Insights, News & Events

“HIPAA COMPLIANT” IS NOT A CERTIFICATION: HOW HEALTHCARE ORGANIZATIONS MUST VET AI VENDORS THAT OVERSTATE THEIR COMPLIANCE

Insights
Jun 22, 2026

“HIPAA Compliant” Is Not a Certification: How Healthcare Organizations Must Vet AI Vendors That Overstate Their Compliance

As healthcare organizations increasingly purchase artificial intelligence tools, they must beware of products stamped or marketed as “HIPAA compliant.” This label carries no government endorsement, and many of these products cannot meet HIPAA’s privacy and security standards. If your AI vendor is non-compliant, it creates potential legal exposure for your organization. This Insight explains everything you need to know and offers a concrete diligence and contracting framework to follow before signing with a vendor or deploying new AI technology.

The Pitch and the Problem

AI vendors are moving into every corner of healthcare: ambient clinical documentation, intake chatbots, prior authorization, claims analytics, patient messaging, and scheduling. Many arrive with a single line of assurance in the sales deck: “We are HIPAA compliant.” Buyers, especially clinical and operations leaders without a privacy background, treat that seal as a checkmark when it comes to compliance. It is not. In a meaningful number of cases the product as architected cannot satisfy HIPAA at all.

There is no federal HIPAA certification, seal, or registry. The Department of Health and Human Services (HHS) Office for Civil Rights (OCR) is the federal agency that enforces HIPAA,

Related People

Daniel Pepper, CIPP/US
Partner

303.218.3661

Hannah Sweiss
Partner

818.230.4255

and it does not pre-clear, certify, or endorse any product as compliant. A vendor that says it is "HIPAA compliant," "HIPAA certified," or that displays a HIPAA "seal" is making a self-assessment, **nothing more**.

In fact, the Federal Trade Commission (FTC) has said directly that these representations can be deceptive under Section 5 of the FTC Act precisely because they imply a government determination that does not exist, and the agency has backed that position with enforcement. The FTC has taken action against several digital and online healthcare platforms for allegedly:

- misrepresenting that it was a HIPAA covered entity and that its practices were HIPAA compliant;
- claiming to be HIPAA compliant even after an independent assessor told it that it fell short in multiple categories; or
- making unauthorized disclosures of consumer health data to advertising platforms.

These actions demonstrate that you cannot rely on any sort of compliance promise made by an AI vendor. When a covered entity or business associate deploys a noncompliant AI tool, the regulated entity still carries the regulatory and contractual risk. We'll explain this further in the sections below.

Dispelling Common Misconceptions

Here are the facts to clear up the top misconceptions about HIPAA compliance when working with an AI vendor.

- **A signed business associate agreement (BAA) does not resolve potential compliance issues with a product built to use protected health information (PHI) in ways the BAA cannot authorize.** Many vendors hand over a BAA while their standard terms of service grant broad rights to use customer data. The two documents contradict each other, and the permissive terms often control in practice.
- **A business associate may use or disclose PHI only as the Privacy Rule and its BAA permit (45 CFR 164.502, 164.504(e)).** Training a vendor's own commercial model on PHI is generally not "proper management and administration" of the BA and is not "data aggregation" performed for the covered entity. Absent valid de-

Service Focus

AI, Data, and Analytics

Counseling and Advice

Data Protection and Cybersecurity

Employee Benefits and Tax

Privacy and Cyber

Industry Focus

Healthcare

Resource Hubs

AI Governance Hub

identification or patient authorization, it is an impermissible use.

- **BAAs are required for each downstream provider.** Most healthcare AI features run on third-party large language model application programming interfaces. PHI passing to that downstream provider requires a BAA with that provider and flow down of equivalent obligations. Many vendors cannot show an unbroken BAA chain, or route PHI through model endpoints that expressly disclaim BA status.

- **Free text notes, images, and voice are hard to de-identify and carry real re-identification risk.** De-identification under HIPAA means Safe Harbor (removal of 18 specified identifiers) or Expert Determination (45 CFR 164.514(a)–(b)). "Anonymized" is not a HIPAA term, so promises that data will be anonymized don't mean much. Data that is not actually de-identified in accordance with HIPAA rules remains PHI.

