

riskonnect

ARTICLE

Vendor Risk Is Patient Risk: Four Regulatory Changes Raising the Stakes for Healthcare Organizations

Healthcare organizations face growing pressure to prove they understand and control their third-party risk. All recently proposed or enacted, the HIPAA Security Rule Notice of Proposed Rulemaking, HHS Healthcare Sector Cybersecurity Performance Goals, the Health Care Cybersecurity and Resiliency Act or S.3315, and evolving CMS Conditions of Participation reflect growing concern about the impact third-party cyber incidents can have on healthcare organizations.

Business associates and other third parties process claims, manage electronic health records, host critical applications, and store protected health information. Many also support essential functions, from pharmacy operations to connected medical devices. These relationships create opportunities to improve care, but they also introduce new vulnerabilities.

Together, these developments are changing expectations for how healthcare organizations identify and monitor vendor risk across the entire lifecycle.

Four Federal Drivers Raising the Standard for Third-Party Oversight

Four federal developments now shape how healthcare organizations approach cybersecurity and third-party risk. While each takes a different approach, they show a broader shift in how federal agencies view healthcare organizations' responsibility for the vendors and business associates that support patient care.

HIPAA Security Rule NPRM

The proposed updates to the HIPAA Security Rule would strengthen cybersecurity requirements for covered entities and business associates while also emphasizing ongoing risk management. The NPRM would require organizations to implement safeguards such as multifactor authentication and encryption. It would also require covered entities to verify in writing that business associates have implemented the security safeguards required under HIPAA.

The written verification requirement raises the bar for vendor oversight. A business associate agreement establishes the responsibilities of each party, but the rule now places more weight on demonstrating that those responsibilities are being met. For healthcare organizations, that means maintaining documentation that shows how vendor safeguards were evaluated and verified over time.

> **Key Takeaway:** The rule shifts vendor oversight toward documented, ongoing verification – rather than relying on contractual commitments or periodic assessments alone.



HHS Healthcare Sector Cybersecurity Performance Goals

HHS introduced the Healthcare Sector Cybersecurity Performance Goals to give healthcare organizations a baseline for strengthening their defenses against common cyber threats. These voluntary goals address areas like multifactor authentication, asset inventory, incident response, and vendor risk management.

Although the CPGs are not regulatory requirements, they provide benchmarks and prioritization for cybersecurity practices. The goals also recognize that an organization's security depends on the third parties it works with.

For healthcare organizations, the CPGs offer a framework for evaluating whether their existing vendor oversight addresses the risks that matter most. They also provide a reference point for bolstering practices before more formal requirements are created.

> **Key Takeaway:** Voluntary guidance can still influence what regulators consider reasonable safeguards. That makes the CPGs a useful benchmark for strengthening third-party cybersecurity practices today.

Health Care Cybersecurity and Resiliency Act or S.3315

The Health Care Cybersecurity and Resiliency Act would establish minimum cybersecurity requirements for covered entities and business associates, including measures such as multifactor authentication, encryption, and penetration testing. It also proposes expanded Safe Harbor protections for organizations that can demonstrate at least 12 months of recognized cybersecurity practices.

The proposal rewards organizations that can demonstrate mature cybersecurity practices over time. For third-party risk programs, that creates a stronger case for maintaining a continuous record of vendor assessments, safeguard verification, remediation, and other oversight activities.

> **Key Takeaway:** The proposed legislation makes documented cybersecurity practices more valuable. Organizations would need evidence showing how they managed risks and maintained safeguards over time.

CMS Conditions of Participation

Cybersecurity expectations are also moving into the operational requirements healthcare organizations must meet to participate in Medicare and Medicaid. CMS has proposed strengthening security risk management expectations for hospitals, including greater attention to the risks created by third-party relationships.

That connection matters because many of the systems that support patient care sit outside the organization's direct control. With that in mind, a security risk management program needs to account for the vendors and dependencies that could interrupt care.

Cybersecurity tying more closely to Conditions of Participation further forces healthcare organizations to treat vendor oversight as part of maintaining safe, resilient operations.

> **Key Takeaway:** Cybersecurity and third-party risk are increasingly connected to the ability to maintain healthcare operations and participate in federal healthcare programs, making vendor oversight an operational and governance responsibility alongside an IT concern.

