Security Requirements Document
Mobile Health App

1. Overview

This Security Requirements Document defines mandatory requirements and best practices to protect user data, privacy, and the integrity of the Mobile Health App.

2. Scope

Applies to all components of the Mobile Health App including client-side, server-side, APIs, and associated backend infrastructure.

3. Security Requirements

3.1 Data Protection

- User data must be encrypted in transit using TLS (minimum version 1.2).
- Sensitive data at rest must use industry-standard encryption algorithms.
- No sensitive data should be stored locally unless necessary and must be encrypted.

3.2 Authentication & Authorization

- Users must authenticate using strong, multi-factor authentication (MFA) if available.
- Role-based access controls (RBAC) must be implemented to restrict data and functionality.
- Password policies must enforce complexity and periodic changes.

3.3 API Security

- APIs must require secure authentication tokens (e.g., OAuth 2.0, JWT).
- Input validation and output encoding must be applied to all API endpoints.
- Rate limiting and monitoring must be enabled to prevent abuse.

3.4 Privacy

- User consent must be obtained before collecting health data.
- Personal Identifiable Information (PII) must be minimized and anonymized where possible.
- Provide mechanisms for users to access, modify, and delete their data.

3.5 Logging & Monitoring

- Record security-relevant events (e.g., logins, failed attempts, data changes).
- Monitor logs for suspicious activity and retain logs securely.
- Ensure logs do not store sensitive data in plaintext.

3.6 Secure Development Lifecycle

- Conduct security code reviews and automated vulnerability scans prior to release.
- Remediate identified vulnerabilities following a risk-based approach.
- Maintain up-to-date third-party libraries and promptly address known vulnerabilities.

4. Compliance

- App must comply with relevant regulations (e.g., HIPAA, GDPR) as applicable to deployment regions.

5. Roles and Responsibilities

Role	Responsibility
App Developers	Implement security controls, conduct code reviews, fix vulnerabilities
Security Team	Define requirements, monitor compliance, manage audits
Operations	Monitor infrastructure, respond to incidents

6. Revision History

Version	Date	Description
1.0	2024-06-09	Initial draft