HIPAA Readiness and Compliance Guidelines for the App

Overview

This document provides a high-level, non-legal overview of HIPAA standards and outlines how the app can be made HIPAA-ready. The intent is to guide product, design, and engineering teams in aligning system behavior with HIPAA expectations without defining implementation details or legal interpretations. This review is being conducted in anticipation of expanded clinical study usage and increased handling of user health-related data. Establishing HIPAA-aligned principles early ensures that future product and backend decisions do not introduce compliance risk and can scale safely as regulatory requirements increase.

HIPAA Readiness vs Formal Compliance

This document describes HIPAA readiness from a product and system-design perspective. Formal HIPAA compliance requires legal validation, operational controls, and contractual agreements (such as Business Associate Agreements) that are outside the scope of this document.

What HIPAA Applies To

HIPAA applies when the application handles Protected Health Information (PHI). In the context of this app, PHI may be considered to include facial images, AI analysis outputs, AI Consultant reports, uploaded medical documents, and user-identifiable information when used in a healthcare or clinical study context.

Core HIPAA Principles and App Alignment

1. Access Control

HIPAA requires that access to PHI be restricted to authorized individuals only. The app should enforce role-based access control, ensuring that users, clinicians, admins, and support staff only access the minimum data required to perform their role.

2. Audit Logging

HIPAA requires the ability to audit access to PHI. The app should maintain immutable audit logs that record when PHI is accessed, viewed, modified, or shared, including the identity of the actor and the timestamp.

3. Encryption and Data Security

HIPAA expects PHI to be protected during storage and transmission. All images, reports, and uploads should be encrypted at rest and encrypted in transit using industry-standard security practices.

4. Data Segregation

PHI should be logically segregated to prevent unintended access. Clinical study data, AI Consultant reports, and non-study user data should be clearly separated while allowing controlled references where required.

5. Consent and Disclosure

HIPAA requires clear user consent and transparency around data usage. The app should explicitly record user consent for clinical study participation and clarify how data will be used, stored, and accessed.

6. Data Retention and Deletion

HIPAA requires defined policies for how long PHI is retained and how it is deleted. The app should have documented retention rules and support deletion or anonymization of data where legally permissible.

7. Infrastructure and Vendor Compliance

HIPAA readiness extends to infrastructure providers. The app should use HIPAA-eligible services and ensure Business Associate Agreements are in place with vendors handling PHI.

What Does Not Require UI Changes

HIPAA readiness can largely be achieved through backend and operational controls. No major UI changes are required. Existing consent flows, optional study enrollment, and informational messaging already support HIPAA-aligned design principles.

Next Steps (Out of Scope for This Document)

• Legal review to validate PHI definitions and obligations • Engineering review to map backend controls to HIPAA safeguards • Vendor and infrastructure review for HIPAA eligibility and BAAs

Disclaimer

This document is for internal planning and product alignment only and does not constitute legal advice. Formal HIPAA compliance should be validated through legal and regulatory review.