

Data Processing Agreement

This Data Processing Agreement (“**Agreement**”) forms part of a Contract for ScriptSwitch Prescribing decision support software.

Between:

Black Country Integrated Care Board (“ICB”)

and

**GP Practice – (“Data Controller” also known as “Organisation”)
Lockstown Practice**

and

Optum Health Solutions UK Ltd (“Supplier”), a company incorporated in England and Wales with registered number 08630286, whose registered address is at: 5 Merchant Square, London, W2 1AS (the “Data Processor”)

Together known as the “**Parties.**”

WHEREAS

- (A) The ICB has procured a contract with the Supplier (NHS Terms and Conditions for the Provision of Services (Contract Version) (January 2018) dated 31/12/2025 of such contract for ScriptSwitch Prescribing decision support software which the ICB is responsible for (“Service Contract”).
- (B) Such Service Contract is for the benefit of all GP Practices that participate in the ICB so that they can (i) access or use (or have previously accessed or used) the ScriptSwitch System (collectively the “Services”) from Supplier; and/or (ii) provide or have previously provided data to Supplier for the purposes of the Services.
- (C) In this arrangement, the GP Practice acts as a Data Controller and the Supplier acts as a Data Processor. Refer to the Data Processing Schedule, Annex 1.
- (D) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 (UK GDPR).
- (E) The Parties wish to lay down their rights and obligations.

Data Processing Agreement Template v1

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalised terms and expressions used in this Agreement shall have the following meaning:

1.1.1 "**Agreement**" means this Data Processing Agreement and all Schedules.

1.1.2 "**Organisation Personal Data**" means any Personal Data Processed by a Contracted Processor on behalf of the GP Practice(s) that participate in the ICB pursuant to or in connection with the Principal Agreement.

1.1.3 "**Contracted Processor**" means the Data Processor.

1.1.4 "**Data Protection Laws**" means (i) the Data Protection Act 2018 (ii) the GDPR, the LED and any applicable national Laws implementing them as amended from time to time (iii) all applicable Law concerning privacy, confidentiality or the processing of personal data including but not limited to the Human Rights Act 1998, the Health and Social Care (Safety and Quality) Act 2015, the Health and Care Act 2022, the common law duty of confidentiality and the Privacy and Electronic Communications (EC Directive) Regulations

1.1.5 "**EEA**" means the European Economic Area

1.1.6 "**GDPR**" means UK GDPR. UK GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27th April 2016 on the protection of natural persons regarding the processing of personal data and on the free movement of such data (General Data Protection Regulation) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.

1.1.7 "**Data Transfer**" means:

1.1.7.1 a transfer of Organisation Personal Data from the ICB and/or GP Practice to a Data Processor; or

1.1.7.2 an onward transfer of Organisation Personal Data from a Contracted Processor to a Subcontracted processor, or between two establishments of a Contracted Processor.

1.1.8 "**Services**" means the services to be carried out by the Data Processor under the terms of the master Contract/SLA, to encourage participation in the National Diabetes Prevention Programme (Framework 3) by contacting patients or by engaging with GP Practices who have a low referral rate into the programme, as stated in the *Annex- Data Processing Services* to this Agreement.

1.1.9 "**Sub processor**" means any person appointed by or on behalf of the Contracted Processor to process Personal Data on behalf of the Organisation in connection with the Agreement.

1.2 The terms, "**Commission**", "**Controller**", "**Data Subject**", "**Member State**",

“Personal Data”, “Personal Data Breach”, “Processing” and “Supervisory Authority” shall have the same meaning as in the UK GDPR, and their cognate

terms shall be construed accordingly. **2.**

Processing of Organisation Personal Data

2.1 The Contracted Processor shall:

2.1.1 comply with all applicable Data Protection Laws in the Processing of Organisation Personal Data; and

2.1.2 not Process Organisation Personal Data other than on the relevant Organisation’s documented instructions.

2.2 The Organisation instructs the Contracted Processor to process Organisation Personal Data.

3. Processor Personnel

The Contracted Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor of any Contracted Processor who may have access to the Organisation Personal Data, ensuring in each case that access is strictly limited to those individuals who need to know/access the relevant Organisation Personal Data, as strictly necessary for the purposes of the Principal Agreement, and to comply with Data Protection Laws in the context of that individual’s duties to the Contracted Processor, ensuring that all such individuals are subject to confidentiality undertakings or professional or statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Contracted Processor shall in relation to the Organisation Personal Data implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Contracted Processor shall take account in particular of the risks that are presented by Processing, in particular from a Personal Data Breach.

