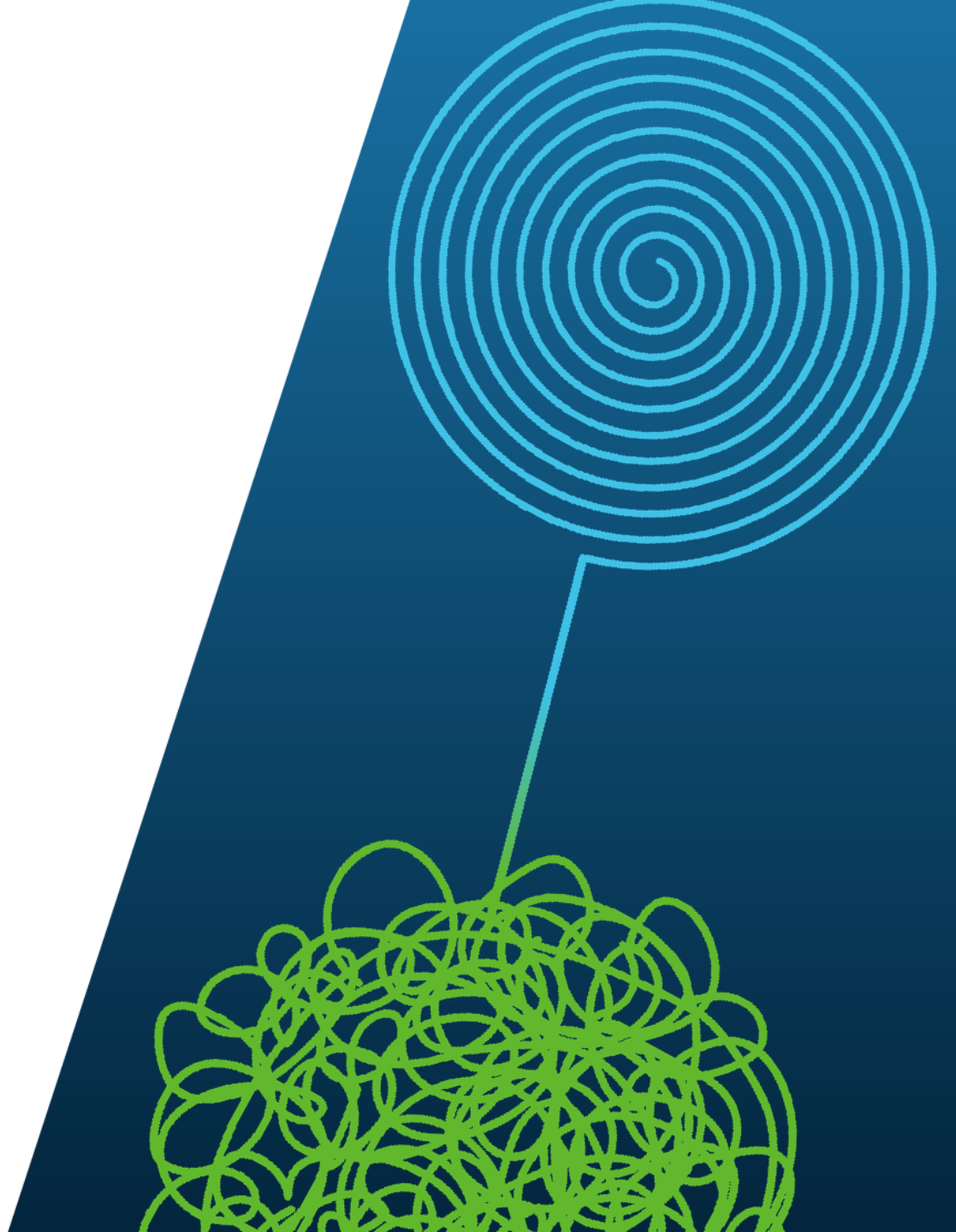
## Healthcare Regulatory Roundup #118

# Managing Third-Party Risk

## Compliance and Cybersecurity

**September 16, 2026**



# Introductions


**Katie Croswell**

Manager

kcroswell@pyapc.com



**Erin Walker**

Manager

ewalker@pyapc.com



PYA

pyapc.com

865.673.0844


ATLANTA | CHARLOTTE | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA

# Today's Session

## General Purpose

- During this session, we will discuss the key elements and importance of an integrated Third-Party Risk Management (TPRM) program with an emphasis on the evolving regulatory and compliance landscape.
- The session will also explore how weak third-party diligence can lead to significant risk and/or data exposure and how organizations can mitigate these risks through best practices and governance

