HIPAA Implementation Guide for EmpowerHealth

Purpose

This document provides a structured implementation roadmap to guide engineering and product tea
building a HIPAA-aligned privacy and security layer into EmpowerHealth.

This is NOT a legal certification of HIPAA compliance. Instead, it outlines the technical, UX, and
safeguards necessary to:

- Protect user health data
- Meet App Store expectations for health data safety
- Minimize liability exposure
- Build user trust through transparency

The goal is to layer compliance without disrupting the warm, supportive feel of the product.

Core Design Philosophy

EmpowerHealth should operate as a:

> Personal advocacy and understanding tool

NOT as a:

> Clinical record system or provider platform

All HIPAA-aligned features should reinforce:

- User ownership of data
- Consent-driven sharing
- Minimal storage of sensitive inputs

Scope of Protection

Sensitive data handled by EmpowerHealth may include:

- Visit summaries
- Pregnancy-related medical context
- Diagnoses and medications
- Emotional health notes

- Provider feedback

Even if user-generated, these may function as PHI depending on usage and integrations.

Implementation Domains

1. User Consent Infrastructure

Required

- First-run privacy and data-use disclosure
- AI usage disclosure
- Explicit opt-in before uploading or entering medical information
- Re-consent required after policy updates

UX Requirements

Tone must remain warm and reassuring:

Example: "Your health story belongs to you. We keep it safe and only use it to support yo journey."

---

2. Data Minimization Strategy

Default system behavior should:

- Avoid storing raw uploaded medical text
- Avoid storing unstructured AI inputs
- Store only structured summaries when possible

Users may optionally choose to retain:

- Original documents
- Raw notes

This must be opt-in.

---

3. Manual Entry Option for Medical Summaries

To reduce PHI handling risk:

Appointment summarization must include:

- PDF Upload Option
- Manual Text Input Option

Manual input should:

- Be processed transiently
- Not stored unless explicitly requested

---

4. AI Boundary Disclosures

All AI-powered interpretations must include:

- Not medical advice notice
- Educational support framing

Example microcopy: "This explanation helps you understand your visit. It does not replace your provider."

---

5. User Data Control

Add Privacy Center containing:

- Download my data
- Delete my data
- AI usage toggle
- Research sharing toggle

Deletion must include:

- Firestore data
- Storage documents
- Notes
- Learning outputs

---

6. Security Controls

Authentication

- Enforce Firebase Auth
- No public access to user data

Authorization

- Strict Firestore rules per user
- Role-based access for admin or research roles

Storage

- Documents stored per-user
- No public URLs unless user initiated

---

7. Cloud Function Safeguards

Functions handling summaries must:

- Require authentication
- Validate all inputs
- Strip identifiable data before AI calls
- Avoid logging raw health content

---

8. Research Data Handling

If data is shared:

- Must be anonymized
- Must be opt-in
- No raw health text shared

---

9. Community Safety

Community features must:

- Prevent exposure of identifiable health details
- Allow anonymous posting
- Clearly indicate public nature of shared content

---

10. Emergency Boundary

Include visible reminder:

"For urgent concerns, contact your provider."

Backend Alignment

Engineering should implement:

- Strict Firestore rules
- Secure Storage access
- Auth-verified function calls
- Input validation
- Rate limiting for AI

Compliance UX Additions (Non-Disruptive)

Allow only:

- Inline banners
- Bottom sheets
- Settings additions

Avoid:

- Full page legal interruptions
- Clinical tone shifts

Deliverables Checklist

- Consent Flow
- Privacy Center
- Manual Summary Input
- AI Disclaimer Layer
- Data Export
- Data Deletion
- Firestore Security Rules
- Storage Isolation
- Function Validation

Remaining Non-Technical Requirements

Engineering implementation does NOT replace:

- Business Associate Agreements
- Policy documentation

- Staff access policies
- Incident response plan

Final Objective

Users should feel:

"My information is safe and in my control."

Not:

"I am interacting with a medical system."