PYA 2025 Summer CPE Symposium, Session 2 – Third-Party Risk Management

Presented June 18, 2025 by PYA's Lori Foley | Part of the PYA 2025 Summer CPE Symposium Webinar Series

https://www.pyapc.com/insights/summer-symposium-session-2-third-party-risk-management/

Please note, this transcript was generated automatically. PYA cannot guarantee its accuracy or completeness.

WEBINAR SUMMARY

This session provided a strategic overview of third-party risk management (TPRM) in healthcare, emphasizing the need for comprehensive frameworks to assess, monitor, and offboard vendors across the lifecycle of a relationship. It highlighted real-world data breaches and presented best practices for mitigating cybersecurity, compliance, and reputational risks.

Key topics include:

- Importance of TPRM in healthcare
- Brief overview of recent incidents or regulatory focus areas
- Definition and types of third parties (e.g., IT vendors, medical device manufacturers, outsourced service providers)
- Regulatory and compliance requirements pertaining to third-party vendors (e.g., BAAs, HIPAA, FDA)
- Core elements of a TPRM program lifecycle (inventory, risk assessment, due diligence, contracting, and ongoing monitoring)
- Coordination of parties in identification and mitigation of risks (e.g., internal audit, compliance, legal, quality, risk management, IT)

WEBINAR HIGHLIGHTS AND FREQUENTLY ASKED QUESTIONS

What is third-party risk management (TPRM)?

- A process for assessing and mitigating risk across the entire vendor lifecycle, from onboarding to offboarding.

Why is TPRM crucial in healthcare today?

- Due to growing cybersecurity threats, regulatory scrutiny, and operational reliance on external vendors.

What are best practices for managing third-party risk?

- Establishing a centralized or hybrid TPRM program, continuous monitoring, issue logging, stakeholder coordination, and regular audits.

How should organizations handle offshoring risks?

- By understanding legal boundaries, ensuring adequate oversight, and accounting for geopolitical and data security challenges.

What role does leadership play in TPRM?

- Executive and board engagement is essential to prioritize risk, ensure accountability, and align oversight with ERM strategies.

ACTION ITEMS

- Establish a multi-disciplinary TPRM committee to oversee third-party relationships.
- Review and update TPRM policies and procedures at least annually to ensure alignment with regulatory changes and operational needs.
- Maintain a centralized log of issues identified with third-party vendors, including remediation plans and responsible parties.
- Provide training and communication to all personnel involved in managing third-party relationships to ensure they understand their roles and responsibilities.

WEBINAR OUTLINE

Introduction to TPRM

- Lori Foley introduces herself and her role at PYA, emphasizing the importance of compliance in healthcare.
- Lori explains that TPRM touches everyone's job in the organization and aims to provide attendees with talking points and perspectives.
- She states the session will cover the big picture of TPRM, including data breaches, supply disruptions, and increased scrutiny on protected health information (PHI).
- Lori highlights that cybersecurity and breaches are the top risks keeping healthcare professionals up at night, especially in the wake of COVID-19.

Overview of TPRM

- Lori discusses the holistic approach to TPRM, which includes governance, risk management, and compliance (GRC) across the entire life cycle of third-party relationships.
- She details the life cycle includes onboarding, ongoing monitoring, and offboarding, with a focus on integrating these processes into the organization's operations.
- Lori explains that economic uncertainty and the rising price of healthcare data are driving organizations to rely more on third parties for cost reduction and operational maintenance.
- She notes the increased use of third parties leads to more government scrutiny, including updates to HIPAA rules and increased focus on cybersecurity and ransomware.

Learning Objectives and Recent Incidents

- Lori outlines the learning objectives for the session, including reviewing recent incidents, regulatory focus areas, and defining categories of third-parties.
- Lori discusses the importance of understanding compliance and regulatory requirements for third-party vendors.
- She states the session will explore core elements of a TPRM program and recommendations for appropriate oversight and board-level reporting.
- Lori provides examples of significant data breaches and incidents in 2024, including the Change Healthcare scenario and the Healthicity platform incident.

Types of Third-Party Vendors

- Lori lists various types of third-party vendors, including medical device manufacturers, billing companies, website developers, and consultants.
- Lori explains that third-party vendors are anyone outside the organization who interacts with it through devices, equipment, or information services.
- She emphasizes the importance of managing third-party relationships to mitigate risk is emphasized, with a focus on the five elements of the TPRM life cycle: onboarding, monitoring, and offboarding.

Onboarding and Due Diligence

- Lori discusses the onboarding process, including due diligence and contract setup, and the importance of having a strong inventory of third-party relationships.
- She explains the onboarding process should include a framework for assessing third-party risk, such as questionnaires and scoring systems.
- Lori emphasizes the need for a centralized inventory of all third-party relationships, including key information about the relationships, access, and vulnerabilities.
- She details importance of due diligence in evaluating vendors, including their history of data privacy breaches, security ratings, and compliance with regulations.

Monitoring and Offboarding

- Lori explains the monitoring phase, which includes risk assessment, evaluating performance, and ensuring compliance with contractual requirements.
- She notes offboarding process is crucial for managing the exit of third-party relationships, including shutting down access and ensuring all deliverables are met.
- Lori discusses the importance of having a mature TPRM program that integrates risk intelligence and regulatory insights into daily decision-making.
- She explains this session will cover the impact of third-party breaches on healthcare, including the frequency and severity of data breaches and the resulting regulatory scrutiny.

Offshoring and Its Risks

- Lori discusses the concept of offshoring, which involves utilizing human or technology resources located outside the United States.
- She details commonly offshored services include audit, billing and coding, call center support, data storage, and transcription.
- Lori highlights the risks associated with offshoring, including technical risks, physical security risks, language barriers, and political instability.
- She emphasizes the importance of ensuring compliance with federal and state laws, including HIPAA and Medicaid.

Coordination of Internal Stakeholders

- Lori discusses the importance of engaging internal stakeholders in the monitoring and performance evaluation of third-party vendors.

- She explains a cross-functional committee should be established, including individuals from internal audit, compliance, legal, quality, risk management, supply chain, and billing.
- She notes this committee should define roles and responsibilities, including subject matter experts who can evaluate technical components of vendor performance.
- Lori emphasizes the importance of using tools such as dashboards for transparency and accountability is highlighted, along with the need for continuous risk assessment and due diligence.

Governance and Oversight

- Lori explains the importance of governance and leadership buy-in for TPRM.
- She notes that executive leadership and the board should receive regular updates on TPRM activities and metrics.
- She discusses the DOJ's evaluation of corporate compliance programs, and the specific expectations related to managing third parties.
- Lori emphasizes the importance of having a robust TPRM program that is integrated into the organization's procurement and vendor management processes.

Establishing a TPRM Structure

- Lori details the different structures for establishing a TPRM program, including centralized, decentralized, and hybrid models.
- She notes a centralized structure is useful in smaller environments, while a decentralized structure can create challenges such as duplication of effort and lack of transparency.
- Lori explains why a hybrid model is recommended, where the TPRM team has assigned responsibilities, but departments interacting with vendors also have defined roles.
- She notes that best practices for establishing a TPRM program include following the risk management life cycle, maintaining current logs of issues, and reviewing questionnaires and documentation standards.

Conclusion and Resources

- Lori provides resources for attendees, including surveys and information on TPRM.
- She emphasizes the importance of engaging others within the organization to understand their role in TPRM.
- Lori encourages attendees to use the information provided to evaluate and improve their TPRM programs.