

## Data Protection Impact Assessment (DPIA) Template

A DPIA is designed to describe your processing and to help manage any potential harm to individuals in the use of their information. DPIAs are also important tools for demonstrating accountability, as they help you as a Controller to comply with the requirements of the Data Protection Legislation. Non-compliance with DPIA requirements can lead to fines imposed by the Information Commissioners Office (ICO); this includes not carrying out a DPIA at all, carrying out a DPIA in an incorrect way or failing to consult the ICO where required.

DPIA's are not new; the use of Privacy Impact Assessments has become common practice in the NHS and can provide evidence of compliance within the Data Security and Protection toolkit (DSPT); DPIAs build on that practice.

It is not always clear whether you should do a DPIA or not but there are a number of situations where a DPIA **should** be considered or where a DPIA is a **legal requirement**. If you can tick against the criteria below it is highly recommended that you undertake a DPIA and if you decide not to, ensure that you document the reasons for your decision.

You as Controller **MUST** carry out a DPIA where you plan to:

	Tick or leave blank
Use <b>profiling or automated decision-making</b> to make significant decisions about people or their access to a service, opportunity or benefit;	<input type="checkbox"/>
Process <b>special-category data or criminal-offence data on a large scale</b> ;	<b>P</b>
<b>+</b>	<input type="checkbox"/>
Use <b>innovative technology</b> in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Carry out <b>profiling</b> on a large scale;	<input type="checkbox"/>
<b>Process biometric or genetic data</b> in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
<b>Combine, compare or match data</b> from multiple sources;	<input type="checkbox"/>
Process personal data <b>without providing a privacy notice</b> directly to the individual in combination with any of the criteria in the European guidelines.	<input type="checkbox"/>
Process personal data in a way that involves <b>tracking</b> individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Process <b>children's</b> personal data for profiling or automated decision-making or for marketing purposes, or offer online services directly to them;	<input type="checkbox"/>
Process personal data that could result in a <b>risk of physical harm</b> in the event of a security breach.	<input type="checkbox"/>

You as Controller should **consider** carrying out a DPIA where you

	Tick or leave blank
Plan any major project involving the use of personal data;	<input checked="" type="checkbox"/>
Plan to do evaluation or scoring;	<input type="checkbox"/>
Want to use systematic monitoring;	<input type="checkbox"/>
Process sensitive data or data of a highly personal nature;	<input type="checkbox"/>
Processing data on a large scale;	<input type="checkbox"/>
Include data concerning vulnerable data subjects;	<input type="checkbox"/>
Plan to use innovative technological or organisational solutions;	<input checked="" type="checkbox"/>

A new DPIA should be carried out if you decide that there is a significant enough change to what you originally intended but it is good practice for DPIAs to be kept under review and revisited when necessary.

There is guidance to help you. Your Data Protection Officer (DPO) can be consulted before completing a DPIA in order to provide specialist advice and guidance or simply to talk things through with you.

Background Information	
<b>Date of your DPIA :</b>	21/07/2023
<b>Title of the activity/processing:</b>	Prescribing Decision Support Software - ScriptSwitch
<b>Who is the person leading this work?</b>	██████████
<b>Who is the Lead Organisation?</b>	BOB Integrated Care Board
<b>Who has prepared this DPIA?</b>	██████████
<b>Who is your Data Protection Officer (DPO)?</b>	██████████
<b>Describe what you are proposing to do:</b> (Include as much background information as you can about why the new system/change in system/sharing of information/data processing is required).	<p>The ICB currently commissions a Prescribing Decision Support Software package in place with OptimiseRx, which is supplied by First Databank (FDB). The contract for this service is due to expire on 31<sup>st</sup> August 2023. Following a review, the decision has been made to move from our current provider, FDB, across to Optum, who provide a package called Scriptswitch Prescribing.</p> <p>Optum Scriptswitch is on the SBS framework and is being procured by the ICB on behalf of the Practices in line with this framework, under a Direct Award.</p> <p>Purpose of the processing is to allow Optum ScriptSwitch™ to undertake the provision of services as outlined in the ScriptSwitch Prescribing contract.</p> <p>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>The Prescribing Decision Support System provides a compliant route for GPs and practice pharmacists to access a computerised system which increases the effectiveness, safety, and cost effectiveness of prescribing medicines. The support system provides clear and concise suggestions of more effective, safer, or cost-effective medicines early in the process, when a prescriber has begun to prescribe a medicine that is deemed likely to be a suboptimal choice. It also presents Safety Alerts aimed at reducing hospital admissions, by processing the patient record and prescribed products to support safer prescribing. The prescribing decision support system considers relevant national guidance.</p> <p>This decision support tool for medicines management is available as a complete off the shelf package.</p>
<b>Are there multiple organisations involved?</b> (If yes – you can use this space to name them, and who their key contact for this work is).	This package will be rolled out across all GP Practices within BOB.
<b>Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA?</b> (If so then include the details here).	Stakeholder GPs have been given the opportunity to have a hands-on session with Scriptswitch.
<b>Detail anything similar that has been undertaken before.</b>	Prescribing Decision Support Software is something GP practices are used to using and have used for the past 5+ years. Scriptswitch

was in place for 3 years prior to OptimiseRx being installed. It is also currently in place for 4 GP practices in Berkshire West locality (*Hungerford Surgery K81057, Lambourn Surgery K81052, Mortimer Surgery K81027, Pembroke Practice K81100*).

