eBOOK · HIPAA

HIPAA Compliance for Health Tech Startups: A Founder's Playbook

From covered entity determination to technical safeguards — HIPAA explained for builders, not lawyers.

36 pages · PDF · Updated May 2026 · **goironfort.com**

Introduction

Every health tech founder eventually asks: "Do we need to be HIPAA compliant?" The answer is almost always yes — and the sooner you build compliance into your product and operations, the less painful it becomes. This playbook cuts through the legal language and gives you a practical, startup-friendly guide to HIPAA.

Are You a Covered Entity or Business Associate?

HIPAA applies to two categories of organizations: **Covered Entities (CEs)** — healthcare providers, health plans, and healthcare clearinghouses that transmit PHI electronically — and **Business Associates (BAs)** — vendors and service providers that handle PHI on behalf of covered entities.

Most health tech startups are Business Associates. If your product stores, processes, or transmits PHI for a hospital, health plan, or physician group — you are a BA, and HIPAA applies to you.

Common health tech BA scenarios:

- SaaS EHR integration that syncs patient data
- Remote patient monitoring platform transmitting vitals
- Telehealth platform storing video visit records
- Medical billing software processing claims
- Population health analytics tool running on hospital data
- Cloud storage provider used by a covered entity for PHI

The Three HIPAA Rule Safeguard Categories

Administrative Safeguards (§164.308)

Policies, procedures, and workforce management. Includes risk analysis, workforce training, access management, and incident response procedures. This is the largest category — 9 standards, 22 implementation specifications.

Physical Safeguards (§164.310)

Physical access controls to systems and facilities that store ePHI. Includes facility access controls, workstation policies, and device/media controls. Relevant for any on-premises infrastructure, co-location, or physical device management.

Technical Safeguards (§164.312)

Technology controls that protect ePHI. Includes access controls, audit controls, integrity controls, and transmission security. This is where MFA, encryption, and audit logging live — and where the 2026 NPRM changes are most significant.

The 5 Things to Do in Your First 60 Days

Step 1: Designate a Privacy & Security Officer

HIPAA requires both roles. In a startup, one person often fills both. This person is responsible for developing and implementing your HIPAA program.

Step 2: Conduct Your Initial Risk Analysis

A formal assessment of threats and vulnerabilities to your ePHI. Required under 45 CFR 164.308(a)(1). Not optional, not deferrable.

Step 3: Implement Core Technical Controls

Enable MFA, configure access controls, set up audit logging, and implement encryption at rest and in transit for all ePHI-touching systems.

Step 4: Develop Required Policies

At minimum: Information Security Policy, Workforce Sanctions Policy, Access Management Policy, Incident Response Policy, and Backup & Disaster Recovery Policy.

Step 5: Execute Your First BAAs

Identify all vendors who access your PHI (AWS, data analytics providers, email platforms, etc.) and execute Business Associate Agreements with each one.

> ■ *Many founders assume AWS, Azure, or GCP handle their HIPAA compliance. They do not. Cloud providers are BAs for the infrastructure layer — but your application, data model, access controls, and workforce practices are entirely your responsibility.*

Book a Free Assessment — Iron Fort

Iron Fort's HIPAA platform automates risk analysis, policy management, BAA tracking, and technical control monitoring. Book a free 30-minute gap assessment at **goironfort.com/demo**.