Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

Template updated: 1st July 2024

Accurx DPIA Template: Providers of Health and Social Care using Accurx Web

This template closely follows the ICO's example of how you can record your DPIA process and outcome. It follows the process set out in the ICO's DPIA guidance, and should be read alongside that guidance and the criteria for an acceptable DPIA set out in European guidelines on DPIAs.

NB: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

If you have feedback or suggestions about how you use these documents, or suggestions on how you'd prefer like to access this kind of information in future, please email us on dpo@accurx.com.

Submitting Controller Details

Name of controller	
Subject/title of DPO	
Name of controller contact / DPO (delete as appropriate)	

Step 1: Identify the need for a DPIA

Summarise why you identified the need for a DPIA.
The aim of the service is to improve communications between healthcare staff and patients to improve outcomes and productivity. The offered features seek to expedite communication throughout the healthcare system and reduce the fragmentation of information regarding a patient's medical history, ultimately improving the quality of care. 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 audio/video consultations (which are not recorded or stored) between healthcare staff and their patients, as well as provide secure access to the patient record to the healthcare professionals involved in their care. For more information on how healthcare professionals can use the Accurx platform, see here.

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

Step 2: Describe the processing

Describe the nature of the processing: how will you collect, use, store and delete data? What is the source of the data? Will you be sharing data with anyone?

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

To use the Accurx platform, the healthcare professional:

1. Logs in with NHSmail Single Sign-on (SSO)
2. Is associated with the organisation returned from SSO
3. Is approved if the associated org matches a whitelist of NHS and social care provider organisations
    a. If healthcare professional does not have an NHSmail account, they can create an Accurx account using a verified *.nhs.uk email account from a whitelisted of NHS (or social care) provider organisation domain
4. Looks up a patient by NHS number and date-of-birth via the Accurx integration with the Personal Demographic Service (PDS)
5. Receives a return of that patient's name and gender only if the PDS search is an exact match
6. Verifies that the patient details returned are correct

Text 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.

Files and Documents

Accurx has 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.

AccuMail / Message GP

This feature enables a healthcare professional to send a message to a patient's GP practice through the Accurx platform. Typical use cases for this are to request more information about a patient, or to send more information about a patient.

Video Consult

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 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 professional's and patient's phone and follows NHS best practice guidelines on health and social care cloud security.

Record View

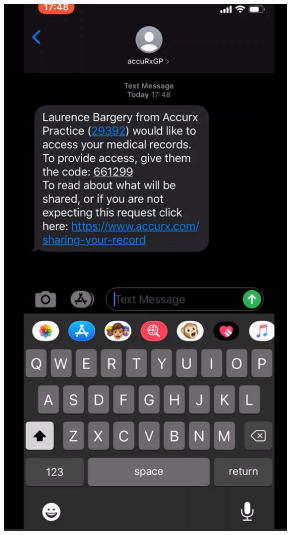
In the case of Record View the process is as follows.

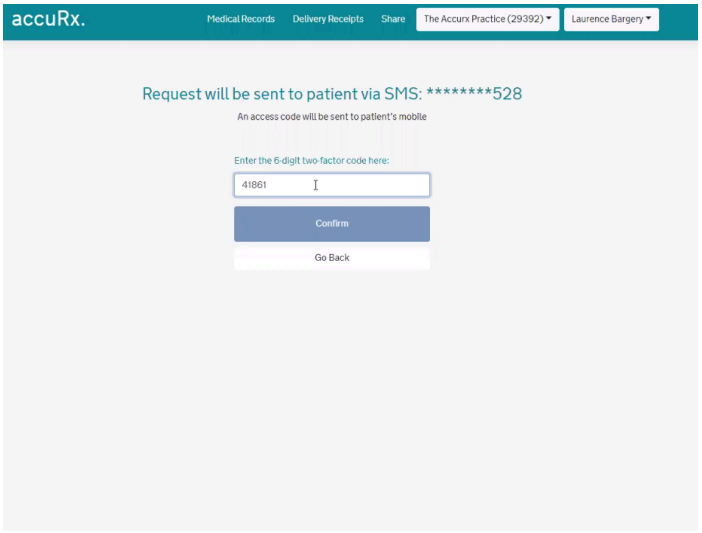
The healthcare professional using AccuRx in the provision of direct care to the patient :