The software provider, Optum, has provided this document in support of GDPR compliance and completion of DPIA.



DPIA ScriptSwitch  
Template July 2023.

## 1. Categories, Legal Basis, Responsibility, Processing, Confidentiality, Purpose, Collection and Use

### 1.1.

What data/information will be used? <small>Tick all that apply.</small>	Tick or leave blank	Complete
Personal Data	<input checked="" type="checkbox"/>	1.2
Special Categories of Personal Data	<input checked="" type="checkbox"/>	1.2 AND 1.3
Personal Confidential Data	<input checked="" type="checkbox"/>	1.2 AND 1.3 AND 1.6
Sensitive Data (usually criminal or law enforcement data )	<input type="checkbox"/>	1.2 but speak to your IG advisor first
Pseudonymised Data	<input checked="" type="checkbox"/>	1.2 and consider at what point the data is to be pseudonymised
Anonymised Data	<input type="checkbox"/>	Consider at what point the data is to be anonymised
Commercially Confidential Information	<input type="checkbox"/>	Consider if a DPIA is appropriate
Other	<input type="checkbox"/>	Consider if a DPIA is appropriate

### 1.2.

Processing has to be lawful so identify which of the following you believe justifies what you are proposing to do and include an explanation as to why in the relevant box. You must select at least one from a – f.

Article 6 (1) of the GDPR includes the following:	
<b>a) THE DATA SUBJECT HAS GIVEN CONSENT</b>	Tick or leave blank <input type="checkbox"/>
<b>Why are you relying on consent from the data subject?</b> <small>Click here to enter text.</small>	
<b>What is the process for obtaining and recording consent from the Data Subject?</b> (How, where, when, by whom). <small>Click here to enter text.</small>	
<b>Describe how your consent form is compliant with the Data Protection requirements?</b> (There is a checklist that can be used to assess this). <small>Click here to enter text.</small>	
<b>b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY</b>	Tick or leave blank <input type="checkbox"/>
<small>(The contract needs to be between the Controller and the individual and not concern data being processed due to someone else having a contract with the Controller. Processing can happen before the contract is entered into e.g. processing a pre-health assessment for a private or cosmetic procedure that is a paid for service with the delivery of that care done under contract between the Patient and the Practitioner).</small>	
<b>What contract is being referred to?</b>	

<b>c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT</b>	Tick or leave blank
(A legal obligation mandates processing of data as a task in itself where there are likely to be legal measures available if not adhered to e.g. an Employer has a legal obligation to disclose salary information to HMRC).	<input type="checkbox"/>
<b>Identify the legislation or legal obligation you believe requires you to undertake this processing.</b> <a href="#">Click here to enter text.</a>	
<b>d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON</b>	Tick or leave blank
(This will apply only when you need to process data to protect someone's life. It must be necessary and does not only relate to the individual whose data is being processed. It can also apply to protect another person's life. Emergency Care is likely to fall into this category but planned care would not. You may need to process a Parent's data to protect the life of a child. The individual concerned is unlikely to be able to provide consent physically or legally; if you are able to gain consent then this legal basis will not apply).	<input type="checkbox"/>
<b>How will you protect the vital interests of the data subject or another natural person by undertaking this activity?</b> <a href="#">Click here to enter text.</a>	
<b>e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER</b>	Tick or leave blank
(This is different to 6 c). If you are processing data using this basis for its lawfulness then you should be able to identify a specific task, function or power that is set out in law. The processing must be necessary, if not then this basis does not apply).	<input checked="" type="checkbox"/>
<b>What statutory power or duty does the Controller derive their official authority from?</b> The ICB is established by order made by the NHS England under powers in 2006 Act with a general function of arranging for the provision of services for the purpose of health service in England.	
<b>f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY</b>	Tick or leave blank
(Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority. See the guidance for more information about the legitimate interest test).	<input type="checkbox"/>
<b>What are the legitimate interests you have?</b> <a href="#">Click here to enter text.</a>	
Article 9 (2) conditions are as follows:	
<b>a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT</b>	Tick or leave blank
(Requirements for consent are the same as those detailed above in section 1.2, a))	<input type="checkbox"/>
<b>b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION</b>	Tick or leave blank
(Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	<input type="checkbox"/>
<b>c) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON WHERE THEY ARE PHYSICALLY OR LEGALLY INCAPABLE OF GIVING CONSENT</b>	Tick or leave blank
(Requirements for this are the same as those detailed above in section 1.2, d))	<input type="checkbox"/>
<i>d) It is necessary for the operations of a not-for-profit organisation such as political, philosophical, trade union and religious body in relation to its members</i>	NA
<i>e) The data has been made public by the data subject</i>	NA
<i>f) For legal claims or courts operating in their judicial category</i>	NA
<b>g) SUBSTANTIAL PUBLIC INTEREST</b>	Tick or leave blank
(Schedule 1, part 2 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).	<input type="checkbox"/>