## Objectives

1. Understand the importance of TPRM in healthcare
2. Review recent incidents and regulatory focus areas
3. Define and categorize types of third parties
4. Identify regulatory and compliance requirements pertaining to third-party vendors
5. Explore the core elements of a TPRM program lifecycle
6. Understand the coordination of internal stakeholders
7. Receive recommendations for appropriate governance oversight, including board-level reporting and escalation protocols

# 1. The Importance of TPRM in Healthcare

# The Big Picture – TPRM Program Importance


- Cyberattacks, ransomware, supply chain shortages, and privacy breaches result in **regulatory focus, fines, and penalties**.
- All demonstrate the **critical importance** of a robust TPRM program for healthcare entities of all sizes.

# TPRM Proposed Updates

- The 2026 proposed updates to the HIPAA Security Rule further underscore this urgency, introducing **new requirements** such as:
  - **Mandatory** multifactor authentication (MFA)
  - Comprehensive risk assessments that **explicitly include third-party vendors**

# 2. Recent Incidents and Regulatory Focus Areas

# The Rising Tide of Third-Party Breaches in Healthcare

In recent years, **healthcare has become the most targeted industry** for third-party data breaches. Healthcare breaches represented 66% of all individuals impacted by breaches in 2025.

These breaches are not only increasing in frequency but also in severity, often resulting in **massive data exposure**, **service disruptions**, and **regulatory scrutiny**.

The reliance on interconnected vendor ecosystems, cloud platforms, and outsourced services has created new vulnerabilities that threat actors are **exploiting with alarming success**.

# Notable Third-Party Breach Examples from 2024/2025

## Change Healthcare

- **Impact:** Affected over 192 million individuals
- **Cause:** Exploitation of network vulnerabilities by the AlphV/Blackcat ransomware group
- **Consequence:** $3.1 billion in response costs (to date) and a $22 million ransom payment. Numerous lawsuits ongoing

## Episource, LLC

- **Impact:** Affected 6.6 million individuals
- **Cause:** Unauthorized network access
- **Consequence:** Episource services multiple health plans. Raised OCR and DOJ concerns about data aggregation risk at vendors (access to richer data sets)

## Blue Shield of CA

- **Impact:** 4.7 million individuals affected
- **Cause:** Inadvertent data disclosure via third-party tracking technologies
- **Consequence:** Demonstrated that vendor configuration and oversight failures, not hacking, can still trigger major HIPAA exposure

# 3. Recognizing Types of Third Parties

# Examples of Third-Party Vendors

- **Medical Device Manufacturers**
- **IT Service Providers** (*IT support, network management, cybersecurity services*)
- **Telehealth Platforms**
- **Electronic Health Record (EHR) Providers**
- **Cloud Service Providers**
- **Third-Party Administrators**
- **Billing and Coding Firms**
- **Laboratory Services**
- **Supply Chain Vendors**
- **Data Analytic Companies**
- **Consultants and Advisors**
- **Marketing and Website Services**