1. Logs in with an approved NHSmail account via NHSmail Single Sign-on (SSO), which is integrated with the AccuRx platform
2. Looks up a patient by NHS number and date-of-birth via the AccuRx integration with the Personal Demographic Service (PDS)
3. Receives a return of that patient's name, gender, and the last three digits of the patient's mobile only if the PDS search is an exact match
4. Verifies that the details returned of the patient (whose record they would like to access) are correct
5. Requests permission for access from the patient via an SMS

The Patient:

6. Receives a unique code via SMS.
7. Multi-factor authenticates their identity - and confirms their permission for the healthcare professional to view their medical record - by verbally confirming the unique code to the healthcare professional.





The healthcare professional:

8. Inputs the code and selects 'Confirm' to then view the patient record.
9. Patient record is then available to the healthcare professional for 24 hours

PAS Integration

Accurx currently integrates with the trust PAS (Patient Administration System) and pull out key details such as demographic/appointment data which we display within our patient lists feature in Accurx Web. This could be a patient on a PIFU pathway being pulled into a list so their pathway can be managed easily, or a clinician having a live feed of the video consultations they are due to have directly in Accurx Web.

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

Quick Launch Integration

Quick Launch is a lightweight EPR integration which allows users to jump straight into Accurx Web, with the patient they had open in their EPR already open in Accurx Web. There is also the option of coupling it with their existing Azure AD authentication to allow the user to seamlessly log into Accurx Web when they open it using the Quick Launch button.

Describe the scope of the processing: what is the nature of the data, and does it include special category or criminal offence data? How much data will you be collecting and using? How often? How long will you keep it? How many individuals are affected? What geographical area does it cover?

The data processed by Accurx is:

- Healthcare staff data (typically name, role, organisation, contact details, identifiers including gender and DoB, 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, medical record, 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 call participants is stored for 90 days as part of technical logs (something Accurx believes to be necessary to assist practices investigating problems with a meeting).
- No other personal information of call participants is collected or stored.

Patients' data is generally kept in line with the Records Management Code of Practice for Health and Social Care 2016. However, Accurx would delete the data earlier than suggested by this code if they were informed that the condition of Article 9(3) GDPR and s. 11(1) Data Protection Act 2018 no longer applies.

Accurx retains the data pertaining to their clients' and prospects' medical teams' members and to non-medical personnel actually or potentially involved in purchasing their services for as long as necessary for the purpose of providing the service, to pursue a sales transaction, or to market their services, subject to the the right to object or not to be subject to direct marketing. Healthcare professionals may contact Accurx (support@accurx.com) to request that Accurx delete the data held about them.

Data may 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. See here and here for further information. Accurx communicates with users about changes to the Accurx service and to let them know about new features that their organisation may be able to access. Users always have the option to unsubscribe from any or all emails, which removes them from all but critical account updates.

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

AccuMail / Message GP (detailed)

When sending an email to a patient's GP practice, the healthcare professional will not be able to see an individual's email address, only the name of the GP practice that they wish to contact. The relevant GP practice is linked to the patient's NHS number and Date of Birth in the Accurx database. The sender ID for sent messages is shown as the healthcare professionals nhs.net email address. All replies from the GP are received to the healthcare professional's NHS Mail inbox and/or to their in product Inbox (depending on whether they have the feature or not).

Video Consultation (detailed)

A unique URL to the video consultation is generated and all participants are visible in the consultation, no third party can 'listen in'. The video and audio communication of the video consultation is only visible to participants on the call, and is not recorded or stored on any server (not Accurx's, not Whereby's and not on any third party's servers). Whereby are based in the European Economic Area (EEA). All communication between the healthcare professional's browser, or the patient's browser, and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure websocket traffic or secure WebRTC). Furthermore, the video consultation connection prioritises 'peer-to-peer' connections between the clinician's and patient's phone over connections via their servers. In some cases, due to NAT/firewall restrictions, the encrypted data content will be relayed through Whereby's TURN server, but never recorded or stored. In such cases, as long as both the clinician and patient are using their computer devices in the European Economic Area, it is guaranteed that any data hosted on a server is within the EEA in line with NHS best practice guidelines on health and social care cloud security.

