

Healthcare Cyber & Privacy

Moving Beyond HIPAA Baselines

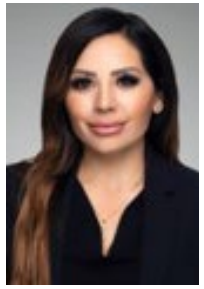
October 2026

forvis mazars

Today’s Presenters



Ray Baxter
Director, IT Risk & Compliance
629.900.2172
ray.baxter@us.forvismazars.com



Diana Ramirez
Manager, IT Risk & Compliance
213.282.8713
diana.ramirez@us.forvismazars.com

© 2026 Forvis Mazars, LLP. All rights reserved.

Learning Objectives
What You Will Leave With

1. **Recognize:** Why HIPAA compliance alone may not address modern cyber, privacy, and operational resilience risk.
2. **Identify:** Common risk areas around PHI, privacy governance, cybersecurity controls, and third parties.
3. **Apply:** Practical ways to align privacy and security readiness before an incident, audit, or inquiry.

© 2026 Forvis Mazars, LLP. All rights reserved.

Agenda

1. HIPAA: The Foundation
2. The Connected Risk Reality
3. Modern Threats & Operational Impact
4. Where PHI Can Be Found
5. A Practical Readiness Model



© 2026 Forvis Mazars, LLP. All rights reserved.

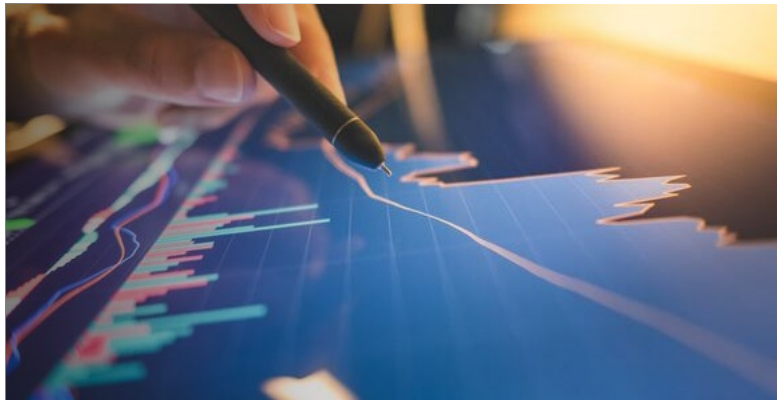
Setting the Scene

HIPAA Is the Foundation, Not the Full Strategy



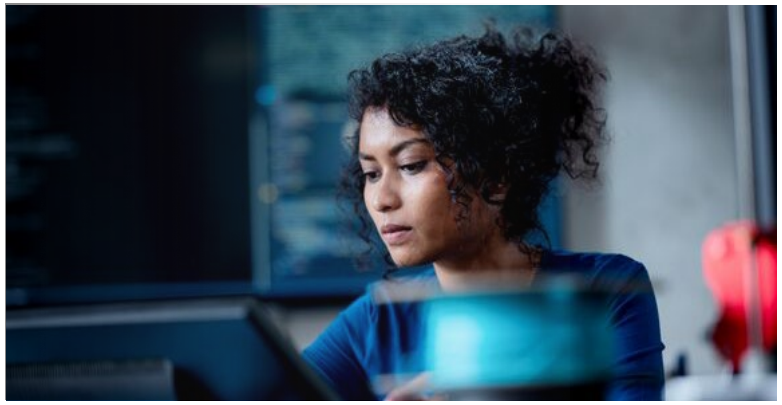
$7.42M

U.S. Healthcare average cost of a data breach in 2025, according to IBM's "Cost of a Data Breach" report.



12

Number of consecutive years that Healthcare has had the highest cost per data breach of any industry, according to IBM's "Cost of a Data Breach" report.