<p><b>h) PROCESSING IS NECESSARY FOR THE PURPOSES OF PREVENTIVE 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 OR PURSUANT TO CONTRACT WITH A HEALTH PROFESSIONAL AND SUBJECT TO CONDITIONS AND SAFEGUARDS</b></p> <p>(Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).</p>	<p>Tick or leave blank</p> <p style="text-align: center;">✓</p>
<p><b>i) PROCESSING IS NECESSARY FOR REASONS OF PUBLIC INTEREST IN THE AREA OF PUBLIC HEALTH, SUCH AS PROTECTING AGAINST SERIOUS CROSS-BORDER THREATS TO HEALTH OR ENSURING HIGH STANDARDS OF QUALITY AND SAFETY OF HEALTH CARE AND OF MEDICINAL PRODUCTS OR MEDICAL DEVICES, ON THE BASIS OF UNION OR MEMBER STATE LAW WHICH PROVIDES FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE RIGHTS AND FREEDOMS OF THE DATA SUBJECT, IN PARTICULAR PROFESSIONAL SECRECY</b></p> <p>(Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).</p>	<p>Tick or leave blank</p> <p style="text-align: center;"><input type="checkbox"/></p>
<p><b>j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH <u>ARTICLE 89(1)</u> BASED ON UNION OR MEMBER STATE LAW WHICH SHALL BE PROPORTIONATE TO THE AIM PURSUED, RESPECT THE ESSENCE OF THE RIGHT TO DATA PROTECTION AND PROVIDE FOR SUITABLE AND SPECIFIC MEASURES TO SAFEGUARD THE FUNDAMENTAL RIGHTS AND THE INTERESTS OF THE DATA SUBJECT.</b></p> <p>(Schedule 1, part 1 of the Data Protection Act 2018 gives more detail on when this can apply to processing and further guidance is available).</p>	<p>Tick or leave blank</p> <p style="text-align: center;"><input type="checkbox"/></p>

### 1.3.

**If using special categories of personal data, a condition for processing under Article 9 of the GDPR must be satisfied in addition to a condition under Article 6. You must select at least 1 from a) to c) or g) to i). NOTE: d), e) and f) are not applicable**

### 1.4.

**Confirm who the Controller and Processor is/are. Confirm if the Controller/s are solely or jointly responsible for any data processed?**

(Identify any other parties who will be included in the agreements and who will have involvement/share responsibility for the data/information involved in this project/activity. Use this space to detail this but you may need to ask your DPO to assist you. Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only).

Name of Organisation	Role
Optum Health Solutions UK Ltd	Processor
Microsoft (Provision of Azure hosting to Optum)	Processor
GP Practices- ICB wide	Sole Controller
BOB ICB (Commissioner and Medicines Optimisation team)	Other
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.
Click here to enter text.	Choose an item.

### 1.5.

**Describe exactly what is being processed, why you want to process it and who will do any of the processing?**

ScriptSwitch prescribing processes the patient data on the practice desktops for the purpose of providing prescribing decision support. This may be more cost effective and recommended drugs, alongside Safety Alerts which will identify prescribing safety related issues for the prescriber to investigate. To present this prescribing advice the patient record is accessed via APIs built to interact directly into the clinical system. The ScriptSwitch software is processing the data and presenting the pop-up to the prescribers.

The data being processed is as follows:

### **ScriptSwitch Prescribing Pop-Up and Safety Alerts**

The Personal Data accessed from the patient record does not leave the Practice desktop. This data is processed by Scriptswitch to determine whether a patient matches the demographic guidelines:

- The clinical systems patient ID (e.g., EMIS, TPP or INPS ID)
- The patient age.
- The patient gender.
  
- The patient's name – presented on the Safety Alert for confirmation of patient purposes only.
- The patient date of birth - presented on the Safety Alert for confirmation of patient purposes only.
- The patient NHS number - presented on the Safety Alert for confirmation of patient purposes only.

The following categories of data from the clinical system patient records:

#### ***Encounter***

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

#### ***Organisation***

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 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

The ICB Meds Optimisation team – working on behalf of the Practices – may use the Scriptswitch profile, analytics system and the pop-ups.