Record View (detailed)

As the Data Processor, AccuRx will store a copy of the patient record for the time laid out above but no longer than that. No data is held locally on the GP's desktop. All data processed from the GP patient record is encrypted in transit via HTTPS and encrypted at rest via TDE in AccuRx's Microsoft Azure servers for up to 7 days only. The data processed from the GP patient record is then removed from AccuRx's servers (either after 24 hours from the link described being first activated, or 7 days from the link being sent).

The only data stored thereafter is metadata to provide an audit trail for General Practice staff, such as who accessed which records when.

In line with the principle of data minimisation, only data necessary for the provision of direct care is displayed. Record View will provide Health and Care Professionals with the information they need to effectively treat patients from the Record.

This will include:

- Patient details (Name, DOB, Address, NHS number)
- GP registration details
- Problem list (current and significant past problems)
- Medications (current, repeat, recent acute medications)
- Allergies
- Investigations during the last two years
- Immunisations
- Health status (smoking, alcohol, BMI)
- Information not necessary for this purpose will be excluded from Record View:

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

Patients with records set to sensitive status (referred to as "S" flagged) on the NHS Personal Demographic Service will not be available to view and will not be returned or requested.

PAS Integration (Detailed)
Healthcare orgs will send us a HL7 feed from which we can pick up the information that is useful to us, and discard the rest. This information is then displayed to an Accurx Web user in the form of a list, from where they can easily communicate with the patient. Demographic data (Full name, D.O.B., NHS number, Gender, Address) Appointment data (Date, time, clinician, type of appointment, PIFU tag, clinic details)

Quick Launch Integration (Detailed)

Quick launch is a 2-step process. In the first step, the trust's system sends to Accurx patient demographics which we then encrypt on the fly and return in the form of a url with a token. In the second step, the trust's system launches that URL in the browser where Accurx decrypts the token from step 1 in order to populate the NHS number and DoB for PDS search. None of the data passed to Accurx by the trust's system is stored.

The request passed to us by the trust holds the patient's NHS number and D.O.B. as that is what is required for us to be able to do a PDS search. It also contains a client ID and password to authenticate the client (the trust in this case). In case of Azure AD integration we also receive user's email, name and upn (which is user's universal identifier in the context of their org). We use the email and name for registration and login and at the moment we discard the upn.

For George Eliot only, we've carried out an integration in which we are provided the users email and name from their EPR itself and we use this to log them in. We've only done this for GEH and won't be doing this for trusts going forward, instead opting for the AD integration detailed above.

Describe the context of the processing: what is the nature of your relationship with the individuals? How much control will they have? Would they expect you to use their data in this way? Do they include children or other vulnerable groups? Are there prior concerns over this type of processing or security flaws? Is it novel in any way? What is the current state of technology in this area? Are there any current issues of public concern that you should factor in? Are you signed up to any approved code of conduct or certification scheme (once any have been approved)?

The nature of the relationships with the individual is that of health and social care staff providing direct care to patients.

The nature of the relationships with the individuals participating in any video consultations is identical to that of face-to-face consultations between healthcare professionals and their patients. 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 use of video consultation via Accurx is more secure than speaking to patients by phone. The connection prioritises 'peer-to-peer' between the healthcare professional's and patient's phone in line with the principle of data minimisation. Most phones are Voice over Internet Protocol (VoIP). However, phone connections typically include personal information (such as patient phone number). In contrast, the Accurx video

consultation does not use any personal demographic information as it is initiated via a unique URL which does not use any patient or healthcare professional information. Accurx specifically selected Whereby services to host video consultations because it fulfilled Accurx privacy by design requirements in not using any personal demographic data for the calls.

The ability to contact a patient's GP practice via the Accurx platform is intended to improve the existing methods of communication that exist between secondary and primary care. This method is more secure and efficient than current processes, which may include dictating letters or calling up GP practices on the phone.

