DATA PROCESSING AGREEMENT (DPA)

GDPR Compliant — Contract Reference: DPA-2025-0055

PARTIES

Data Controller:	HealthTrack NHS Trust, St. Mary's Hospital, London, W2 1NY
Data Processor:	MedAnalytics Ltd, 77 Health Tech Park, Cambridge, CB1 2AB
Effective Date:	1 January 2025
Review Date:	31 December 2025 (annual review required)

1. PURPOSE & LAWFUL BASIS

MedAnalytics Ltd processes personal health data on behalf of HealthTrack NHS Trust solely for the purpose of patient outcome analytics and NHS reporting. Processing is carried out under Article 9(2)(h) GDPR (healthcare purposes) and Article 6(1)(e) (public task). Data subjects are patients of HealthTrack NHS Trust.

2. DATA CATEGORIES & RETENTION

Categories processed: NHS patient identifiers, diagnosis codes (ICD-10), treatment records, anonymised outcome data. Special category data (health) requires explicit consent or Schedule 1 DPA 2018 condition. Retention: identifiable data maximum 7 years post-treatment; anonymised data indefinitely. Data must be pseudonymised at point of transfer where technically feasible.

3. PROCESSOR OBLIGATIONS

MedAnalytics shall: (a) process data only on documented instructions from HealthTrack; (b) ensure all staff are bound by confidentiality obligations; (c) implement appropriate technical and organisational security measures per Article 32 GDPR; (d) not engage sub-processors without prior written approval; (e) assist Controller with subject access requests within 5 working days; (f) notify Controller of data breaches within 24 hours of discovery.

4. SECURITY MEASURES

Minimum required controls: AES-256 encryption at rest and in transit; multi-factor authentication for all system access; annual penetration testing with results shared with Controller; ISO 27001 certification maintained; role-based access controls with quarterly access reviews; data loss prevention tools deployed across all endpoints.

5. DATA TRANSFERS

No transfer of personal data outside the UK/EEA without explicit written approval. Any approved transfers must be protected by Standard Contractual Clauses (SCCs), adequacy decision, or appropriate safeguards under UK GDPR Chapter 5. Transfer impact assessments required for all third-country transfers.

6. AUDIT RIGHTS

HealthTrack NHS Trust retains the right to audit MedAnalytics' compliance with this DPA upon 14 days written notice, maximum once per year unless a breach has occurred. MedAnalytics shall provide all requested documentation within 10 working days and cooperate fully with audit activities.

7. TERMINATION & DATA RETURN

Upon termination, MedAnalytics shall return all personal data in agreed format within 20 working days and provide written certification of secure deletion of all copies. Anonymised, aggregated data may be retained indefinitely provided it cannot be re-identified.

RISK ASSESSMENT: COMPLIANCE — Standard GDPR DPA. Key obligations: 24-hour breach notification; sub-processor approval required; audit rights retained by controller.