5. Sub processing

5.1 The Contracted Processor shall not appoint (or disclose any Organisation Personal Data to) any Sub processor unless required or authorised by the Organisation.

6. Data Subject Rights

6.1 Considering the nature of the Processing, the Contracted Processor shall assist the Organisation by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Organisational obligations, as reasonably understood by the Organisation, to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 Processor shall:

6.2.1 promptly notify Organisation if it receives a request from a Data Subject under any Data Protection Law in respect of Organisation Personal Data;

and

6.2.2 ensure that it does not respond to that request except on the documented instructions of Organisation or as required by Data Protection Laws to which the Contracted Processor is subject, in which case the Contracted Processor shall to the extent permitted by Data Protection Laws inform Organisation of that legal requirement before the Contracted Processor responds to the request.

7. Personal Data Breach

7.1 The Contracted Processor shall notify the Organisation without undue delay upon becoming aware of a Personal Data Breach affecting Organisation Personal Data, providing the Organisation with sufficient information to allow the Organisation to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 The Contracted Processor shall cooperate with the Organisation and take reasonable steps as are directed by the Organisation to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

The Contracted Processor shall provide reasonable assistance to the Organisation with any Data Protection Impact Assessments, and prior consultations with Supervising Authorities or other competent data privacy authorities, which the Organisation reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law, in each case solely in relation to Processing of Organisation Personal Data by, and taking into account the nature of the Processing and information available to, the Contracted Processors.

9. Deletion or return of Organisation Personal Data

9.1 Subject to this section 9, the Contracted Processor shall promptly and in any event within 10 business days of the date of cessation of any Services involving the processing of Organisation Personal Data, delete and procure the deletion of all copies of those Organisation Personal Data.

9.2 The Contracted Processor shall provide written certification to Organisation that it has fully complied with this section 9 within 10 business days of the Cessation Date.

10. Audit rights

10.1 Subject to this section 10, the Contracted Processor shall make available to the Organisation on request all information necessary to demonstrate compliance with this Agreement, and shall allow for and contribute to audits, including inspections, by the Organisation or an auditor mandated by the Organisation in relation to the Processing of the Organisational Personal Data by the Contracted Processor.

10.2 Information and audit rights of the Organisation only arise under section 10.1 to the extent that the Agreement does not otherwise give them information and audit rights meeting the relevant requirements of Data Protection Law.

11. Data Transfer

11.1 The Contracted Processor may not transfer or authorise the transfer of Organisation Personal Data to countries outside the EU and/or the European Economic Area (EAA) without the prior written consent of the Organisation. If personal data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses for the transfer of personal data.

12. General Terms

12.1 **Confidentiality.** Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement ("Confidential Information") confidential and must not use or disclose that Confidential Information without the prior consent of the other Party except to the extent that:

- (a) disclosure is required by law.
- (b) the relevant information is already in the public domain.

12.2 **Notices.** All notices and communications given under this Agreement must be in writing, sent by post or sent by email to the address or email address set out in the heading of this Agreement or such other address as notified from time to time by the Parties changing address.

13. Governing Law and Jurisdiction

13.1 This Agreement is governed by the laws of the United Kingdom.

13.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of the United Kingdom, subject to possible appeal.

14. Novation

Organisation and ICB acknowledge that certain Supplier products and/or Services provided under the Agreement will be transferred to and assumed by **Egton Medical Information Systems Limited**, a company incorporated and registered in England and Wales under company number 02117205 and whose registered office is at Fulford Grange, Micklefield Lane, Rawdon, Leeds, LS19 6BA, England ("**EMIS**"), in connection with the acquisition of EMIS by TPG, a leading global alternative asset management firm with healthcare and healthcare focused software investing expertise (the "**Transaction**"). Completion of the Transaction is subject to the satisfaction of certain regulatory conditions and is expected to occur before the end of March 2026 (the "**Effective Date**").