- **Security signals – such as "SOC 2 Type II / HITRUST certified / encrypted" do not mean HIPAA compliance.** "SOC 2" is a controls attestation against criteria the vendor selects. HITRUST maps to HIPAA but is not an OCR determination. Encryption is one safeguard among many. These signals are substitutes for a deployment-specific Security Rule risk analysis.

- **HIPAA requires audit controls, unique user identification, access management, and defined retention and disposal (45 CFR 164.312).** AI tools frequently retain prompts, outputs, and logs in ways the buyer never sees, in regions and for periods that conflict with the BAA and the buyer's own retention policy.

Why the Liability Remains Yours

Reliance on a vendor's compliance representation does not discharge a covered entity's or business associate's own obligations. Risks can include:

1. Direct HIPAA Liability. The regulated entity must conduct an accurate, deployment-specific risk analysis (45 CFR 164.308(a)(1)(ii)(A)) covering every system that creates, receives, maintains, or transmits electronic PHI (ePHI). An AI tool that touches PHI is squarely within scope. A vendor's marketing claim is not a risk analysis, and OCR has

repeatedly identified deficient risk analysis as the single most common failing in its investigations.

2. Contractual and Indemnity Exposure. If the BAA is hollow or contradicted by the vendor's standard terms, the covered entity may have no effective remedy when the vendor uses PHI improperly or suffers a breach. Diligence failures also weaken cyber insurance positioning at renewal and at claim time.

3. Your Own FTC Section 5 Exposure. If your organization repeats the "HIPAA compliant" claim to patients or members, or builds patient facing assurances on top of a vendor representation you never verified, you can inherit the deceptive practice problem directly. A compliance claim is an enforceable promise, and a false one is its own violation, regardless of whether a breach ever occurs.

> **Note on Employer-Sponsored Health Plans.** For employers, the same analysis reaches self-insured group health plans. AI tools introduced by a TPA, PBM, or wellness vendor that touch plan PHI implicate the plan sponsor's HIPAA obligations and its vendor oversight duties.

The Regulatory Floor is Rising

On top of it all, here are two key growing compliance areas that you should be following:

- **Proposed HIPAA Security Rule Overhaul.** OCR issued a proposed rule in January 2025 that would, among other things, require a written technology asset inventory and network map, mandate regular risk analysis updates, and eliminate the longstanding distinction between "required" and "addressable" implementation specifications, making nearly all safeguards mandatory. As of mid 2026 the rule remains proposed, not final. While OCR targeted a final rule in 2026, that date has slipped, and a coalition of industry groups has petitioned HHS to withdraw it. Regardless of whether it is ultimately finalized in its current form, it signals OCR's direction, and an asset inventory requirement would force AI systems handling ePHI into the documented compliance perimeter.
- **Broader Enforcement and Increasing State Laws.** The FTC continues to treat health data claims and

unauthorized health data sharing as priority targets, including through the Health Breach Notification Rule for entities outside HIPAA. In addition, state consumer health data laws (such as Washington's My Health My Data Act), comprehensive state privacy statutes, and emerging state AI legislation (including Colorado's AI Act) impose obligations that attach to AI uses of health data independent of HIPAA, often with private rights of action or attorney general enforcement.

What Healthcare Organizations Should Be Evaluating Now

If you are a regulated entity under HIPAA, you should consider taking the following steps:

1. Inventory AI now. Identify every AI tool in use or in procurement that touches PHI, including features that may have been added to platforms you already license without your knowledge.

2. Re-paper the contracts. Make your BAA and security addendum control, and add explicit restrictions on training and secondary use of PHI.

3. Pull the evidence, not the badge. Collect risk analyses, attestations, subprocessor lists, and breach terms before deployment.

4. Bring AI into your risk analysis. Document each tool in your Security Rule risk analysis and technology asset inventory.

5. Police your own claims. Scrub patient and member facing materials of unverified "HIPAA compliant" assurances.

6. Build a standing intake gate. Route every new AI tool through privacy and security review before it reaches PHI.

Conclusion

We will continue to monitor developments in this area and provide updates as warranted, so make sure you are subscribed to the Fisher Phillips Insight System to receive the latest developments straight to your inbox. If you have any questions, contact your Fisher Phillips attorney, the authors of this Insight, any attorney in Privacy and Cyber Practice Group, or any attorney on our Healthcare Industry Team.