#### ***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

### **Support & Communication**

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

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

Along with the following information relating to the practices.

- Client IP Addresses
- Client Machine Names

### **1.6.**

**Tick here if you owe a duty of confidentiality to any information.** ✓

**If so, specify what types of information.** (e.g., clinical records, occupational health details, payroll information)

Patient related data

### **1.7.**

**How are you satisfying the common law duty of confidentiality?**

Consent - Implied

**If you have selected an option which asks for further information, please enter it here.**

[Click here to enter text.](#)

### **1.8.**

**Are you applying any anonymisation/pseudonymisation technique or encryption to any of the data to preserve the confidentiality of any information?**

Yes

**If you are then describe what you are doing.**

No pseudo or anonymisation is applied, data is protected by encryption.

Encryption: All data is encrypted in transit and at rest – AES 256bit *the patient ID is anonymised using SHA-512*

The data is encrypted between the clinical system and the API on the GP desktop. This data never leaves the practice and is only ever presented back to the prescriber accessing the patient record at that point.

The data that does leave the practice that would be potential be classed as PID is the patient ID. For the withholding feature Optum process the patient ID and store on hosted servers - this is encrypted. For EMIS and INPS this is the clinical system patient ID, for TPP it is the NHS patient ID.

If you don't know then please find this information out as there are potential privacy implications with the processing.

**1.9.**

**Tick here if you are intending to use any information for a purpose that isn't considered as direct patient care.**

**If so, describe that purpose.**

[Click here to enter text.](#)

**1.10.**

**Approximately how many people will be the subject of the processing?**

GP Practice population

**1.11.**

**How are you collecting the data?** (e.g., verbal, electronic, paper (if you need to add more selections then copy the last 'choose an item' and paste, the text has been left unlocked for you to do this.)

Other method not listed

Choose an item.

Choose an item.

Choose an item.

**If you have selected 'other method not listed' describe what that method is.**

Information is processed on the Practice desktop via the APIs both customised and standard APIs provided by the clinical system providers

**1.12.**

**How will you edit the data?**

Patient data is not edited by the Processor.

**1.13.**

**How will you quality check the data?**

No requirement, the information is provided directly from the system. GP practice responsible for data quality.

**1.14.**

**Review your business continuity or contingency plans to include this activity. Have you identified any risks?**

No

**If yes include in the risk section of this template.**

**1.15.**

**What training is planned to support this activity?**

Training is provided for Medicines Optimisation team members on build of profile, analytics system and the pop-ups.

Practices are invited to engagement sessions, onboarding webinars. An electronic user guide is available along with online videos for the different areas of the pop-up.

## **2. Linkage, Data flows, Sharing and Data Opt Out, Sharing Agreements, Reports, NHS Digital**

**2.1.**

**Are you proposing to combine any data sets?**

No

**If yes then provide the details here.**



[Click here to enter text.](#)

## 2.2.

### What are the Data Flows?

#### How does ScriptSwitch Prescribing Operate

1. The approved and authorized local prescribing Recommendation Profile will be stored on the Cloud and delivered to GP practice machines installed with the Desktop Application (no PID).
2. The Desktop machines make an outbound call to the Optum database to request the latest recommendation profile. This is stored on the practice desktops and updated every 30 minutes if changes are made. Only the changes are provided every 30 minutes. (No PID).
3. ScriptSwitch Safety Alerts - When the GP or other end user opens the clinical system record and displays a patient, the optional Safety Alerts will run on the GP machine to establish whether there are any medication safety related items that need to be addressed. These are presented on the desktop as a pop-up window and allows the end user to record the action taken e.g. Alert guidance actioned, scheduled consultation, book a test, Call patient, refer patient, Action not required. This action is then sent to the Optum reporting system. (No PID) The only data that is transferred to the Optum servers is the actual action taken by the prescriber as a result of being presented with a safety alert.
4. The alerts will use the clinical system published APIs to access the patient record and run the rules. No PID leaves the Practice desktop.
5. The Alerts will access the patient record and process, patient name, date of birth, NHS patient ID, to present the Alert – this is used to confirm the correct patient is being accessed. Along with the diagnoses, medications, past history, to establish whether the patient record triggers any of the Alert rules. Interrogates PID but all the processing takes place on the end-user desktop.
6. Safety Alert Information returned to Optum will include the type of alert presented, the date presented, when available the action taken, and this will be aggregated at practice and ICB/Health Board level to provide information relating to this part of the software. No patient identifiable data is stored by Optum.
7. At the point of prescribing on the clinical system, the ScriptSwitch Prescribing software will present if an alternative product is recommended to that being prescribed by the clinician.
8. At the point of prescribing the ScriptSwitch Prescribing software will access the patient record and process the age, gender, and clinical system patient ID or for TPP the NHS Patient ID, along with the prescriber's clinical system ID. This information is used in two ways as follows:
  - Patient age and gender, to establish whether the replacement recommendation is suitable for the patient based on demographic information. All information processed on the desktop only
  - To establish whether the recommendation should be withheld and not presented. This optional feature allows the CCG/HB to opt into withholding recommendations that have been previously recommended for the patient and rejected by the clinician. Processing includes the transfer of the practice ODS code, patient ID, the GP ID and the recommendation ID to the Optum cloud database, where it will be stored for 12 months. Each time a clinician prescribes for a patient the ScriptSwitch Prescribing software accesses the database in the cloud to establish whether a recommendation has previously been rejected for the patient/GP/recommendation combination and if it has, the recommended alternative will not