By signing this Agreement, and in consideration of the ongoing compliance with the Agreement by EMIS, Organisation and ICB irrevocably to the assignment and


novation of all Supplier's rights and obligations under the Agreement, with effect from the Effective Date. With effect from the Effective Date:

- a. EMIS will perform the Agreement, be bound by its terms and enjoy its benefits in every way as it were the original party to it in place of Supplier.
- b. Any reference in the Agreement to Supplier will be deemed to be a reference to EMIS.
- c. Organisation and ICB will perform the Agreement and be bound by its terms in every way as if EMIS were the original party to it in place of Supplier.
- d. Organisation, ICB, and Supplier each release and discharge the other Parties from any and all claims and demands under or in connection with the Agreement whether arising before, on, or after the Effective Date, and in each case whether known or unknown to the releasing party.
- e. Organisation, ICB, and EMIS will each have the right to enforce the Agreement and pursue any and all claims and demands under it against the other Parties with respect to matters arising before, on or after the Effective Date, as if EMIS were the original party to the Agreement instead of Supplier.


EMIS will inform Organisation and ICB when the Transaction has completed and the Effective Date has occurred. From the Effective Date, Organisation and ICB should deal solely with EMIS in respect of the Agreement and correspondence relating to the Agreement should be sent to EMIS at the address set out above.

This Agreement is entered into with effect from the date first set out below.

GP Practice/Organisation ("Controller")


Signed by for and on behalf of GP Practice	
Signature:	
Title:	Dr R Mandal
Date signed:	20.4.2026

Black Country Integrated Care Board ("ICB")

Signed by for and on behalf of ICB	
Signature:	
Title:	Jodi Perks, Senior Manager – Assurance and Governance Data Protection Officer

Date signed:	02.04.2026

Contracted Processor

Signed by for and on behalf of Optum Health Solutions UK :	
Signature:	 Neil Anderson (03/11/2026 09:06:05 PDT)
Title:	Senior Director, Accounting
Date signed:	03/11/2026

ANNEX 1 – Data Processing Schedule

1. The Contracted Processor shall comply with any further written instructions with respect to processing by the Organisation. Any such further instructions shall be incorporated into this Annex.

Description	Details
Subject matter of the Processing	Provide ScriptSwitch system to the Contracting Authority and the GP practices.
Duration of the Processing	<p><u>System Recommendation and Patient Record Integration Functionality & Withholding feature</u></p> <p>The Personal Data will be retained by the Data Processor for the periods set forth below plus any additional retention period required by applicable law and in conjunction with the NHS England Code Of Practice</p> <p>Personal Data accessed from the patient record to determine whether a patient matches the demographic guidelines for a recommendation will be held on the prescriber’s desktop. Depending on the clinical system, the Personal Data will be held either only for the period that the patient’s record is open, or for either the period that the clinical system is open or until five patient records have been opened, whichever comes first.</p> <p>Personal Data processed to determine whether a recommendation has been rejected previously (the withholding feature) will be held for up to one (1) year on Optum secure servers from the date of the original script.</p> <p><u>Support & Communication</u></p> <p>Personal Data held for the purposes of application access will be held for 14 days after termination or expiration of the relevant contract.</p> <p>Personal Data held for support and communication purposes will be removed from our systems 30 days after the termination or expiration of the Relevant Contract.</p> <p><u>ScriptSwitch Decision Safety Alerts</u></p> <p>Personal Data accessed from the patient record to determine whether a patient matches the ScriptSwitch Safety alert will be processed on the prescriber’s desktop. Data transferred to Optum will be information establishing the numerical counts of safety alerts presented and the interaction of the clinician and does not constitute personal, pseudonymised or anonymised data.</p>

<p>Nature and purposes of the Processing</p>	<p>To allow Optum ScriptSwitch™ to undertake the provision of services as outlined in the ScriptSwitch Prescribing contract. ScriptSwitch Prescribing processes information on the end users' desktop to provide the end user with patient centric prescribing decision support and the Safety Alerts.</p> <p><u>System Recommendation and Patient Record Integration Functionality (including withholding function)</u></p> <p>The ScriptSwitch System is a decision support system that enables Medicines Management Teams (MMT) to create recommendations that are presented to prescribers when a medication is issued within the clinical system.</p> <p>When a product is prescribed, if there is a recommendation in the ScriptSwitch System associated with that product the ScriptSwitch System will either present the prescriber with an information message and/or a switch recommendation. A switch recommendation suggests a switch from the medication originally prescribed by the prescriber to an alternate product in line with the Contracting Authority's formulary.</p> <p>The ScriptSwitch System utilises Personal Data from the patient record (as further described below) as well as data relating to whether a recommendation has previously been rejected for the purpose of determining whether a recommendation is appropriate to be displayed for a specific patient.</p> <p><u>ScriptSwitch Safety Alerts (if applicable)</u></p> <p>In order to provide the Contracting Authority and its practices with prescribing decision support alerts for the purposes of direct care and prescribing activities, the Data Processor processes certain Personal Data as defined below.</p> <p><u>Support & Communication</u></p> <p>In order to support, maintain and deliver the ScriptSwitch System to the Contracting Authority and the practices, the Data Processor processes certain Personal Data provided by the Contracting Authority or the practices, relating to the Contracting Authority's or the Beneficiaries' employees (which may include name, business email address and mobile phone number), for the purposes of providing access to the ScriptSwitch System and for ongoing Contracting Authority communication during the term of the Relevant Contract.</p>
--	---

