



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 profiling or automated decision-making to make significant decisions about people or their access to a service, opportunity or benefit;	<input type="checkbox"/>
Process special-category data or criminal-offence data on a large scale ;	<input type="checkbox"/>
Monitor a publicly accessible place on a large scale;	<input type="checkbox"/>
Use innovative technology in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Carry out profiling on a large scale;	<input type="checkbox"/>
Process biometric or genetic data in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Combine, compare or match data from multiple sources;	<input type="checkbox"/>
Process personal data without providing a privacy notice 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 tracking individuals' online or offline location or behaviour, in combination with any of the criteria in the European guidelines;	<input type="checkbox"/>
Process children's 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 risk of physical harm 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 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 checked="" 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	
Date of your DPIA :	18/08/2023
Title of the activity/processing:	AccuRx – communication with Patients.
Who is the person leading this work?	██████████
Who is the Lead Organisation?	BOB ICB
Who has prepared this DPIA?	████████████████████
Who is your Data Protection Officer (DPO)?	██████████ – BOB ICB DPO
Describe what you are proposing to do: (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 aim of the Accurx platform is to improve communications between healthcare staff and patients to improve outcomes and productivity.</p> <p>The need for a DPIA is the processing on a large scale of special categories of data for the use of the Accurx platform to: exchange and store messages pertaining to patients and medical staff; perform video consultations (which are not recorded or stored) between healthcare staff and their patients; allow patients to communicate with their GP practice through responses that include free-text, answers questionnaires and submitting images/documents.</p> <p>AccuRx is used for the following functionalities:</p> <ol style="list-style-type: none"> 1. Text (SMS) Messaging The messaging feature allows NHS staff to instantly send SMS text messages to patients. Typical use-cases for this include sending a link to video consultations, advice to patients, notifying a patient of normal results, and reminding them to book appointments. Every patient communication is saved in the patient record. Text messages can be sent on ad hoc basis or as batch messages. Accurx Batch Messaging allows to send the same message to a group of patients. This includes attaching SNOMED codes or documents or collecting structured information from a group of patients by sending Florey questionnaires as a batch message. 2. Email messaging The messaging feature allows NHS staff to instantly send email messages to patients. Typical use-cases for this include sending a link to video consultations, advice to patients, notifying a patient of normal results, and reminding them to book appointments. Email messages are sent on ad hoc basis currently although there are plans to enable email batch messages. 3. Video Consultations

In the video consultation, the healthcare professional will record the observations and outcome of the consultation in the same way as a face-to-face consultation is recorded in the patient's electronic primary care record and any agreed actions are carried out.

The video consultation service is hosted by Whereby who are fully compliant with UK GDPR. The video and audio communication is only visible to participants on the call and is not recorded or stored on any server. The connection prioritises 'peer-to-peer' between the healthcare professionals' and patients' phone and follows NHS best practice guidelines on health and social care cloud security.

4. Patient Photos

Patients may be asked to submit an image (or multiple images) to the GP practice. The data is collected via a secure web-based form which is accessed via a unique link that the healthcare professional sends to the patient via SMS.

Patient images received can be "logically" deleted: i.e. resulting in the underlying data being marked in such a way that it is no longer visible to any user of the record. AccuRx follow [NHS Digital IG requirements](#), which require them to keep a photo for audit trail purposes, even if deleted the file is deleted from their platform. They can only physically (i.e. permanently and completely) delete a photo from the audit trail that they hold in response to 1) receiving a valid physical deletion request, or 2) relevant court orders or other legislative circumstances.

5. Files, documents or forms

Accurx have developed a feature that allows healthcare staff to send files or documents (such as sick notes, leaflets, letters, imaging request forms, blood forms, etc.) via SMS to patients. The document is accessible for 28 days. The patient will need to save/take a screenshot of/download/forward to email, etc. the document in order to keep a copy for their records.

6. Floreys (Health Questionnaires)

Floreys or health questionnaires are used by GP practices to gather structured information from patients which can be coded back to the patient's record using SNOMED codes. Accurx provides a library of Florey questionnaires which are standardised in-house by the clinical leads in GP Practices for users to collect symptoms and information from patients asynchronously. Florey builder allows users to go one step further and create their own questionnaires with SNOMED codes in a customised and localised way. This can be used to also send out Floreys as batch messages.

7. Patient Responses

Accurx allows healthcare professionals to send links to surveys hosted with multiple or single questions to respond to. Patients are asked to input their date of birth as identity verification, before being able to access the survey. Patients may then respond to the

	questions in those surveys related to their health which is saved in patient records.
Are there multiple organisations involved? (If yes – you can use this space to name them, and who their key contact for this work is).	Yes British Telecommunications PLC (BTEE) as SMS gateway carrier ██████████ – Main contact in BTEE
Can you think of any other Key Stakeholders that should be consulted or involved in this DPIA? (If so then include the details here).	No
Detail anything similar that has been undertaken before?	No

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

1.1.

What data/information will be used? Tick all that apply.	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 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:	
a) THE DATA SUBJECT HAS GIVEN CONSENT	Tick or leave blank <input type="checkbox"/>
Why are you relying on consent from the data subject? Click here to enter text.	
What is the process for obtaining and recording consent from the Data Subject? (How, where, when, by whom). Click here to enter text.	
Describe how your consent form is compliant with the Data Protection requirements? (There is a checklist that can be used to assess this). Click here to enter text.	
b) IT IS NECESSARY FOR THE PERFORMANCE OF A CONTRACT TO WHICH THE DATA SUBJECT IS PARTY	Tick or leave blank

(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).	<input type="checkbox"/>
What contract is being referred to? Click here to enter text.	
c) IT IS NECESSARY UNDER A LEGAL OBLIGATION TO WHICH THE CONTROLLER IS SUBJECT (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).	Tick or leave blank <input type="checkbox"/>
Identify the legislation or legal obligation you believe requires you to undertake this processing. Click here to enter text.	
d) IT IS NECESSARY TO PROTECT THE VITAL INTERESTS OF THE DATA SUBJECT OR ANOTHER NATURAL PERSON (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).	Tick or leave blank <input type="checkbox"/>
How will you protect the vital interests of the data subject or another natural person by undertaking this activity? Click here to enter text.	
e) IT IS NECESSARY FOR THE PERFORMANCE OF A TASK CARRIED OUT IN THE PUBLIC INTEREST OR UNDER OFFICIAL AUTHORITY VESTED IN THE CONTROLLER	Tick or leave blank <input checked="" type="checkbox"/>
What statutory power or duty does the Controller derive their official authority from? Health & Social Care Act – direct patient care.	
f) IT IS NECESSARY FOR THE LEGITIMATE INTERESTS OF THE CONTROLLER OR THIRD PARTY (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).	Tick or leave blank <input type="checkbox"/>
What are the legitimate interests you have?	
Article 9 (2) conditions are as follows:	
a) THE DATA SUBJECT HAS GIVEN EXPLICIT CONSENT (Requirements for consent are the same as those detailed above in section 1.2, a))	Tick or leave blank <input type="checkbox"/>

b) FOR THE PURPOSES OF EMPLOYMENT, SOCIAL SECURITY OR SOCIAL PROTECTION (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).	Tick or leave blank <input type="checkbox"/>
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 (Requirements for this are the same as those detailed above in section 1.2, d))	Tick or leave blank <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
g) SUBSTANTIAL PUBLIC INTEREST (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).	Tick or leave blank <input type="checkbox"/>
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 (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).	Tick or leave blank <input checked="" type="checkbox"/>
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 (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).	Tick or leave blank <input type="checkbox"/>
j) PROCESSING IS NECESSARY FOR ARCHIVING PURPOSES IN THE PUBLIC INTEREST, SCIENTIFIC OR HISTORICAL RESEARCH PURPOSES OR STATISTICAL PURPOSES IN ACCORDANCE WITH ARTICLE 89(1) 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. (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).	Tick or leave blank <input type="checkbox"/>

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 j). 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?

The GP practice is the data controller, and Accurx the data processor, as per Accurx's Data Processing Agreement.

Name of Organisation	Role
Individual BOB GP Practices	Sole Controller
AccuRx	Processor
British Telecommunications PLC (BTEE)	Processor
BOB ICB	Other
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?

The data processed by AccuRx are listed in:

- **Healthcare staff personal data** (typically name, role, organisation, contact details, messages, metadata, signatures, login and other application-use related data)
- **Patient data** (typically name, identifiers, contact details - mobile number and email, demographic data, message content, patient images, documents/notes, survey responses, metadata).

The video and audio communication of any video consultation is only visible to participants on the call and is not recorded or stored on any server. The IP address of all participants will be stored as part of metadata stored, however, no other personal information of call participants is collected or stored.

Data will be shared with sub-processors such as cloud services used for AccuRx's own storage, communications, security, engineering, and similar purposes. AccuRx's sub-processors operate based on Article 28 GDPR-compliant agreements. AccuRx data is encrypted in transit via HTTPS and encrypted at rest via TDE. AccuRx follows the Microsoft Azure Security and Compliant Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services.

Patients' data is kept in line with the Records Management Code of Practice for Health and Social Care. However, Accurx will follow the data controller's instructions.

All patient data is processed within the UK.

Defined procedures are in place for secure and confidential data storage and sharing, the handling of sensitive data, and information security. AccuRx primary application servers are based in UK Microsoft Azure Data Centres configured with the NHS security blueprint. Microsoft Azure is a secure cloud-hosted service where data/information is stored in compliance with NHS Digital guidance.

Some of the personal data is processed outside the United Kingdom where the Processing of Personal Data is permitted. The following table shows sub processors and where the data is processed.

Third party	Where data is processed?
Fire Text Communications Ltd UK	UK

BT Ltd UK	UK
NHS Mail UK	UK
Whereby Ltd. EEA	EEA
SendGrid Inc.	US

AccuRx uses the following Third parties for their user support functions only:

Third party	Where data is processed?
Intercom UK Ltd.	US
Active Campaign	US
TeamViewer UK Ltd.	EEA

EEA arrangements:

Whereby Ltd.

Whereby is a secure meeting room service that Accurx uses to host video consultations between healthcare and/or social care staff and their patients. No content of the call is recorded or retained by Accurx, Whereby or any other service. Technical logs are created to ensure Accurx and Whereby can monitor services. They are retained to allow Accurx and Whereby to investigate any issues with the service for up to 90 days.

Data processed through Whereby is processed in the EEA (Ireland and Luxembourg). This means the image and audio for the call, plus the metadata required to set up and maintain encrypted connection between the user's device and patient's device.

TeamViewer UK Ltd.

TeamViewer provides a software service that allows Support specialists to connect and remotely view Accurx users' screens to provide technical support. This is only used when the live or email conversation has not resolved the problem, and only with the permission of the Accurx user (they have to install TeamViewer themselves in order to proceed).

Before connection, the Accurx Support specialist will advise the user to hide any personally identifiable information that's not pertinent to the support query. No content of the viewing session is retained beyond the end of it.

TeamViewer is a company registered in Germany and it processes data under its Data Processing Agreement in accordance with the EU GDPR and the Federal Data Protection Act (a German statute).

Compliance with relevant legislation Ireland, Luxembourg and Germany are all members of the EU and therefore abide by appropriate data protection legislation (the EU GDPR legislation).

US arrangements:

Sendgrid Inc.

Sendgrid is an email campaign service provider used within Accurx to send automated account emails (e.g. 'forgot password') to Accurx users only. This means Sendgrid only has access to email addresses of staff who use Accurx. No patient data is processed using Sendgrid.

ActiveCampaign

ActiveCampaign is an email campaign service provider that is used to send out mass emails to AccuRx users only to inform them of changes in the product. Only users' names and email addresses are processed. No patient data is processed using ActiveCampaign.

Intercom UK Ltd.

AccuRx use of Intercom's platform for support services means user data is transmitted through Intercom's US-based servers. The data items that flow there include contents of messages sent between Accurx users and AccuRx support team operators; metadata of these chats; contact email addresses for those users.

Compliance with relevant legislation

AccuRx has consulted their DPO and read the ICO guidance to understand the implications of Brexit and rulings like Shrems II on their data transfers with sub-processors outside of the UK. They have conducted risk assessments of each sub-processor and engaged with them to assure transfers would continue to be compliant with relevant legislation and rulings.

Before using these sub-processors, AccuRx assess the risks involved, follow the ICO guidance and insert UK approved 'Standard Contractual Clauses' into their existing agreements. AccuRx also constantly monitor for new related compliance developments.



DTAC form - Accurx - 30-Sep-22.pdf

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 medical records and personal contact details.

Type of personal data:

1. Personal Data (relating to patients of the Data Controller):

- Patient demographic details (name; date of birth; gender)
- NHS number
- Mobile phone number
- Email address

2. Personal Data (relating to healthcare and/or social care professionals):

- Name
- Email address
- Mobile phone number
- Affiliated organisations
- Job role

3. Sensitive Personal Data

- Content of the communications with – or regarding - patients sent via the Services (which may include patient images or documents and contain data concerning health).
- Other types of data, including third party data, (which may include contents of the patient's GP Medical Record and data concerning health that may from time to time be required to provide the Services).

3.1. How are you satisfying the common law duty of confidentiality?

Reasonable expectations (please specify)

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

GP Practices to make patients aware (e.g. via registration form, privacy notice, call in screen) that they will use their mobile number and email address to send messages relating to their direct care. Patients should be informed about the agreed uses (e.g. appointment reminders, referrals, questionnaires, text results) and what to do if they do not want to receive communications by text or email.

Patient consent is taken into consideration when messaging patients and those who have not given consent are not contacted via text messages or email.

3.2. 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.

All personal data sent via AccuRx is pseudonymised and encrypted automatically. Encryption is in place whilst data is in transit and at rest. Patients are also asked to input their date of birth as identity verification before accessing the document. Documents are accessible for 28 days.

3.3. 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.](#)

3.4. Approximately how many people will be the subject of the processing?

Unknown - specific patient cohort

3.5. 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

By text

By e-mail

Face to face - Video enabled

Choose an item.

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

AccuRx links to practice clinical systems such as EMIS and System One to pull patient/s demographic data. Once the message is sent it is recorded in the patient record. Practices also gather structured information from patients which can be coded using SNOMED codes.

3.6. How will you edit the data?

Data will not be edited. Additional information may be added in the form of dates for annual reviews, blood tests needed and medication reviews all detailed in the form of a text message and email or attachment to a text message and email directly to the patient.

3.7. How will you quality check the data?

Not applicable

3.8. 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.

3.9. What training is planned to support this activity?

Those using the system have been trained in its use and the outcomes expected.

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

2.1. Are you proposing to combine any data sets?

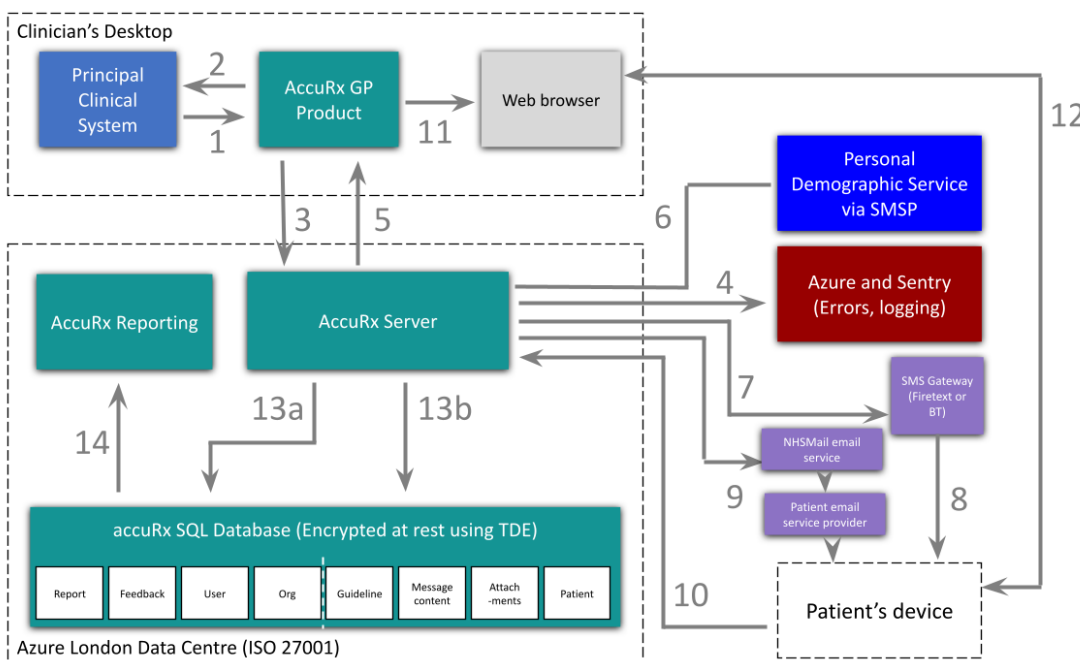
No

If yes then provide the details here.

2.2. What are the Data Flows? (Detail and/or attach a diagram if you have one).

1. Patient record entered/stored on EMIS Web or System One. Mobile phone or email address information accessed
2. Launch AccuRx which pulls in patient telephone number and name. Text detail added
3. Text is sent to patient via AccuRx using BT/EE as SMS carrier or to the NHS app
4. Emails are sent via NHS mail to recipients who will likely have emails such as Gmail, Hotmail, etc.
5. Copy of text saved in patient record in EMIS/System One
6. Usage data for monitoring purposes made available to BOB ICB via AccuRx and BTEE Soprano dashboard

DATA FLOW:



AccuRx hold the data necessary for the functioning of their platform and for audit purposes.

2.3. What data/information are you planning to share?

Information isn't shared with anyone but the patient. Patient records are all stored in Practice clinical systems such as EMIS and System One.

2.4. Is any of the data subject to the National Data Opt Out?

No - it is not subject to the national data opt out

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

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

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?

Information isn't shared with anyone but the patient. Patient records are all stored in Practice clinical systems such as EMIS and System One.

2.6. Why is this data/information being shared?

Information isn't shared with anyone but the patient. Patient records are all stored in GP Practice clinical systems such as EMIS and System One.

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

AccuRx staff cannot routinely see patient data. The message is sent by the GP practice to their patients, and it is patient choice to respond to it in the way that is convenient for them e.g. via telephone, in person or online.

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 [Click here to enter text.](#)

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

Contract is in place between BOB ICB and AccuRx, and between BTEE and BOB ICB. Practice is bound by AccuRx's Data Processing Agreement (DPA) which is published on their [website](#)

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

Monthly report on number of SMS fragments used per practice is sent from BTEE to the BOB ICB Digital, Data and Technology (DDaT) team with no patient identifiable data.

The DDaT team also has access to:

- AccuRx reporting dashboard
- BTEE Soprano reporting dashboard

Both these dashboards have no patient identifiable data.

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.

AccuRx Ltd. – 7 Curtain Road, London, England, EC2A 3LT, Company number - 10184077.




British Telecommunications PLC (BTEE) - 1 Braham Street, LONDON, E1 8EE - 01800000

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
AccuRx Ltd	Yes	ZA202115 Registered in England and Wales with company number 10184077, whose registered office is 7  Registration Certificate - Accurx.pdf Curtain Road, London, EX2A 3LT
British Telecommunications PLC (BTEE)	Yes	 Registration Certificate - BT.pdf Z5164594
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.
Click here to enter text.	Choose an item.	Click here to enter text.

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
----------------------	--

AccuRx Ltd	<ul style="list-style-type: none"> • Cyber Essentials Plus: Cyber Security Accreditation • Data Security and Protection Toolkit - Standards Exceeded • ISO27001 certified • NHS digital approved supplier
BTEE	<ul style="list-style-type: none"> • Cyber Essentials Plus: Soprano • GDPR statement • ISO27001 certified • NHS digital approved supplier <div style="display: flex; justify-content: space-around; align-items: center;"> <div style="text-align: center;">  BT GDPR Statement.pdf </div> <div style="text-align: center;">  Cyber Essentials Plus Soprano.pdf </div> <div style="text-align: center;">  ISO 27001 Certification..pdf </div> </div>
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.

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

DSP Toolkit

Name of organisation	ODS Code	Status	Published date
AccuRx Ltd	8JT17	21/22 Standards Exceeded	27/07/2023
BTEE?	N/A	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.	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?

On the practice clinical systems such as EMIS and System One as well as on AccuRx & BTEE system. Data is encrypted via the AccuRx system to allow for secure messaging. Full masking of data in place by BTEE which means the text message content is not visible to BTEE staff.

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

Access to clinical systems such as EMIS is via secure logins to windows desktop and EMIS web via smartcard/login ID.

Healthcare professionals are authenticated by requiring: NHS mail to register for an account; clinical system profiles such as EMIS, SystemOne or Vision; and an administrator at their GP practice to approve them. This is to prevent people who do not actually and currently work at the provider organisation from accessing the Accurx system.

Furthermore, patient demographic data is only pulled from clinical systems. This ensures that a healthcare professional can only access data of patients registered at their practice.

Data is routinely accessed by Practice staff, all of whom have their own password protected access. On occasion, such as for technical faults, the AccuRx staff may need to access data. The data will be deleted once the fault is resolved.

3.7 Is there any use of Cloud technology? Yes

If yes add the details here.

Used during the encryption process to protect the data in transit.

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

- Cyber Essentials Plus
- Data Security and Protection Toolkit – Standards Exceeded
- ISO27001 certified

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?

No

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

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?

BOB ICB commissioned service. Contract is in place between BOB ICB and AccuRx. Practice is bound by Accurx's Data Processing Agreement (DPA) which is published on their [website](#)

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?

Use of text messaging has been reinforced on AccuRX Privacy Notice, giving further details about encryption. <https://www accurx.com/security#faq>

4.2 How will this activity impact on individual rights under the GDPR?

No impact. The GP practice will remain the data controller of all data within the GP medical record and data held in the AccuRx system. All patient text messages and emails will be automatically copied and held on the patient record. Patients can contact the practice if they want to access information held within either system or they do not wish to receive text messages or emails.

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

Accurx is required to follow the retention schedule for GP Patient Records provided in the NHS Records Management Code of Practice for Health and Social Care 2021, which in this case, it states that patient data needs to be kept for 10 years after the data subject is deceased.

4.4 How will the data/information be archived?

Patient data along with patient images are kept in line with the Records Management Code of Practice for Health and Social Care 2021. These require AccuRx to hold records on behalf of GP practices until 10 years after a patient has died. However, AccuRx would delete the data earlier than suggested by this code if either: they receive an applicable instruction to delete it from the data controller (see below).

Or:

They are informed that the condition of Article 9(3) GDPR and s. 11(1) **Data Protection Act 2018** no longer applies: “that the circumstances in which the processing of personal data is carried out... [is] by or under the responsibility of a health professional or a social work professional”.

The patient health record in the GP Practice clinical system is archived according to NHS archiving policy.