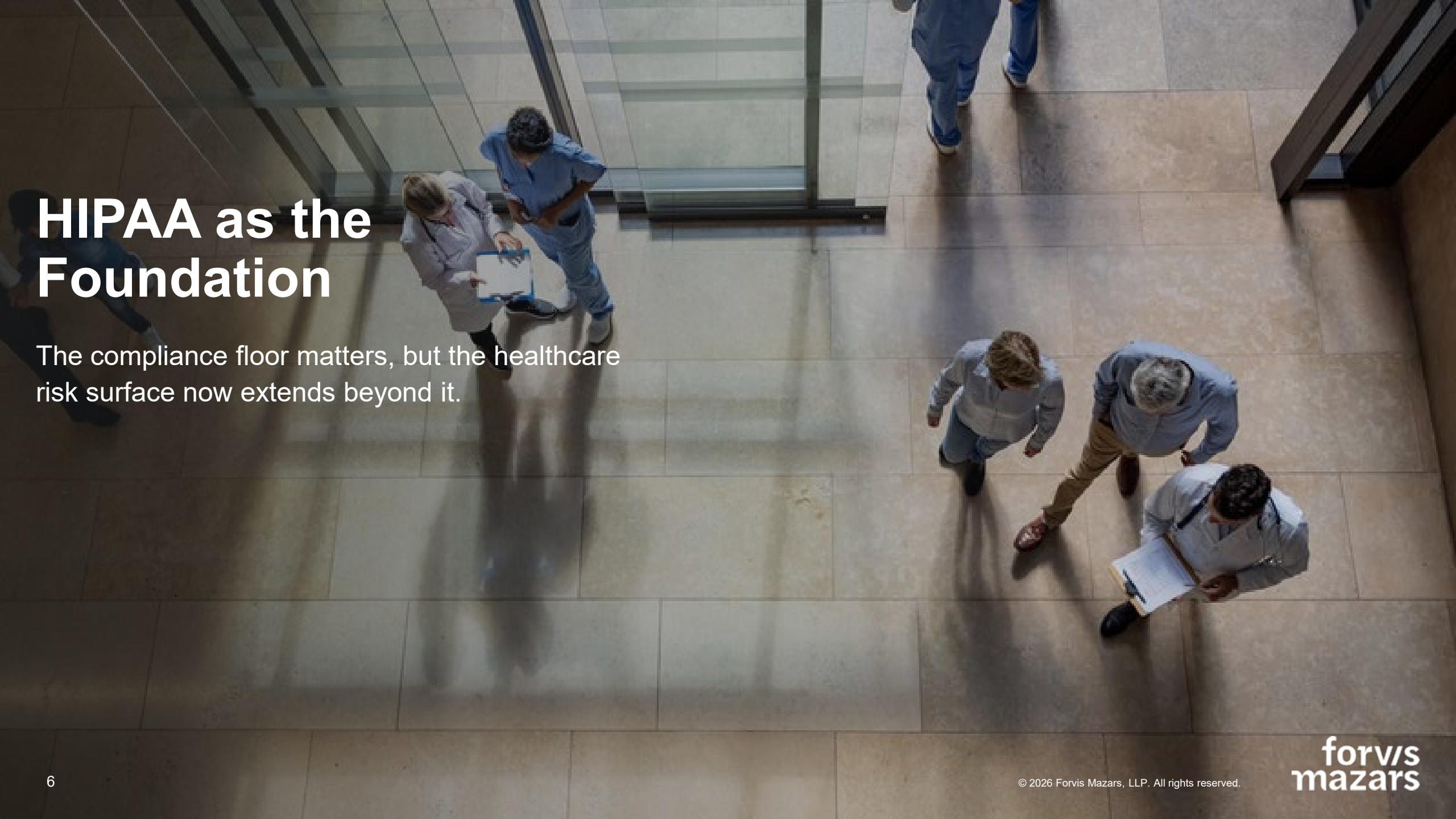
1

Connected challenge: protecting PHI while sustaining care delivery and trust

Source: "Cost of a Data Breach Report 2026," IBM and Ponemon Institute, via beckershospitalreview.com, July 31, 2026.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars



HIPAA as the Foundation

The compliance floor matters, but the healthcare risk surface now extends beyond it.

© 2026 Forvis Mazars, LLP. All rights reserved.

HIPAA as the Foundation
The Compliance Floor, Not the Ceiling

HIPAA defines the minimum standard for protecting PHI. Today's risk surface extends well past it.

What HIPAA Establishes

- Privacy expectations for permitted use and disclosure
- Administrative, physical, and technical safeguards
- Breach notification duties and timelines
- Business associate obligations

What Resilience Must Also Address

- Ransomware and clinical disruption
- Cloud, analytics, and end-user data flows
- Third- and fourth-party concentration risk
- State privacy and tracking-technology exposure
- Evidence expected during inquiries

Meeting the standard is the starting point. Connected readiness is the operating model.

© 2026 Forvis Mazars, LLP. All rights reserved.

How the Baseline Evolved
Built for 1996, Stretched Ever Since

The regulatory floor has shifted slowly. The healthcare risk surface has not.

1996

HIPAA Enacted

National baseline

2009

HITECH Act

Breach notice and enforcement

2013

Omnibus Rule

Direct business associate liability

Today

Beyond the Baseline

Cloud, AI, analytics, vendors, preparations for proposed rule changes taking effect in July 2027

Regulatory change is incremental. Technology and dependency change is continuous.

© 2026 Forvis Mazars, LLP. All rights reserved.

The Connected Risk Reality

Attackers, regulators, and patients experience privacy, cyber, and operations as one system.



© 2026 Forvis Mazars, LLP. All rights reserved.

The Current Reality
Connected Risk, Managed Separately

Privacy
Different owners and tools

Operations
Care delivery and downtime

Security
Technical controls and threats

Third parties
Shared data and dependencies

The Gap | No shared inventory, evidence model, escalation path, or decision forum

The highest-consequence failures often happen between programs, not inside one program.

© 2026 Forvis Mazars, LLP. All rights reserved.

The Emerging Problem
Healthcare Data Has Outgrown the EHR

Expanded Data

- Wearables
- Apps
- Genomics
- AI-derived insights
- Social determinants

Expanded Entities

- Cloud platforms
- Data brokers
- AI/ML providers
- Telehealth
- Research partners

Expanded Obligations

- State privacy laws
- Health-data statutes
- FTC enforcement
- Wiretap claims
- International transfers

A HIPAA-only inventory can miss high-risk healthcare data, systems, and relationships.



© 2026 Forvis Mazars, LLP. All rights reserved.

State Privacy Laws
Entity Coverage Does Not Equal Data Coverage

HIPAA-Regulated Data

- Patient medical records
- Treatment information
- Healthcare billing
- Clinical records subject to HIPAA

Data That May Require Separate Analysis

- Workforce data
- Marketing preferences
- Website and app analytics
- Nonclinical consumer interactions

Classify the data flow before relying on an exemption.

© 2026 Forvis Mazars, LLP. All rights reserved.

Modern Threats & Operational Impact

Today’s attacks disrupt care delivery, not just data, and the operational fallout outlasts the incident.



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Operational Impact

Measure the Blast Radius Across Five Lenses

01	02	03	04	05
Patient Safety	**Operations**	**Financial**	**Regulatory**	**Trust**
Delayed or diverted care	Downtime and manual workflows	Recovery cost and lost revenue	Investigation and notification	Patient, workforce, and partner confidence

A technically contained incident can still become an enterprise crisis.

© 2026 Forvis Mazars, LLP. All rights reserved.

Threat-to-Impact Chain

A Cyber Event Becomes a Care Event

01	02	03	04	05
Initial Access	**Propagation**	**Disruption**	**Obligations**	**Recovery**
Phishing, stolen credentials, exposed service	Privilege escalation and lateral movement	EHR, imaging, pharmacy, or scheduling unavailable	Containment, patient safety, contracts, notices	Restore, validate, communicate, learn

Containment, patient safety, and notification obligations have the same starting line.

© 2026 Forvis Mazars, LLP. All rights reserved.

Audience Discussion

Tabletop Scenario: A Critical Vendor Goes Dark

At 8:10 a.m., a patient-facing platform becomes unavailable. The vendor reports “an active security event” but cannot provide a restoration time.

First 30 minutes	First 4 hours	First 24 hours
• Who declares the incident? • How is patient safety assessed?	• What manual workflows activate? • Which leaders and vendors engage?	• What evidence is preserved? • What notifications are evaluated?

The test is not whether the plan exists. It’s whether decisions can be made under uncertainty.

© 2026 Forvis Mazars, LLP. All rights reserved.

Where PHI Risk Can Be Found

PHI and health-related data move through systems, vendors, analytics, endpoints, and everyday workflows.



© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

PHI Journey Map

Follow the Data, Not Just the System

01	02	03	04	05
Collect	**Use**	**Enrich**	**Share**	**Retain / Delete**
Portal, call center, device	Care, billing, operations	Analytics, AI, research	Vendors, partners, exchanges	Archives, backups, disposal

Evidence to retain | Owner • purpose • data elements • legal basis • vendors • security controls • retention • deletion

The most useful inventory connects data, systems, purposes, owners, vendors, and evidence.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Where to Look First
Six High-Friction Risk Hotspots

01 Websites & Portals
Pixels, tags, session replay

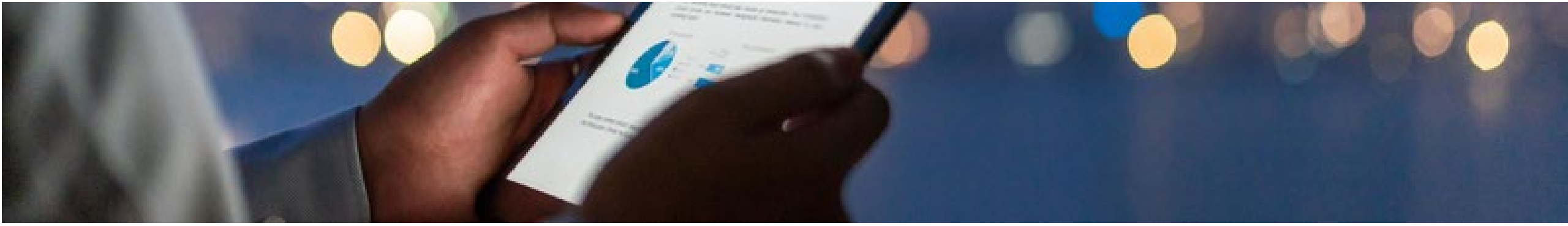
02 Vendor Ecosystem
SaaS, AI, adtech, subprocessors

03 Identity & Access
Shared accounts, excess privilege

04 Ambient AI
Recording, transcription, secondary use

05 End-User Tools
Email, files, collaboration, downloads

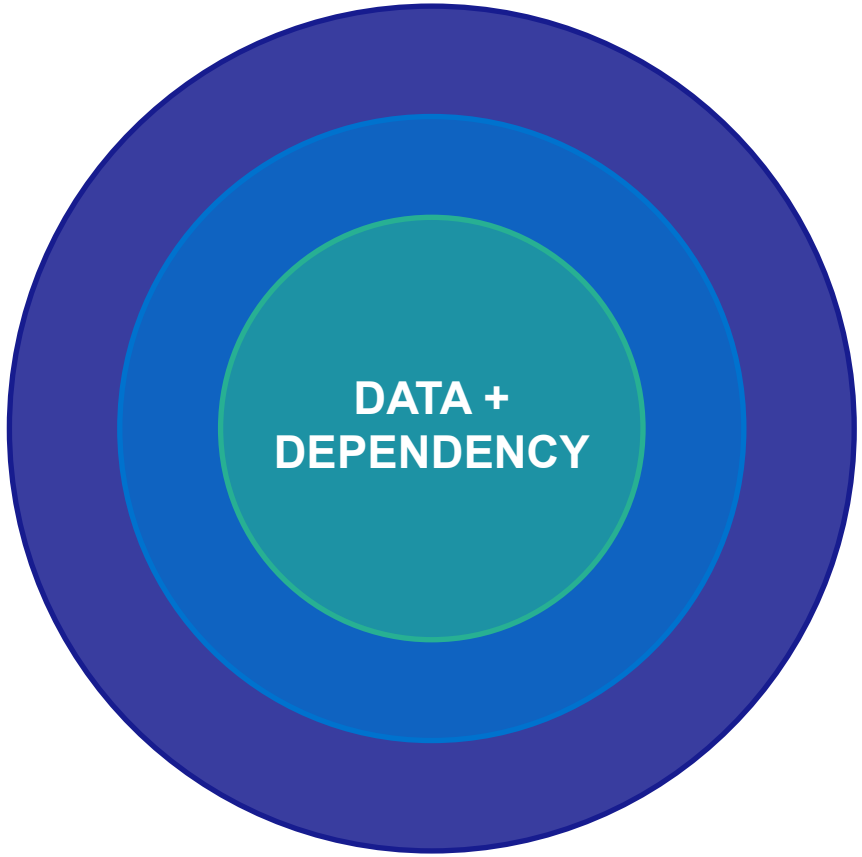
06 Policy Mismatch
Published promise vs. actual practice



© 2026 Forvis Mazars, LLP. All rights reserved.

Dependency View

Third-Party Risk Is Core Operational Risk



Know the dependency

Service, data, integrations, privileged access, and downstream providers

Set the response contract

Notification, evidence, cooperation, restoration, and communications

Test the failure mode

Outage, breach, data integrity issue, and vendor unavailability

You inherit your vendor’s dependencies—including the ones you never contracted with.

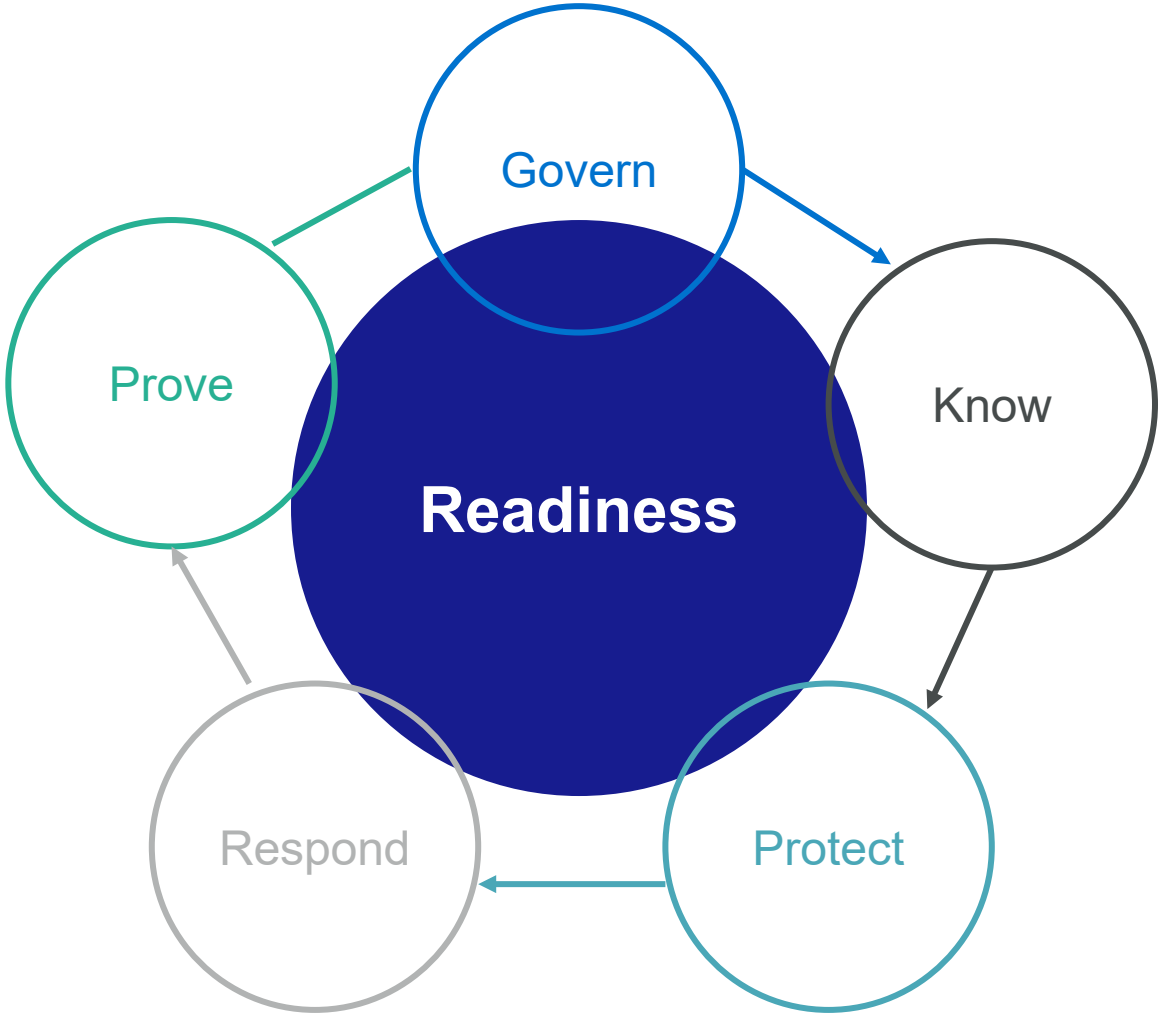
© 2026 Forvis Mazars, LLP. All rights reserved.