<p>Legal Basis for sharing (can be more than one)</p>	<p>Article 6 Performance of a contract Article 9(h) Processing is necessary for the purposes of preventative or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State Law.</p>
---	--

<p>Type of Personal Data</p>	<p><u>System Recommendation and Patient Record Integration Functionality & withholding feature</u></p> <p>The Personal Data accessed from the patient record to determine whether a patient matches the demographic guidelines and held on the prescriber's desktop is:</p> <p>The clinical systems patient ID (e.g. EMIS, TPP or INPS ID)</p> <p>The patient age</p> <p>The patient gender</p> <p>The Personal Data that leaves the prescribers desktop and is returned to Data Processor for the purposes of identifying whether a recommendation has previously been rejected is</p> <p>The clinical system prescriber ID</p> <p>The clinical systems patient ID</p> <p><u>ScriptSwitch Safety Alerts (if applicable)</u></p> <p>The Personal Data Processed for the purposes of providing prescribing decision support alerts:</p> <p>The clinical system patient IDs (e.g. EMIS or INPS ID)</p> <p>The patient name</p> <p>The patient date of birth</p> <p>The patient NHS number</p> <p>The following categories of data from the clinical system patient records:</p> <p><u>Encounter</u></p> <p>Represents encounter/consultation record. An encounter represents a meeting between a patient and a clinician in a particular location at a point time. It serves as a context in which events can occur and medications are prescribed. An Encounter can be linked to an Appointment Slot. e.g. an admission to hospital <u>Organisation</u></p> <p>Organisations associated with resources in the extract e.g. the patient's registered practice, the organisation providing a service that a patient is referred to, the organisations that practitioners</p>
------------------------------	---

work for.

e.g. patient's practice

Observation

Represents record entries covering diagnosis, current condition, past conditions

e.g. asthma, heart failure, fractured pelvis, fall

Allergy

Represents allergy, intolerance and adverse reactions recorded in source systems.

e.g. allergy to penicillin

Immunisation

Represents Immunisations recorded on source systems. e.g. covid vaccine

Referral

Represents referral of a patient for care by an external party or service or inbound referrals to provide a service related to the patient.

e.g. to mental health services or fertility clinics

Recall

Represents recall/ reminder/ diary record content in source systems

e.g. Future booking/reminder for outreach

Medication

Represents medication records in source systems. This is a combination of both Authorisation and Issue records and current and past drugs as well as acute and repeat prescriptions e.g. current and past medications (prescriptions)

Report Specimen

This view represents a Pathology Report, lab result, physical test result, scan or similar.

e.g. urine analysis, full blood count, MRI scan, x-ray, HBA1C, blood pressure.

This Personal Data is Processed on the practice desktop

Support & Communication

The Personal Data of the Contracting Authority or End User Processed for the purposes of support and communication include:

- Employee name
- Employee business email address
- Employee phone numbers including mobile numbers, where provided

<p>Categories of Data Subject</p>	<p>Contracting Authority's and practices employee data, system data and patient data as described above.</p>
<p>Plan for return and destruction of the data once the Processing is complete UNLESS requirement under union or member state law to preserve that type of data</p>	<p>All personal data will be removed within 30 days of end of contract.</p> <p>Patient NHS ID or Clinical system ID is deleted on a rolling 12 month cycle by script. This will be deleted at the end of the contract</p> <p>Other prescription transaction data e.g. non identifiable is retained for the life of the product in line with Medical Device regulations</p>