be presented. This data is encrypted and automatically deleted 12 months after collection.

**9. Personal Data transferred to Optum Cloud databases in anonymised format as a result of the Prescribing and Safety Alerts actions is:**

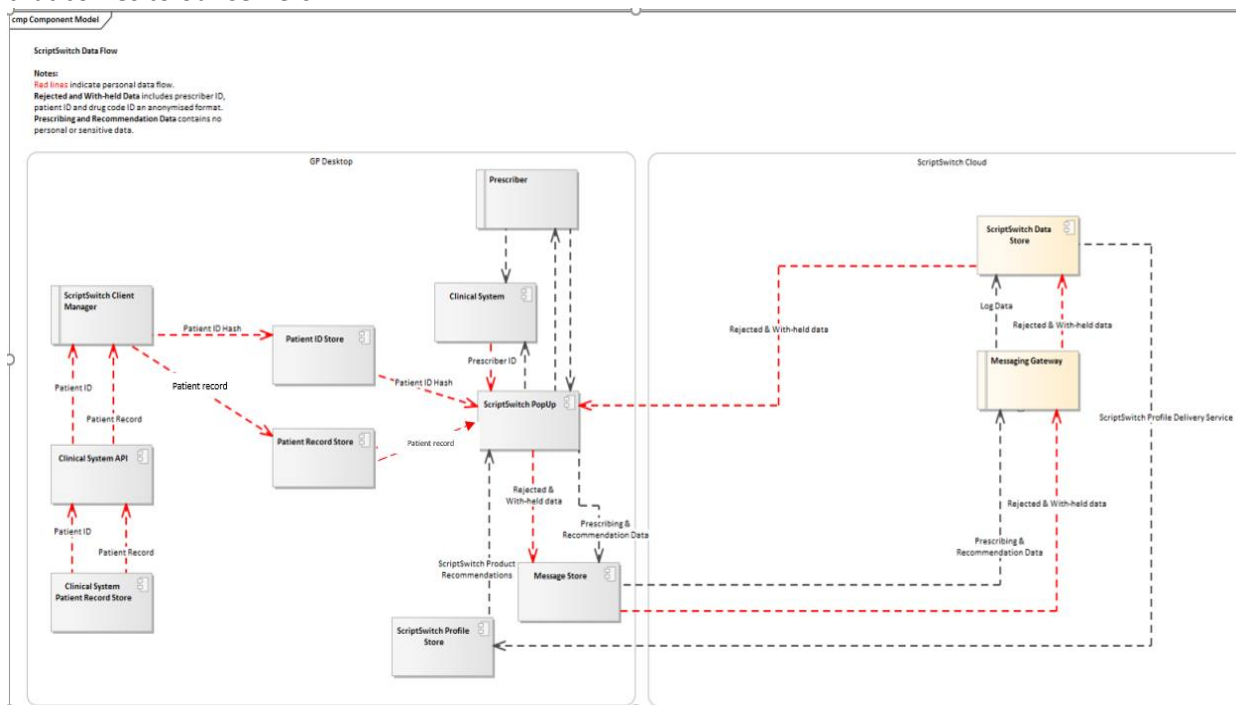
- Clinical system patient ID (for support purposes only to investigate any incidents)
- Clinical system prescriber ID – anonymized format
- Client IP Addresses
- Client Machine Names

Further detail is available in the attached document – refer to page 12 for the data flow and the explanation.



DPIA ScriptSwitch  
Template July 2023.

The red lines show the flow of the data. Left side of the diagram is the GP desktop app, right side is the data that comes to our servers.



**2.3.**

**What data/information are you planning to share?**

The following data is shared with the Optum servers

- Clinical system patient ID (for support purposes only to investigate any incidents)
- Clinical system prescriber ID – anonymized format
- Client IP Addresses
- Client Machine Names

For the withholding feature, which suppresses a switch if a GP has rejected twice in 12 months, we transfer the practice ODS code, patient ID, the GP ID and the drug recommendation ID.