How Do Vendor Cyber Incidents Affect Patient Care?

The growing emphasis on continuous third-party oversight stresses the reality that cyber incidents involving vendors now have immediate consequences for healthcare delivery.

A recent example is the ransomware attack on revenue cycle management vendor Unlimited Technology Systems, which affected approximately 3.8 million patients. The vendor provides billing and revenue cycle services for thousands of healthcare providers, meaning many of the affected patients had never interacted with the company directly. Yet the breach exposed sensitive information including Social Security numbers, medical records, diagnosis and treatment details, and scanned insurance cards.

This incident is part of a broader pattern. According to MedCity News, vendors that process claims, billing, and medical records accounted for six of the 10 largest healthcare breaches reported in 2026.

The consequences also extend beyond compromised data. Recent attacks affecting organizations such as Change Healthcare, Conduent, Ascension, and PIH Health demonstrated how quickly disruptions can spread across the healthcare ecosystem. Claims processing stalled, pharmacies experienced delays, clinical workflows were interrupted, and providers were forced to activate contingency plans to continue delivering care. What began as cybersecurity incidents quickly became operational crises affecting patients and clinicians.

Research reinforces the connection between cybersecurity incidents and patient care. Hacking and other IT incidents account for the overwhelming majority of large healthcare breaches, while business associates continue to play an increasingly prominent role in those events. Among healthcare organizations whose patient care was disrupted by a cyberattack, nearly one-third reported increases in patient mortality rates. Those serious outcomes put the implications of vendor risk into perspective.



Five Steps to Build a More Resilient Approach to Third-Party Oversight

Healthcare organizations can strengthen their third-party oversight by focusing on five main areas. This approach creates greater visibility into vendor risk, as well as a stronger record of how those risks are managed.

1. **Identify and tier critical vendors.** Organizations can prioritize business associates and downstream vendors based on factors such as their impact on patient care, operational continuity, regulatory requirements, and concentration risk. This helps focus resources on relationships where a disruption could have the greatest consequences.

2. **Monitor vendors continuously.** Vendor risk can change significantly between annual assessments. Continuous monitoring helps teams identify changes in vendor risk and respond before annual reviews expose the problem. Extending oversight across onboarding, ongoing monitoring, and offboarding also creates a more complete picture of the vendor relationship.

3. **Maintain documented evidence.** Written verification can demonstrate how vendor risks were evaluated and addressed over time. Keeping that evidence accessible and organized also makes it easier to respond to an OCR investigation, CMS review, or other inquiry.

4. **Connect risk signals across the organization.** Cybersecurity findings provide only one view of vendor risk. Financial health, fourth-party dependencies, resilience, compliance, incident activity, and patient safety can all affect the potential impact of a vendor. Connecting these signals within a shared vendor profile creates a more complete view of exposure and helps teams identify issues that might otherwise remain disconnected.

5. **Establish cross-functional governance.** Compliance, enterprise risk, business continuity, resilience, and clinical teams may all have a role in assessing the potential impact of a critical vendor. A shared risk register and coordinated response process can give these teams a common view of vendor risk and clearer accountability when issues emerge.

Vendors aren't just a compliance concern anymore. They're part of the healthcare delivery chain. When a critical vendor experiences a cyber incident, the consequences can reach patients, clinicians, and operations almost immediately. Healthcare organizations that build continuous, evidence-based oversight programs will be better prepared for regulatory scrutiny and better positioned to protect patient care.

For more information on third-party risk management, read our ebook, Rethinking Supply Chain Risk Management: A Practical Guide to Better Assurance, and download our Reduce Third-Party Exposures toolkit.

Start anywhere. Expand everywhere.

Riskonnect is the leading provider of software that brings risk under one roof. The technology empowers organisations to anticipate, manage, and respond in real time to strategic and operational risks across the extended enterprise.

More than 2,700 customers across six continents partner with Riskonnect to gain previously unattainable insights that deliver better business outcomes. Riskonnect has more than 1,500 risk management experts in the Americas, Europe, and Asia-Pacific.
To learn more, visit riskonnect.com.

INSURABLE RISK | GOVERNANCE, RISK & COMPLIANCE | BUSINESS CONTINUITY & RESILIENCE

CONNECT NOW

riskonnect.

Copyright © 2026 Riskonnect, Inc.
All rights reserved.

09.26