# 4. The TPRM Program Lifecycle

# TPRM Lifecycle

**Onboarding:** Initiating the relationship with the vendor, including due diligence and contract setup

**Risk Assessment:** Evaluating potential risks such as compliance, financial, and operational risks

**Monitoring:** Ongoing oversight of vendor performance and risk indicators

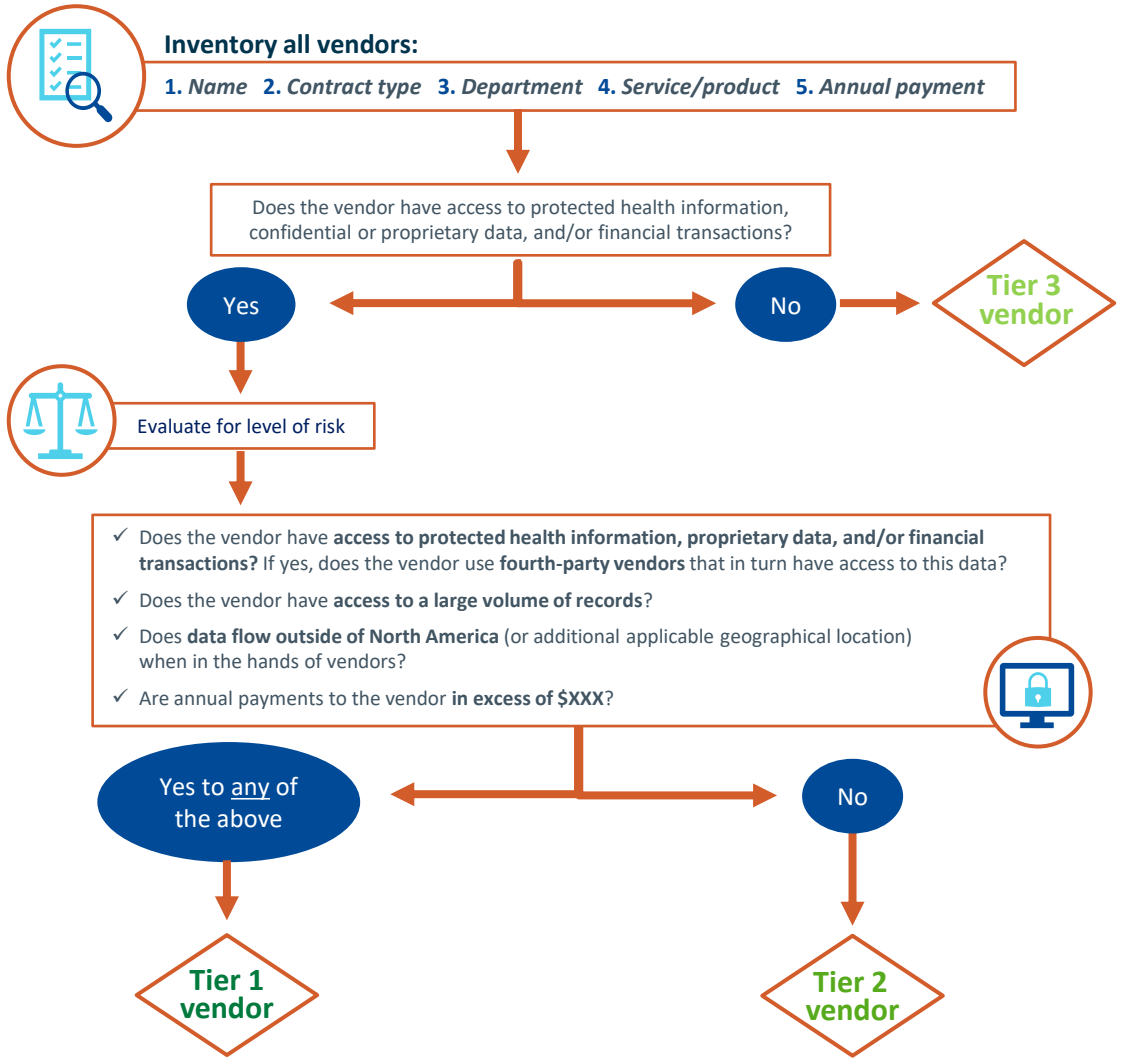
**Performance Evaluation:** Reviewing vendor deliverables and service levels against expectations

**Offboarding:** Properly terminating the relationship and ensuring data and compliance closure

# Inventory and Onboarding Considerations

| | |
|---|---|
| **Maintain** | Develop and maintain a centralized inventory of all third-party relationships. |
| **Classify** | Classify vendors by risk tier (e.g., critical, high, medium, low). |
| **Require** | Require security attestations or certifications (e.g., SOC 2, HITRUST, ISO 27001) for high-risk vendors. |

# Sample Vendor Tier Determination Flowchart




**Compliance requirements:**

### Tier 3

- ✓ Exclusion check for vendor entity
- ✓ Financial due diligence

### Tier 2

- ✓ All Tier 3 requirements
- ✓ SOC 2 or similar compliance certification
- ✓ Signed attestation of adherence to compliance standards and code of conduct
- ✓ Completion of vendor risk assessment form

### Tier 1

- ✓ All Tier 2 and 3 requirements
- ✓ Fully executed business associate agreement (if PHI is involved)
- ✓ Executed attestation of completion of compliance training for all vendor representatives
- ✓ Completion of organizational orientation and compliance training for all contracted employees
- ✓ Annual evaluation of contract performance

# 5. Regulatory and Compliance Requirements for TPRM

# Vendor Risk Assessment: Due Diligence Considerations

***Do your homework!***

- Data Privacy and Security Breaches
- Regulatory Non-Compliance/Settlement Agreements (e.g., CIAs)
- Cybersecurity Incidents and Security Ratings
- Conflicts of Interest
- Compliance Program Maturity
- Financial and Operational Stability
- Excluded Providers

# IT TPRM Due Diligence and Contractual Considerations

## Security and Data Protection

- Cybersecurity posture
- Access controls
- Initial and ongoing IT security risk assessments
- Controls aligned to recognized framework (NIST, ISO, HITRUST)
- MFA