For EMIS and INPS the patient ID is the clinical system patient ID, for TPP it is the NHS patient ID.

Transactional data will be shared with the ICB Medicines Optimisation Team – acceptance rates, rejection rates and savings generated by each practice

**2.4.**

**Is any of the data subject to the National Data opt Out?**

Yes - it has already been applied

**If your organisation has to apply it describe the agreed approach to this**

Applied at the GP

**If another organisation has applied, it add their details and identify what data it has been applied to**

[Click here to enter text.](#)

If you do not know if it applies to any of the data involved, then you need to speak to your Data Protection Officer to ensure this is assessed.

**2.5.****Who are you planning to share the data/information with?**

Prescribers and limited information will be held by Optum, and transactional data will be shared with the ICB Medicines Optimisation Team. This will not include any patient identifiable data.

The ICB Medicines Optimisation Team will have access to data relating to prescriber interaction with the ScriptSwitch recommendations e.g acceptance rates, rejection rates and savings generated. These will be used to produce reports that will be shared with practices to increase engagement with the tool. There is no plan to share any of this information beyond the ICB or constituent practices.

**2.6.****Why is this data/information being shared?**

The data allows the Scriptswitch product to function by offering prescribing decision support that is more patient relevant, e.g., it will take account of patient age, gender, medications, tests, ensuring that the presented recommendation.

For the safety alerts

**2.7.****How will you share it?** (Consider and detail all means of sharing)

The information is used to present a pop up, so the data as such is not being shared.

For the safety alerts the patient name, age and NHS ID is shared with the prescriber on the pop up

**Tick if you are planning to use Microsoft Teams or another similar online networking/meeting solution that may have the facility to store or record conversations or related data as part of the sharing arrangements**  
✓

**Provide details of how you have considered any privacy risks of using one of these solutions.**

**2.8.****What data sharing agreements are or will be in place?**

The contract contains a data processing agreement between Optum Health Solutions (UK) Ltd, the provider of the ScriptSwitch software, and the contract holder, BOB ICB.

**2.9.****What reports will be generated from this data/information?**

All reports hold transactional data only. No PID information is available to the reporting suite.

Support related reports used by the customer services team will identify machine names for monitoring of overall performance of the service and allows for technical issue resolution.

The ICB Medicines Optimisation Team will create reports relating to acceptance rates, rejection rates and savings generated from prescribers interacting with the software. These will be shared with practices to increase engagement.

Financial reports will be shared with relevant directorates within the ICB.

### 2.10.

**Are you proposing to use Data that may have come from NHS Digital (e.g., SUS data, HES data etc.)?**

No

**If yes, are all the right agreements in place?**

Choose an item.

**Give details of the agreement that you believe covers the use of the NHSD data.**

[Click here to enter text.](#)

If no or don't know then you need to speak to your Data Protection Officer to ensure they are put in place if needed.

## 3. Data Processor, IG Assurances, Storage, Access, Cloud, Security, Non-UK processing, DPA

### 3.1

**Are you proposing to use a third party, a data processor or a commercial system supplier?**

Yes

**If yes use these spaces to add their details including their official name and address. If there is more than one, then include all organisations. If you don't know then stop and try and find this information before proceeding.**

Optum Health Solutions UK Ltd – as solution provider and data processor  
10<sup>th</sup> Floor, 5 Merchant Square, London, W2 1AS

Microsoft UK Limited – UK instance Microsoft Azure

Amazon Web Services EMEA - EU based servers for security services and log monitoring

[Click here to enter text.](#)

[Click here to enter text.](#)

### 3.2

**Is each organisation involved registered with the Information Commissioner?** Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Registered	Registration details or comments if not registered
Optum	Yes	<b>ZA085401</b>
Microsoft	Yes	<b>Z6296785</b>
Amazon	Yes	<b>ZA481902</b>
<a href="#">Click here to enter text.</a>	Choose an item.	<a href="#">Click here to enter text.</a>
<a href="#">Click here to enter text.</a>	Choose an item.	<a href="#">Click here to enter text.</a>
<a href="#">Click here to enter text.</a>	Choose an item.	<a href="#">Click here to enter text.</a>

### 3.3

**What IG assurances have been provided to you and does any contract contain IG clauses that protect you as the Controller?** (e.g. in terms and conditions, their contract, their tender submission). Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	Brief description of assurances obtained
Optum	ISO 27001, CE cert no efd88e55-6fb2-47ec-b623-84189bd3e21f, DSP Toolkit
Microsoft	ISO 27001, ISO 27018, CE+

Amazon	DSPT toolkit, ISO 27001:2013 Certification; Cyber Essentials + Certification.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.

