LeadingIT

June 2026

The NetWork

IN THIS EDITION:

Who Must Comply with HIPAA: A Decision Framework for Covered Entities and Business Associates

IBM's 2023 Cost of a Data Breach Report found that healthcare organizations faced an average breach cost of $10.93 million — the highest of any industry. HHS has assessed civil monetary penalties against organizations of every size, from solo practices to large hospital networks.

The question many SMB owners and IT managers cannot confidently answer is more fundamental: does HIPAA even apply to my organization?

The Two Categories That Create HIPAA Obligations

Covered entities are the organizations HIPAA was originally written for: health plans, healthcare providers that submit electronic transactions, and healthcare clearinghouses. If your organization falls into one of these categories, both the Privacy Rule and Security Rule apply directly to your operations.

Business associates are where most SMBs outside healthcare get caught off guard. A business associate is any person or organization that creates, receives, maintains, or transmits protected health information (PHI) on behalf of a covered entity. Your industry label does not matter. What you do with the data does.

Common SMB categories that trigger business associate status:

- **Managed IT providers** supporting systems where PHI is stored or transmitted
- **Legal and accounting firms** that access patient records or healthcare financials
- **Cloud storage** and **SaaS vendors** hosting platforms where patient data resides
- **Medical billing companies** and **document management firms** handling patient records

A vendor cannot opt out of HIPAA obligations by declining to sign a Business Associate Agreement (BAA). Business associates are directly subject to the Security Rule by statute.

What PHI Actually Covers

Protected health information is any individually identifiable data connecting a person's identity to their health condition, treatment history, or payment for care. HHS specifies 18 identifier types — including names, phone numbers, email addresses, dates, and account numbers — that constitute PHI when linked to health information.

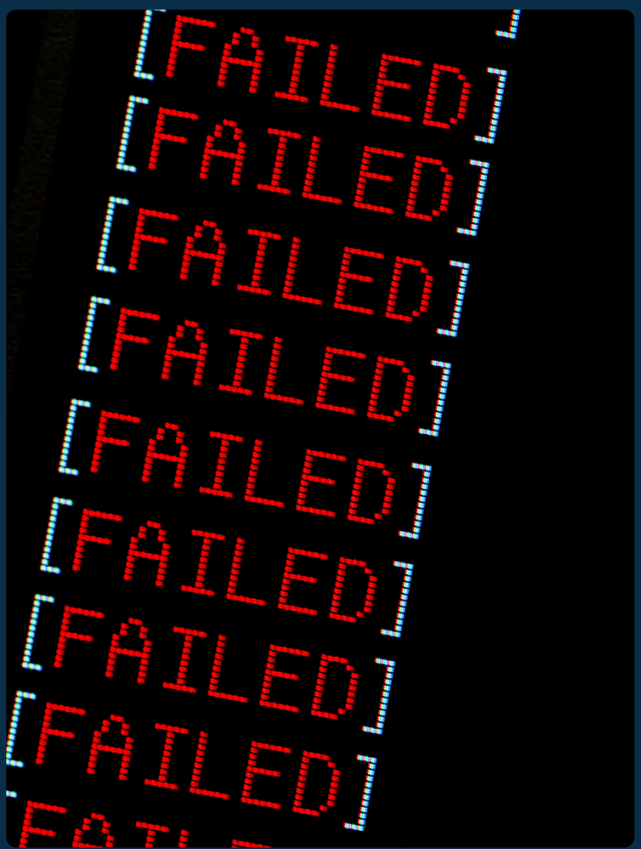
PHI surfaces in places organizations do not always anticipate: automated backup systems, IT support tickets, email threads, and shared file drives. A data-flow mapping is a required first step, not optional.

A Five-Question Decision Framework

Work through these in order:

1. Are you a health plan, a healthcare provider that submits electronic transactions, or a clearinghouse? **If yes, you are a covered entity.**
2. Do you provide services to a covered entity that involve handling PHI on their behalf? **If yes, you are a business associate.**
3. Is a signed BAA in place with every covered-entity client sharing PHI with you? **If not, this is your highest-priority action.**
4. Do any of your systems store or process electronic PHI? **If yes, Security Rule requirements apply: access controls, audit logging, and encryption at rest and in transit.**
5. Is your compliance position documented? **An undocumented assumption that HIPAA does not apply provides no protection during an audit.**

If your analysis determines HIPAA does not apply, document that conclusion formally. Other frameworks — including the FTC Safeguards Rule — may still govern your data practices.



