> - Emphasizes the critical role of vendor management in protecting healthcare data, including the development of vendor management programs and the assessment of vendors' cybersecurity practices.
4. <https://www.bitsight.com/blog/automating-healthcare-vendor-risk-management> - Highlights the financial and operational impacts of data breaches in healthcare, including the cost and the importance of collaborative risk mitigation with vendors.
5. <https://www.upguard.com/blog/vrm-guide-for-healthcare> - Details the benefits of a robust vendor risk management program, such as streamlined vendor procurement, enhanced due diligence, and improved regulatory compliance.
6. <https://blog.charlesit.com/vendor-management-in-healthcare-navigating-security-risks> - Discusses the best practices for managing vendor security risks, including the importance of clear policies and procedures for vendor selection and ongoing management.
7. <https://www.bitsight.com/blog/automating-healthcare-vendor-risk-management> - Explains the need for continuous monitoring of vendors' security posture and the use of tools to notify security teams of potential risks.
8. <https://www.upguard.com/blog/vrm-guide-for-healthcare> - Outlines the importance of tiering vendors based on the level of risk they present and collaborating with vendors to develop incident response plans.
9. <https://blog.charlesit.com/vendor-management-in-healthcare-navigating-security-risks> - Highlights the high volume of breaches in the healthcare sector attributed to third-party vendors and the need for modern, flexible IT systems to enhance security.
10. <https://www.bitsight.com/blog/automating-healthcare-vendor-risk-management> - Mentions the regulatory requirements, such as HIPAA and HITECH, that mandate robust healthcare vendor risk management programs.
11. <https://news.google.com/rss/articles/CBMiuAFBVV95cUxNdU9jQzJXdXVnaVd2akdpRE1idVdoaWtDcmhZZ1FoSGxhN1FZd1RPS1lQbXpfLU9RSUlsVHh1X1dORFZkQUVZZTk4bUZmWktMalZSNTd4a2N0aW5RakQyejZFNXdrV1k2SFpycmxYaWUxZVFLYnlQX1h1a2JwcHppUVJzRTVkMlhhMjBLWWVoSFpldFJLcjNaWHh1a2lESnI5WXZMMkVUXzNBd3NmQmY0aEJUN1JibDht?oc=5&hl=en-US&gl=US&ceid=US:en> - Please view link - unable to able to access data