



Tweak & Eat - Information Security & Patient Data Protection Overview

CISO & Hospital IT Security Brief

1. Data Ownership & Responsibility

Hospital retains full ownership of patient data. Tweak & Eat acts strictly as a Data Processor. No resale, reuse, or AI training on hospital data without explicit written consent.

2. Data Minimization & Privacy by Design

Only nutrition-relevant data is ingested. No full EMR access required. Patient identifiers are pseudonymized wherever feasible.

3. Secure Architecture

TLS 1.2+ encryption in transit, AES-256 encryption at rest, logical tenant isolation per hospital, secure API-based integrations, and separated Prod/Staging/Dev environments.

4. Access Control & Monitoring

RBAC, least-privilege access, MFA, and comprehensive audit logging.

5. AI & Model Safety

No exposure of patient data to public AI systems. No raw PII sent to external LLMs. Architected to prevent memorization or reconstruction.

6. Compliance Alignment

Designed in alignment with India's DPDP Act.

7. Security Operations

Vulnerability scans, penetration testing, incident response, and BCP controls.

Threat Model Summary

Threat Scenario	Key Controls	Residual Risk
Unauthorized access	RBAC, MFA, audit logs	Low
Data interception	TLS encryption	Low
Cross-hospital leakage	Tenant isolation	Very Low
Insider threat	Access reviews, logging	Medium–Low
AI data leakage	Masking, no public LLMs	Very Low
API abuse	Rate limiting, key rotation	Low
DPDP non-compliance	Consent & retention controls	Low
Disaster / data loss	Backups, DR plan	Low

ISO 27001 & SOC 2 Control Mapping

Control Area	Tweak & Eat Control	ISO 27001	SOC 2
Access Control	RBAC, MFA, least privilege	A.5.15–18	CC6.1–6.3
Encryption	AES-256 at rest, TLS 1.2+	A.8.23–24	CC6.7–6.8
Data Minimization	Nutrition-only data ingestion	A.5.10	CC3.1
AI Data Protection	No PII to public LLMs	A.5.34	CC6.6
Logging & Monitoring	Audit logs & alerts	A.8.15–16	CC7.2–7.3
Incident Response	Documented IR & notification	A.5.25–26	CC7.4
BCP / DR	Backups & defined RPO/RTO	A.5.30	CC7.5