The Most Common Failure Point

For SMBs that qualify as covered entities or business associates, the most common compliance failure is not deliberate violation. **It is undocumented processes, unmapped data flows, and vendor relationships operating without proper agreements in place.**

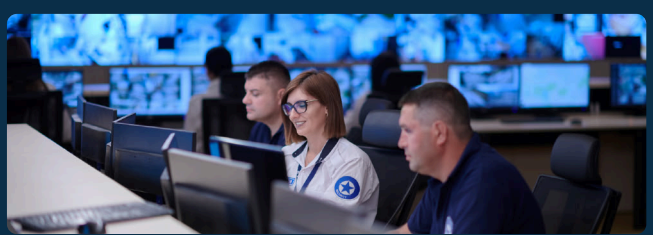
Civil penalties range from $145 to $73,011 per violation, with annual caps that compound quickly. HIPAA compliance is not a one-time project. It requires ongoing risk analysis, documented policies, trained staff, and technical controls that evolve as the organization changes.

VAPT vs SOC vs Pen Testing: Which Security Service Does Your Business Actually Need?

Security vendors treat "VAPT," "SOC," and "pen test" as interchangeable. They are not. Each answers a different question, operates on a different timeline, and addresses a different layer of risk. Choosing the wrong one wastes budget and creates a false sense of security while real exposures go undetected.

What Each Service Actually Does

VAPT (Vulnerability Assessment and Penetration Testing) is a two-phase engagement. The assessment phase catalogs known weaknesses. The penetration testing phase then actively attempts to exploit the most critical findings, proving what an attacker could accomplish. Breadth first, then depth.



A managed SOC (Security Operations Center) provides continuous monitoring of your network, logs, and alerts around the clock. Where VAPT asks "what weaknesses exist," a SOC asks "what is happening right now." Those are fundamentally different questions.

Standalone pen testing is a targeted attack simulation scoped to specific systems. It goes deep on a defined target but skips the full attack surface assessment that VAPT includes.

The Timeline Is the Key Difference

VAPT and pen tests are point-in-time. They produce an accurate picture of your security posture on the day testing occurs — and that picture starts going stale the moment a new user is added, an application is updated, or network access is reconfigured.

SOC monitoring is continuous. A business running one VAPT per year goes 364 days without visibility into newly introduced exposures. New vulnerabilities are published daily, and that gap is real, active attack surface.

When to Choose Each One

Start with VAPT if:

- You have never had a formal security assessment
- A compliance deadline (PCI DSS, HIPAA, SOC 2) falls within the next 12 months
- You recently completed a major infrastructure change or cloud migration
- You are applying for or renewing a cyber insurance policy

Move toward managed SOC when:

- You have remediated critical findings from at least one VAPT cycle
- Your industry or data type makes continuous detection a regulatory requirement
- You lack internal staff to monitor and triage alerts around the clock

They Work Best Together

Annual VAPT cycles and continuous SOC monitoring reinforce each other. Testing surfaces structural weaknesses. Monitoring catches active exploitation between cycles. The mature approach runs both, but sequencing matters — establish your baseline first, then add continuous detection as the next layer.

According to IBM's 2025 Cost of a Data Breach Report, the average breach cost reached $4.44 million globally. For a 50-person business, a fraction of that figure is enough to trigger regulatory penalties, customer loss, or permanent closure. The right security service is the difference between detecting a threat in minutes and discovering it weeks later.

The 5 R's of Cloud Migration: Security Considerations for SMBs

According to IBM's 2024 Cost of a Data Breach Report, the average breach cost reached $4.88 million. Breaches involving cloud environments consistently rank among the most expensive, and the configuration decisions made during migration are a primary driver. For SMBs planning a cloud move, the security conversation belongs at the planning stage, not after the cutover.

What the 5 R's Are

Gartner's 5 R's framework helps organizations categorize every application before migrating:

- **Rehost**: Move workloads to the cloud with minimal changes (lift and shift)
- **Replatform**: Make targeted optimizations without a full rewrite
- **Refactor**: Redesign applications as microservices for cloud-native architecture
- **Repurchase**: Replace on-premises software with a SaaS alternative
- **Retire**: Decommission workloads that no longer serve the business

Most SMBs apply several of these across different applications. Assigning the wrong strategy is one of the most common causes of post-migration security gaps.