### 3.4

#### What is the status of each organisation's Data Security Protection Toolkit?

##### DSP Toolkit

Copy and paste the last empty row in the table to add organisations where required (the text has been left unlocked for this purpose on that row only)

Name of organisation	ODS Code	Status	Published date
Optum	8GW39	Standards Met	14/03/2023
Microsoft	8JH14	Standards Exceeded	16/05/2023
Amazon	8JX11	Standards exceeded	28/03/2023
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.
Click here to enter text.	Click here to enter text.	Click here to enter text.	Click here to enter text.

### 3.5

#### How and where will the data/information be stored? (Consider your answer to 2.7 and the potential storage of data in any online meeting or networking solution).

Data is stored in databases hosted within Optum.  
ScriptSwitch Prescribing application, administered by Optum.

The geographical location of servers is as follows.

Microsoft Azure UK South region (London)

Microsoft Azure UK West region (Cardiff)

Amazon Web Services (AWS) in EU, for application and network security logging processes only

Scriptswitch Prescribing service has full disaster recovery, with second site ready to spin up in the instance of failure. If the hosted site fails, the GPs will still see Scriptswitch, but profile deployments won't happen until service restored. Scriptswitch carry out BCP tabletop exercise at least annually and processes fall under their ISO 27001 certification. Note that as a system, Scriptswitch Prescribing is not critical to prescribing, and some GP practices chose to turn it off.

### 3.6

#### How is the data/information accessed and how will this be controlled?

Optum holds non identifiable data. Transactional data is accessed via the reporting suite – MO Team and practices have role specific access.

Personal data is only used to inform of information related to the service, ie. Outages, software updates, training

End user access to the desktop application is governed by the prescribing roles in place within the clinical system with an additional activation step to activate those users with prescribing roles for the ScriptSwitch product.

Optum DBAs have access to data for investigation of issues. MFA is in place for access following permission granted to allow access.

### 3.7

#### Is there any use of Cloud technology?

Yes

**If yes add the details here.**

Microsoft Azure Cloud is used to host the solution used by the MO Team and the reporting suite, plus the back-end tools and databases.

**3.8**

**What security measures will be in place to protect the data/information?**

Restricted user access to recommendation profile and reporting data. Controlled by ICB project lead and requested through Optum Customer Services.

Unique user id and password control,

Geo blocking on servers.

Optum DBA – MFA access to data for support purposes

**Is a specific System Level Security Policy needed?**

No

If yes or don't know then you need to speak to your Data Protection Officer to ensure one is put in place if needed.

**3.9**

**Is any data transferring outside of the UK?** (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

**If yes describe where and what additional measures are or will be in place to protect the data.**

[Click here to enter text.](#)

**3.10**

**What Data Processing Agreement is already in place or if none, what agreement will be in place with the organisation and who will be responsible for managing it?**

Data processing agreement is part of the standard contract template with Optum.

## 4. Privacy Notice, Individual Rights, Records Management, Direct Marketing

**4.1**

**Describe any changes you plan or need to make to your Privacy Notice and your proposed completion date?**

(There is a checklist that can be used to assess the potential changes required or if you wish for it to be reviewed then add the link below).

None

**4.2**

**How will this activity impact on individual rights under the GDPR?** (Consider the right of access, erasure, portability, restriction, profiling, automated decision making).

No impact on individual rights – data subjects can access directly from GP's.

**4.3**

**How long is the data/information to be retained?**

Retention period is for the life of the contract in line with regulatory requirements for medical devices.

Patient ID data is held for 12 months only, to support the With-holding feature and automatically deleted by the ScriptSwitch Prescribing code by an automated script.

Any personal data captured for support purposes, e.g., MO team names and contact details will be removed from systems at the end of the contract. It will be retained on the audit trail of the profile as dictated by regulatory requirements.

An optional feature of Scriptswitch, to establish whether the prescription recommendation should be withheld and not presented, allows the ICB/HB to opt into withholding recommendations that have been previously recommended for the patient and rejected by the clinician. Processing includes the transfer of the practice ODS code, patient ID, the GP ID and the recommendation ID to the Optum cloud database, where it will be stored for 12 months. Each time a clinician prescribes for a patient the ScriptSwitch Prescribing software accesses the database in the cloud to establish whether a recommendation has previously been rejected for the patient/GP/recommendation combination and if it has, the recommended alternative will not be presented. This data is encrypted and automatically deleted 12 months after collection.

#### 4.4

##### How will the data/information be archived?

Transactional data is archived automatically to long term storage 24 months after the transaction. Personal data held in support systems is anonymised at the end of the contract, retaining just the interactions for any incidents as required by regulatory bodies (Med device cert).

#### 4.5

##### What is the process for the destruction of records?

Personal and health data in patient record is processed on the desktop at the Practice and not held by Optum.

Personal data, if requested by end users, will be removed from support systems once request to the service desk, ticket logged, and work actioned, and ticket closed.