4.5 What is the process for the destruction of records?

When the AccuRx contract comes to an end, Accurx would delete data in line with AccuRx Data Processing Agreement, after they have received written instruction from the data controller (GP Practice) and within 90 days after the contract is terminated.

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

Information only stays on EMIS and Systm One, so no impact. Data sent via AccuRx will automatically delete after 14 days.

4.7 Will you use any data for direct marketing purposes?

No

If yes please detail.

[Click here to enter text.](#)

5. Risks and Issues

5.1


What risks and issues have you identified? The DPO can provide advice to help complete this section and consider any measures to mitigate potential risks.

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 process for sending of messages is initiated by practice staff, however, in event of a system fault, AccuRx staff might see patient details when correcting the fault.	Possible	Significant	Medium
Text messages or emails may be sent to the wrong phone number or the wrong email address	Possible	Significant	Medium
Text message or emails may be sent to patient who has told you they do not wish to receive SMS messages	Possible	Significant	Medium

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 process for sending of messages is initiated by Practice staff, however, in event of a system fault, AccuRx staff might see patient details when correcting the fault.	All staff undertake annual confidentiality and data protection training AccuRx are ICO Data Protection compliant. Data Security and Protection Toolkit - Standards Exceeded	Reduced	Low	
Text messages or email may be sent to the wrong phone number /opened by the wrong recipient if patient hasn't informed us of change of address.	Privacy notice reminds patients to keep their records up to date. Practice to make use of other possible ways where appropriate to remind patients to advise if their contact details change (e.g. via call in screens, posters, prescriptions, text footer).	Reduced	Low	

	<p>Messages should not be sent to mobile telephones that are registered to more than one adult.</p> <p>Messages should not be sent to the mobile number of children over the age of 11 unless they have been deemed Gillick competent and consented for their parent/guardian to continue to receive messages on their behalf.</p>			
Text message or email may be sent to patient who has told you they do not wish to receive SMS messages	<p>Practice procedure to be in place for managing objections.</p> <p>Patient record to be coded with SMS refusal</p>	Reduced	Low	
5.3 What if anything would affect this piece of work?				
5.4 Please include any additional comments that do not fit elsewhere in the DPIA? Click here to enter text.				
6. Consultation				
6.1 Have you consulted with any external organisation about this DPIA? No If yes, who and what was the outcome? If no, detail why consultation was not felt necessary. AccuRx are already a NHS approved supplier and system was commissioned by the ICB.				
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	<p>The practice should read and adhere to risk mitigations. Procedure for dealing with patients who do not wish to receive SMS messages to be in place. Attached text guidance includes SMS refusal code details</p> <p> Guidance Texting v3.docx</p>			

<p>The practice to review and update their Information Asset Register and Data Flow Map if relevant.</p> <p>The practice to update their privacy notice. Suggested wording is provided below (this can be added to Appendix A if using the SCW privacy notice templates)</p>	
<p>Messaging Service</p>	<p>Purpose – Personal identifiable information is shared with the messaging service in order that messages including appointment reminders; results; referrals; campaign messages related to specific patients health needs; and direct messages to patients, can be transferred to the patient in a safe way.</p> <p>Legal Basis – UK GDPR Article 6 1 (b) Contract, Article 6 1 (e) Public task, Article 9 2 (h) Health data</p> <p>Provider - AccuRx</p>
<p>Having taken account of the comments and assurances received, the risks identified have been appropriately mitigated and explanations for processing outside of the UK explained. The GP DPO has also reviewed the document. On this basis as BOB ICB DPO I am assured on the project.</p>	

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

A) No unmitigated or identified risks outstanding

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 SCW CSU

Name: [REDACTED]

Job Title: Senior Information Governance Consultant

Signature: [REDACTED]

Date: 05/09/2023

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

Name: [REDACTED]

Job Title: Data Protection Officer

Signature: [REDACTED]

Date: 07/09/2023

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:

Click here to enter text.