BiteSmart - Security and Risk Management Overview

Overview

BiteSmart is an AI-powered ingredient scanner that handles sensitive user health data. We prioritize security, privacy, and regulatory compliance to protect our users and align with global standards.

Security Questionnaires Designed

- Data Protection: GDPR, HIPAA compliance, data anonymization, minimal data retention.
- Encryption Standards: TLS 1.3, AES-256 encryption at MongoDB Atlas, client-side encryption.
- Application Security: OAuth 2.0 authentication, JWT tokens, OWASP API Top 10 practices.
- Mobile Security: EncryptedSharedPreferences, root detection, code obfuscation.
- Cloud Security: RBAC, IP whitelisting, automated backup and recovery.

Vendor Risk Assessments Conducted

- MongoDB Atlas: Assessed against SOC 2, ISO 27001, HIPAA, GDPR standards.
- OCR Providers: GDPR review, HIPAA Business Associate Agreement (BAA) evaluation.
- Third-Party Libraries: Monitored with GitHub Dependabot and Snyk for vulnerabilities.

Compliance Frameworks Followed

- HIPAA: Protected Health Information (PHI) safeguards, breach notification readiness.
- GDPR: User consent management, right to erasure, transparent privacy policy.
- ISO/IEC 27001: ISMS best practices adoption.
- OWASP Mobile & API Security: Secured app development.
- SOC 2 Type II: Focused on security, availability, confidentiality.

Identified Compliance Gaps

- Lack of HIPAA BAA from certain OCR vendors.
- Incomplete data deletion policies from some third-party libraries.

Mitigation Strategies Proposed

- Switch to HIPAA-compliant OCR vendors or local processing.
- Enforce end-to-end encryption on all transactions.
- Implement bi-annual vendor security assessments.
- Design Right to be Forgotten workflows (GDPR Article 17 compliance).

- Formalize Incident Response Plans per HIPAA standards.

Alignment with Organizational Goals

- SDG 3: Good Health and Well-being
- SDG 12: Responsible Consumption
- Trust Building: Transparent, secure handling of user data

Prepared By

Utsav Acharya
Nitesh Baniya
Pragyan Ghimire
Prabesh
April 2025