#### 4.6

##### What will happen to the data/information if any part of your activity ends?

Retained in line with regulatory requirements of a medical device. Activity ends on termination of contract with no storage of data by Optum.

#### 4.7

**Will you use any data for direct marketing purposes?** (you must determine this so only select don't know if you have further investigations to make but the DPIA will not be approved without this information)

No

**If yes please detail.**

## 5. Risks and Issues

### 5.1

Low risks identified.

Describe the source of risk and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	Likelihood of harm	Severity of harm	Overall risk
The API could fail and present a safety alert for the wrong patient, but it's an alert not an action. The GP still needs to act. E.g., it might warn that a blood test is out of date. The GP has to check the last blood test before requesting another. The safety alert has the detail of the patient's name and DOB to help	Remote	Minimal	Low

mitigate issues. The GP would see that patient was incorrect patient			
Unauthorised access to patient data	Remote	Minimal	Low
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

## 5.2

### Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in 5.1

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved (SIRO)
The API could fail and present a safety alert for the wrong patient, but it's an alert not an action. The GP still needs to act. E.g., it might warn that a blood test is out of date. The GP has to check the last blood test before requesting another. The safety alert has the detail of the patient's name and DOB to help mitigate issues. The GP would see that patient was incorrect patient	This is data quality risk - any inaccuracy is flagged to the GP within the patient record.	Reduced	Low	No
Unauthorised access to patient data	The patient record does not leave the Practice desktop. Access to the patient record is managed by the Practice. An automated script is run according to set profile, no additional login to the patient record. System is encrypted.	Reduced	Low	No
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

## 5.3

### What if anything would affect this piece of work?

n/a

## 5.4

### Please include any additional comments that do not fit elsewhere in the DPIA?

n/a

## 6. Consultation

### 6.1

#### Have you consulted with any external organisation about this DPIA?

Yes



**If yes, who and what was the outcome? If no, detail why consultation was not felt necessary.**

With Optum the supplier to gather information to support the DPIA

**6.2**

**Will you need to discuss the DPIA or the processing with the Information Commissioners Office?** (You may need the help of your DPO with this)

No

**If yes, explain why you have come to this conclusion.**

[Click here to enter text.](#)

## 7. Data Protection Officer Comments and Observations

**7.1**

**Comments/observations/specific issues**

██████████:

DPO review on behalf of GPs – dated Monday 25 September.

Further review of the DPIA, which has been completed comprehensively, the risks noted as 'low risks identified'.

GP practices recommended Privacy Notices to be updated as follows:

The purpose of using Prescribing Decision Support Software - ScriptSwitch:

ScriptSwitch prescribing processes the patient data on the practice desktops for the purpose of providing prescribing decision support. This maybe more cost effective and recommended drugs, alongside Safety Alerts which will identify prescribing safety related issues for the prescriber to investigate. To present this prescribing advice the patient record is accessed via Application Programming Interfaces (APIs) built to interact directly into the clinical system. The ScriptSwitch software is processing the data and presenting the pop-up to the prescribers.

Processing is necessary for the purposes of preventive 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 or pursuant to contract with a health professional and subject to conditions and safeguards.

██████████:

Low risk and practices recommended to update Privacy Notices.

## 8. Review and Outcome

**Based on the information contained in this DPIA along with any supporting documents, you have determined that the outcome is as follows:**

A) There are no further actions needed and we can proceed

**If you have selected item B), C) or D) then please add comments as to why you made that selection.**

[Click here to enter text.](#)

**We believe there are.** Choose an item.

If you have selected item B) or C) then list these in the amber boxes below and then consider additional measures, you could take and include these in the green boxes below

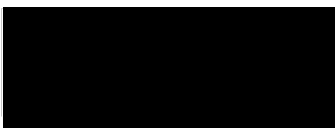
Residual risks and nature of potential impact on individuals. (Include associated compliance and corporate risks as necessary and copy and paste the complete bottom row to add more risks (the text has been left unlocked in both tables to enable you to do this)).	Likelihood of harm	Severity of harm	Overall risk
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Additional measures you could take to reduce or eliminate residual risks identified as medium or high risk above (B and C)				
Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved (SIRO)
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.
Click here to enter text.	Click here to enter text.	Choose an item.	Choose an item.	Choose an item.

Signed and approved on behalf of Buckinghamshire Oxfordshire and Berkshire West Integrated Care Board

Name: 

Job Title: Data Protection Officer

Signature: 

Date: 02/10/2023

Signed and approved on behalf of Click here to enter text.

Name: Click here to enter text.

Job Title: Click here to enter text.

Signature: Click here to enter text. Date: Click here to enter a date.

**Please note:** You should ensure that your Information Asset Register and Data Flow Mapping Schedules are updated where this is relevant.

This DPIA can be disclosed if requested under the Freedom of Information Act (2000). If there are any exemptions that should be considered to prevent disclosure detail them here: