

# Managed Third-Party Risk Management for Healthcare

HIPAA-aligned vendor risk oversight built for covered entities and business associates. Your platform or ours.

<h2 style="color: #00A696;">725+</h2> <p>large healthcare breaches reported to OCR in 2024</p>	<h2 style="color: #00A696;">180 days</h2> <p>compliance window once the final rule is published</p>	<h2 style="color: #00A696;">\$9.77M</h2> <p>average cost of a healthcare data breach</p>
--	---	--

The HIPAA Security Rule is about to change everything about how you manage vendor risk. The proposed NPRM eliminates the distinction between "required" and "addressable" safeguards, mandates annual written verification of business associate technical controls by a cybersecurity subject matter expert, and requires documented risk assessments of every BA relationship. Whether the final rule lands in 2026 or beyond, the direction is clear—and the time to prepare is now.

## ENGAGEMENT MODELS

### Two Ways to Work With Us

<p><b>Bring Your Own Platform</b></p> <p>We operate your existing TPRM tool</p> <ul style="list-style-type: none"> <li>✓ Full administration of your platform</li> <li>✓ Vendor onboarding, tiering &amp; classification</li> <li>✓ Questionnaire distribution &amp; follow-up</li> <li>✓ Risk scoring &amp; remediation tracking</li> <li>✓ Reporting aligned to your workflows</li> <li>✓ Platform optimization &amp; configuration tuning</li> </ul>	<p><b>Fully Hosted Solution</b></p> <p>We provide the platform and the program</p> <ul style="list-style-type: none"> <li>✓ Turnkey TPRM platform provisioned for you</li> <li>✓ Complete vendor inventory buildout</li> <li>✓ Full assessment lifecycle management</li> <li>✓ Continuous monitoring &amp; automated alerts</li> <li>✓ Executive dashboards &amp; board-ready reporting</li> <li>✓ No capital outlay—platform included in service</li> </ul>
---	--

## SERVICE SCOPE

### What's Included

<p><b>BA Inventory &amp; Tiering</b></p> <p>Business associates classified by ePHI access scope, data sensitivity, criticality, and BAA obligations. Risk tiers drive assessment depth, frequency, and annual verification requirements.</p>	<p><b>Assessment Management</b></p> <p>HECVAT, SIG, or custom HIPAA-aligned questionnaires—distributed, tracked, and analyzed. We chase vendor responses and validate evidence against Security Rule safeguards.</p>
--	--

<p><b>Risk Scoring &amp; Remediation</b></p> <p>Quantified risk ratings mapped to HIPAA Security Rule safeguards, with issue-level remediation plans, POA&amp;Ms, and tracked deadlines—ready for OCR examination.</p>	<p><b>Continuous Monitoring</b></p> <p>Dark web ePHI exposure monitoring, OCR breach report tracking, financial health signals, and cyber rating feeds on critical business associates between assessment cycles.</p>
<p><b>Regulatory Alignment</b></p> <p>Mapped to the current HIPAA Security Rule and proposed NPRM requirements, including mandatory encryption, MFA, annual BA verification, and 72-hour recovery mandates.</p>	<p><b>Reporting &amp; Governance</b></p> <p>Monthly operational reports, quarterly executive summaries, annual maturity assessments, and audit-ready evidence packages aligned to OCR examination protocols.</p>

**IMPLEMENTATION**

## Low-Friction Onboarding

Our streamlined onboarding process gets your managed TPRM program operational quickly with minimal disruption to your team. From initial discovery through steady-state operations, we handle the heavy lifting so your organization can focus on patient care—not vendor paperwork.

**BUILT FOR HEALTHCARE**

## Who This Is For

- ✓ Health systems and hospitals managing hundreds of business associate relationships
- ✓ Health plans and payers with complex vendor ecosystems touching member ePHI
- ✓ Community health centers and physician groups without dedicated TPRM staff
- ✓ Organizations preparing for OCR Phase 3 audits or cyber insurance renewal
- ✓ Healthcare clearinghouses and HIT vendors with downstream BA obligations

**DIFFERENTIATORS**

## Why The Fowler Group

<p><b>Practitioner-Led</b></p> <p>Managed by CISSP/CISM-certified professionals with direct healthcare CISO experience and deep HIPAA regulatory knowledge.</p>	<p><b>Platform Agnostic</b></p> <p>We work inside your existing tool or deploy our own. No vendor lock-in. Purpose-built for BAA lifecycle management.</p>	<p><b>Healthcare Native</b></p> <p>HIPAA Security Rule crosswalks, NPRM readiness assessments, OCR audit preparation, and HITRUST alignment in our playbook.</p>
<p><b>Scales on Demand</b></p> <p>From 25 critical business associates to 500+. Scales with your vendor ecosystem and M&amp;A; activity without adding FTEs.</p>	<p><b>Informed by Experience</b></p> <p>Our evaluation process is informed by decades of experience dealing with real threats and incidents involving third parties.</p>	

**Ready to get ahead of the HIPAA Security Rule changes?**

Schedule a complimentary HIPAA TPRM readiness assessment. [info@thefowlergroupllc.com](mailto:info@thefowlergroupllc.com) · [tfgcyber.com](http://tfgcyber.com)