Data Flow Mapping & Information Assets

This document outlines how data moves through the CheckTick platform and identifies the core information assets supporting our health and care services.

1. System Data Flow Diagram (Logical)

Stage	Origin	Destination	Protocol	Encryption
Data Collection	Patient Browser	CheckTick App (Django)	HTTPS	TLS 1.2+ (In-transit)
Data Storage	Django Backend	RDS/PostgreSQL	Internal	AES-256 (At-rest)
Key Recovery	Admin User	Vault / Environment	HTTPS	TLS + Secret Masking
Data Export	CheckTick App	Healthcare User	HTTPS	Encrypted CSV/JSON
Backup	Database Asset	Snapshot Storage	Internal	AES-256 (UK Only)

2. Information Asset Register (IAR)

Asset ID	Asset Name	Description	Location	Owner
ASSET-01	Production DB	Encrypted survey responses	Northflank (UK)	CheckTick Admin
ASSET-02	App Servers	Containerized Django Environment	Northflank (UK)	CheckTick Admin
ASSET-03	Secret Vault	Production keys and recovery credentials	Northflank Secrets	CheckTick Admin
ASSET-04	Source Code	Application logic and DSPT documentation	GitHub (Public)	CheckTick Admin
ASSET-05	Admin Laptops	Endpoints used for system management	UK (Encrypted)	2x Employees

3. Detailed Data Flows

External Inflow (Collection)

Survey responses are initiated by patients via a web-native interface. Data is encrypted using TLS 1.2+ before leaving the browser. The Django backend receives the payload and processes it into the database immediately.

Internal Storage & Processing

Data is stored on Northflank managed infrastructure within the UK-South region. We utilize database-level encryption (AES-256). Sensitive credentials required for decryption are never stored in the application code; they are injected at runtime via a secure Vault.

Access & Outflow

Healthcare professionals access survey results via an authenticated dashboard. Data exports are only permitted after "Survey Closure" (as defined in our Data Governance Policy). Every export requires a purpose statement and is logged in the immutable audit trail.

Backup and Residency

Automated backups are performed daily. All backup data is stored within the UK geography. We do not transfer patient-identifiable data outside of the United Kingdom for any support or maintenance purposes.

---

4. Document Control & Approval

- **Initial Review:** 29th December 2025
- **Last Approval Date:** 29th December 2025
- **Approved By:** Simon Chapman, SIRO
- **Review Cycle:** Annual (or upon major architectural change)

5. API Data Flows & Security

The CheckTick API allows for secure, programmatic integration with external healthcare systems (e.g., EPRs or Clinical Dashboards).

API Data Movement

- **Direction:** Outbound (typically) – Survey data pulled by authorized external clients.
- **Protocol:** RESTful API over **HTTPS (TLS 1.2+)**.
- **Authentication:** Secured via **Scoped API Keys** or **OIDC/OAuth2 tokens**.
- **Data Format:** JSON (Encrypted in transit).

API Security Controls

1. **Appropriate Scoping:** API keys are restricted using the "Principle of Least Privilege." A key generated for a specific survey cannot access data from other surveys or organization settings.
2. **Rate Limiting:** To prevent brute-force attacks and ensure service availability, the API implements strict rate limiting at the Northflank ingress layer.
3. **Audit Logging:** Every API request is logged, including the timestamp, the identity of the API key used, the endpoint accessed, and the IP address.
4. **IP Whitelisting (Optional):** For high-sensitivity healthcare integrations, we support restricting API access to specific trusted IP ranges.

API Asset Entry (For IAR)

Asset ID	Asset Name	Description	Location
ASSET-06	API Gateway	The entry point for programmatic data access.	Northflank Ingress