Data Protection Impact Assessment (DPIA) Summary

Project: CheckTick Health Survey Platform
Date: 29/12/2025 **Lead:** Simon Chapman

1. Description of Processing

CheckTick processes health-related survey data on behalf of healthcare providers. Data is collected via web forms, encrypted in transit (TLS), and stored encrypted at rest (AES-256).

2. Necessity and Proportionality

Processing is limited to the minimum data required for the survey creator's specific health goal. Our auto-deletion policy (6-24 months) ensures we do not hold data longer than necessary.

3. Risk Assessment & Mitigation

Risk Identified	Level	Mitigation
Unauthorized Access	High	Role-Based Access Control (RBAC), MFA for admins, and Scoped API keys.
Data Breach in Transit	Med	Strict TLS 1.2+ requirement; no insecure HTTP allowed.
Loss of Encryption Keys	Med	Distributed Vault Unseal keys and documented recovery procedures.
Server Failure	Low	Daily encrypted backups in Northflank UK region; RTO < 1 hour.

4. Outcome

The residual risk is considered **Low**. All processing is conducted within the UK, and high-level encryption is applied at every stage of the data lifecycle.