A Practical Readiness Model

Connect governance, security, privacy, third-party risk, incident response, and evidence before the pressure arrives.

© 2026 Forvis Mazars, LLP. All rights reserved.

Connected Readiness Model
Five Capabilities That Reinforce One Another



© 2026 Forvis Mazars, LLP. All rights reserved.

Audit & Inquiry Readiness
Turn Policies Into Evidence

01	02	03	04	05
Policy	**Procedure**	**Control**	**Evidence**	**Decision**
What should happen	How work is performed	What prevents or detects failure	Proof the control operated	How exceptions and risk are resolved

Regulators and boards need supportable evidence, not only assurances.

© 2026 Forvis Mazars, LLP. All rights reserved.

Integrated Response
One Incident, Five Coordinated Workstreams

Technical
Detect, contain, eradicate, restore

Clinical / Operations
Protect care delivery and activate downtime

Privacy / Legal
Assess data, obligations, privilege, notices

Third Party
Coordinate vendor evidence and restoration

Communications
Align workforce, patient, regulator, and media messages



© 2026 Forvis Mazars, LLP. All rights reserved.

Three Takeaways to Bring Back



1. **HIPAA is foundational, not complete:** Use it as the floor for a connected cyber, privacy, and resilience strategy.
2. **PHI risk follows the data and dependency:** Look beyond the EHR into vendors, cloud, analytics, AI, and end-user tools.
3. **Readiness is a team capability:** Connect governance, controls, response, and evidence before an incident or inquiry.

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars



IT Risk & Compliance

Questions?

© 2026 Forvis Mazars, LLP. All rights reserved.



Don’t Miss the Next Session of the

2026 Cybersecurity Virtual Symposium

Deepfake Vishing: Stopping a Voice-Cloned CEO in 20 Minutes

Tomorrow at 10:00 a.m. - 11:00 a.m. ET

© 2026 Forvis Mazars, LLP. All rights reserved.

forvis mazars

Contact

Forvis Mazars

Ray Baxter
Director, IT Risk & Compliance
P: 629.900.2172
ray.baxter@us.forvismazars.com

Diana Ramirez
Manager, IT Risk & Compliance
P: 213.282.8713
diana.ramirez@us.forvismazars.com

The information set forth in this presentation contains the analysis and conclusions of the author(s) based upon his/her/their research and analysis of industry information and legal authorities. Such analysis and conclusions should not be deemed opinions or conclusions by Forvis Mazars or the author(s) as to any individual situation as situations are fact-specific. The reader should perform their own analysis and form their own conclusions regarding any specific situation. Further, the author(s)' conclusions may be revised without notice with or without changes in industry information and legal authorities.

© 2026 Forvis Mazars, LLP. All rights reserved.