Three Risks That Apply to Every Path

Three security problems appear consistently in post-migration breach investigations, regardless of which strategy you use:

- Cloud misconfiguration: Publicly accessible storage, open buckets, and overpermissive access policies
- Identity sprawl: Multiple accounts, inconsistent MFA enforcement, and stale credentials accumulating across environments- Missing network segmentation: Segmentation that existed on-premises does not transfer automatically and must be deliberately rebuilt in the new environment

Before the First Workload Moves

Security work before migration prevents the most expensive post-migration fixes. At minimum: classify every application by data sensitivity, establish identity governance and MFA enforcement, validate that backups are tested and recoverable, and define a rollback plan for each migration wave.

The shared responsibility model means the cloud provider secures physical infrastructure. Data classification, access controls, and application security sit on your side — and most SMBs underestimate how much territory that covers.

Free Antivirus for Business: Why "Free" Costs SMBs More Than They Think

IBM's 2024 Cost of a Data Breach Report puts the average breach cost at $4.88 million. Most small businesses cannot absorb a loss anywhere near that scale. Yet many run their entire endpoint security strategy on tools built for a single home computer, simply because those tools carry a $0 price tag.

Licensing software across 50 workstations adds up fast, and when free tools rank alongside paid products in search results, the $0 option looks like responsible budget management. The problem most business owners never discover until it is too late: nearly every major free antivirus product explicitly prohibits commercial use in its license agreement. The tool is free. The liability is not.

The EULA Problem

Avast, AVG, and Avira all restrict their free tiers to personal, non-commercial use. Installing any of them on company hardware violates the agreement, voids vendor support, and creates legal exposure if the issue surfaces during a breach investigation or compliance audit.

Some vendors offer a "free business" tier. In practice it removes the centralized management console and policy enforcement capabilities that make endpoint security functional across a networked organization. What remains is a single-device scanner with a business-sounding label.

What Free Tools Actually Cover

Free antivirus tools protect one device in isolation. For a business with 25 or more employees, that limitation is structural:

- No centralized dashboard. Administrators cannot see protection status or active threats across the organization from a single view.
- No automated response. Free tools cannot isolate a compromised device or alert others on the same network.
- No compliance reporting. HIPAA, PCI DSS, and similar frameworks require audit-ready documentation consumer tools cannot produce.

Is Windows Defender Enough?

No. For a business network it lacks centralized policy management, cross-endpoint threat correlation, and automated incident response. Business-grade Microsoft protection requires a paid subscription — Defender for Business or Microsoft 365 Business Premium — and organizations running unmanaged Defender have no reliable way to confirm every endpoint is current.

What Business-Grade Protection Actually Includes

Managed endpoint protection is not a more expensive version of what free tools do. It is a different category entirely:

- Centralized visibility across all Windows, Mac, and Android devices
- Behavioral detection that catches ransomware and zero-day threats free tools miss
- Automated isolation of compromised endpoints before threats spread
- Compliance-ready reporting for regulated industries

The Bottom Line

Free antivirus tools were built for home users, not networked business environments with compliance obligations and real data at stake. The licensing violation makes them indefensible in a breach investigation. The technical gaps make them ineffective before one occurs.

For SMBs that have outgrown consumer-grade security, managed endpoint protection under a predictable monthly cost is the more defensible answer.

$1000 REFERRAL PROGRAM

Do you know an organization that needs unlimited IT and cybersecurity support with an unbeatable guarantee?

You'll earn **$50** for every referral. If they sign up, you'll receive **$1000!**

815-788-6041 **GOLEADINGIT.COM/REFER**

SCAN TO LEARN MORE

Supporting Our Community

We were honored to support and attend the recent **NAMI McHenry County Vision of Hope Gala** alongside so many incredible community leaders and organizations. LeadingIT proudly supports NAMI throughout the year as a sponsor of their Mental Health in the Workplace workshops, and we're thrilled to celebrate their incredible success in raising more than **$110,000** to support mental health resources, education, and advocacy throughout our community.