# The Health Tech Founder's HIPAA Compliance Checklist

## 10 Things You Must Have Before Launch

**Ankita (Ann) Srivastava**

Founder & Principal Attorney, Gavel Speaks Inc.

Harvard LL.M. | 500+ Global Clients | 9+ Years

**compliance.gavelspeaks.com**

# Why This Checklist?

Before you launch your health tech product, use this checklist to identify and close your HIPAA compliance gaps. Each item represents a common failure point I've seen across 500+ health tech engagements.

HIPAA violations carry penalties of up to **$50,000 per violation**, and the average cost of a healthcare data breach is **$7.42 million**. Yet most of these violations stem from gaps that could have been caught with a simple pre-launch review.

This checklist won't make you compliant on its own — compliance requires tailored legal architecture specific to your product, your data flows, and your jurisdictions. But it will tell you **where your gaps are** so you know exactly what to fix before you go live.

## How to Use This Checklist

- Go through each item honestly. If you can't check the box, that's a gap.
- Prioritize: Items 1-3 are foundational. Items 4-6 are operational. Items 7-10 are ongoing.
- If you have more than 3 unchecked items, you're not ready to launch.
- Use the CTA at the end to book a free discovery call if you need help closing gaps.

# The Checklist

## 1 ■ Data Flow Mapping

Document every system, vendor, and integration that touches Protected Health Information (PHI). Include data at rest, in transit, and in backup. Map where PHI enters your system, where it's stored, who can access it, and where it goes when it leaves.

*Why it matters: You can't protect what you can't see. Data flow mapping is the foundation of every other compliance activity.*

## 2 ■ Security Risk Assessment (SRA)

Conduct a formal SRA identifying threats, vulnerabilities, and risk levels for every system that handles PHI. Document findings, assign risk ratings, and create a remediation plan with timelines.

*Why it matters: This is the #1 document OCR asks for in any investigation. No SRA = no defensible compliance posture.*

## 3 ■ Business Associate Agreements (BAAs)

Sign BAAs with EVERY vendor that touches PHI — cloud providers, AI APIs, analytics tools, email services, customer support platforms. If they can access PHI, they need a BAA. No exceptions.

*Why it matters: Using vendors without BAAs is the single most common HIPAA violation for startups. One unsigned BAA can trigger a $50K fine.*

## 4 ■ AI Usage Policies

If you use AI or machine learning on patient data, document: what data is processed, who owns the outputs, whether data is used for model training, and what third-party AI services are in your stack (OpenAI, ElevenLabs, etc.).

*Why it matters: AI introduces novel compliance risks that template policies don't cover. OCR is actively investigating AI-related PHI handling.*

## 5 ■ Privacy Officer & Security Officer

Designate named individuals responsible for HIPAA privacy and security compliance. At a startup, this can be the same person. Document the appointment and their responsibilities.

*Why it matters: HIPAA requires designated officers. 'Everyone is responsible' means no one is accountable.*

# The Checklist (continued)

### 6 ■ Workforce Training

All team members with PHI access must complete HIPAA training covering: recognizing PHI, phishing avoidance, secure handling procedures, and incident reporting. Document completion. Repeat annually.

*Why it matters: Most breaches stem from human error, not technical failures. Training is your most cost-effective security measure.*

### 7 ■ Encryption Standards

PHI must be encrypted at rest (AES-256) and in transit (TLS 1.2+). Verify your cloud provider configuration actually meets these standards — don't assume. Check databases, backups, API calls, and file storage.

*Why it matters: Encryption is a 'safe harbor' under HIPAA. Properly encrypted data that's breached doesn't trigger notification requirements.*

### 8 ■ Access Controls

Implement role-based access following the minimum necessary standard. Require unique user IDs for every person who accesses PHI. Set automatic session timeouts. Log all access events.

*Why it matters: Overly broad access is a compliance and security liability. Audit logs prove who accessed what and when.*

### 9 ■ Breach Response Plan

Create a written plan covering: detection procedures, assessment criteria, containment steps, notification workflows (60-day deadline to individuals, 72 hours if 500+ affected), and documentation requirements.

*Why it matters: When a breach happens, you won't have time to figure out your plan. Build it now so you can execute under pressure.*

### 10 ■ Ongoing Compliance Program

Schedule quarterly compliance reviews, annual SRA updates, BAA audits when vendors change, and regular training refreshers. Assign ownership. Track completion dates.

*Why it matters: Compliance isn't a one-time project. The startups that get fined are the ones that did compliance once and never revisited it.*

# What's Next?

If you have unchecked items on this list, you have compliance gaps that could delay your launch, expose you to fines, or put your patients' data at risk.

I help health tech founders close these gaps — fast. In a free 15-minute discovery call, I'll review your product, your data flows, and your vendor stack, and tell you exactly what you need.

## Book Your Free Discovery Call

**calendly.com/ann-gavelspeaks/free-introductory-call**

Email: ann@gavelspeaks.com

Web: compliance.gavelspeaks.com

**Gavel Speaks Inc. — Cross-Border Healthcare Compliance**