## Compliance and Legal

- Regulatory compliance
- Contractual obligations
- Audit rights
- Security questionnaires
- Third-party audits (high-risk vendors)
- Evidenced-based assurances (SOC 2 Type II, penetration testing)

## Operational Risk

- Business continuity and disaster recovery
- Incident detection and response
- Subcontractor management

## Financial and Organizational Health

- Financial stability
- Reputation and history
- Insurance coverage – **in 2025 the average cost of a healthcare data breach was $7.42 million**

## Performance and Service Delivery

- Service levels
- Scalability and flexibility
- Support and responsiveness

# A Word About Offshoring…

**DEFINITION**

**Utilization of human or technology resources that are located outside of the United States, districts and territories of the U.S. The U.S. judicial system has limited authority to enforce violations.**

## Offshore Vendor Risks

- Technical risks
- Physical security (e.g., clean room standards)
- Language barriers and interpretations
- Management of offshored services challenging
- Some restrictions for use of offshore vendors at the state and federal levels

## Commonly Offshored Services

- Audit (internal/external)
- Billing
- Coding, billing, payment posting
- Call center
- Data storage and hosting
- Utilization review
- Transcription

# 6. Coordinating Internal Stakeholders

# Coordination of Internal Stakeholders in Monitoring and Performance Evaluation

**Establish**

Establish a **cross-functional** TPRM committee – Internal Audit, Compliance, Legal, Quality, Risk Management, Supply Chain, IT, Billing and Service Line Leaders for significant outsourced departments (e.g., wound care)

**Define**

Define clear roles and responsibilities across departments. Identify Subject Matter Experts (SMEs) who will be involved in due diligence and **ongoing monitoring** of the vendor against the contractual requirements.

**Use**

Use shared dashboards for transparency and accountability**. Due diligence is not a one-time event.** Review high risk and critical vendors at least annually. Consider a third-party risk management platform to store BAAs, manage due diligence documentation and monitoring.

# Develop a Continuous Risk Assessment Mindset

**Never stop learning!**

Monitor regulatory updates (*e.g., HIPAA Privacy and Security Rule*) and align TPRM policies accordingly.

Participate in threat intelligence sharing networks (*e.g., American Hospital Association's Health Information Sharing and Analysis Center*).

Conduct post-incident reviews to update risk models and controls.

# 7. TPRM Governance and Board Oversight Recommendations

# Governance Oversight

Provide regular TPRM updates to executive leadership and the board.


Align TPRM metrics with enterprise risk appetite – financial, operational, compliance, and reputational risks.

Conduct annual reviews of the TPRM framework and update policies as needed.

**Test via “desktop” exercise.**

# DOJ's Evaluation of Corporate Compliance Programs (March 2023)

## Third-party management expectations:

**Risk-based and integrated processes**

- Integrated with the entity's procurement and vendor management processes

**Appropriate controls**

- Ensuring appropriate business rationale for the use of third parties
- Do contract terms specifically identify the services to be performed?

**Management of relationships**

- How does the company monitor performance? Audit rights?

**Real actions and consequences**

- Mitigation of due diligence identified risks

# Questions Board Members Should Be Asking About TPRM

1. Has a multi-disciplinary TPRM Committee been created? Who is involved?
2. What is the business rationale for the use of third parties?
3. How are third parties selected? Are conflicts of interest evaluated?
4. How are third-parties audited? Monitored? By whom?
5. Has the organization considered and analyzed compensation structures for third parties against compliance risks?
6. How are due diligence “red flags” addressed?

## Our Next Webinars

### September 24; 12:30 – 1:30 pm ET

*CPE Webinar*

**The Bottom Line #2:**

**Occupational Fraud: A Risk Every Organization Faces**

**(1 CPE credit in Accounting available)**

### September 30; 11 am – 12:30 pm ET

*Special topic 90-min HCRR*

**Healthcare Regulatory Roundup #119:**

**OB/GYN Reimbursement Changes & Physician Compensation**

*Please leave a comment regarding topics for future HCRR webinars!*

# Thank you for attending!

PYA's subject matter experts untangle the latest industry developments every month in our popular Healthcare Regulatory Roundup webinar series.

For on-demand recordings of this and all previous HCRR webinars, and information on upcoming topics and dates, please follow the link below.

pyapc.com/hcrr-webinars

pyapc.com | 865.673.0844

ATLANTA | CHARLOTTE | KANSAS CITY | KNOXVILLE | NASHVILLE | TAMPA


A national healthcare advisory services firm providing consulting, audit, and tax services