Similarly, the processing of the patient record on AccuRx is actually more secure than existing methods. These include: GPs printing out relevant pieces of the record for home visits; hospital doctors requesting the GP medical record via phone (with no identity verification); and, components of the GP medical record being sent via email without a retention time limit.

On AccuRx the healthcare professional must login with an NHSmail account via Single Sign On which returns an organisation that matches an whitelist of NHS organisations providing direct care (approved by the NHSD PDS team) and agree to an acceptable use policy. Furthermore, the healthcare professional will be asked to confirm that they would like to request access to the patient record before they do so.

Describe the purposes of the processing: what do you want to achieve? What is the intended effect on individuals? What are the benefits of the processing – for you, and more broadly?

The purpose of using the Accurx platform is for healthcare staff to communicate with patients and with each other regarding patients for the provision of healthcare or social care services.

The purpose of accessing the patient record is to reduce the fragmentation of information regarding a patient's health history and to enable all health and social care providers to improve the quality of care offered to that patient. The solution directly addresses the Long Term Plan goals to: *"Ensure that clinicians can access and interact with patient records and care plans wherever they are"; and, "Protect Patient's privacy and give them control over their medical record"*.

Step 3: Consultation Process

Consider how to consult with relevant stakeholders: describe when and how you will seek individuals' views – or justify why it's not appropriate to do so. Who else do you need to involve within your organisation? Do you need to ask your processors to assist? Do you plan to consult information security experts, or any other experts?

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

For the main platform, views have been gathered from Accurx users across c.7000 GP practices and 150 Trusts. Over 2 million video consultations have been completed to date. Accurx has also engaged patients and CCIOs on its Information Governance and Data Protection approach.

For Record View, views have been gathered from over 30 GP interviews and product demonstrations, all of whom wanted immediate access to the new feature. 5 GPs piloted the solution for access to their own patient records only. Feedback has been overwhelmingly positive.

In addition, there has been consultation with all of the following bodies who have seen a demo of AccuRx's solution and presentation on the IG approach - all of whom have given either excellent feedback or no negative feedback: National Data Guardian; Royal College of General Practitioners; British Medical Association; Joint GP IT Committee; and, Joint GP IT Liaison Committee.

The full text of the National Data Guardian's letter, that specifically addresses the fact that there is no need for Data Sharing Agreements, is available here.

Patient research has shown that many assume that data sharing of this kind goes on, they are surprised to be informed that the content of the GP record is not something easily accessed within other settings, and so they are well-disposed to helping facilitate that access through the permission they provide in Record View.

Step 4: Assess necessity and proportionality

Describe compliance and proportionality measures, in particular: what is your lawful basis for processing? Does the processing actually achieve your purpose? Is there another way to achieve the same outcome? How will you prevent function creep? How will you ensure data quality and data minimisation? What information will you give individuals? How will you help to support their rights? What measures do you take to ensure processors comply? How do you safeguard any international transfers?

The lawful bases of healthcare staff using the Accurx platform for communicating with patients is the **provision of health care or social care services:**
6(1)(e) '...necessary for the performance of a task carried out in the public interest or in the exercise of official authority...'.
9(2)(h) '...medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems...'

Accurx has successfully completed NHS Data Security and Protection Toolkit assurance (under NHS ODS code 8JT17), and both the Cyber Essentials and Cyber Essentials Plus certification. Cyber Essentials is a scheme run by the UK government and the National Centre for Cyber Security to help you know that you can trust your data with a given supplier. 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 follow the Microsoft Azure Security and Compliance Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services.

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

SMS Messaging

Healthcare professionals are authenticated by being required to logon via NHSmail Single Sign-on (SSO) and having their associated organisation (in SSO) matched to a whitelist of NHS (or social care) provider organisations. This is to prevent people who do not actually and currently work at the provider organisation from accessing the Accurx system.

Healthcare professionals have to agree to an acceptable use policy that includes confirming that the service only be used: for the purposes of direct care; with the approval of their healthcare organisation; and, to not use the SMS messaging feature to communicate messages that are sensitive or clinically urgent messages. Full audit trails are kept of all searches and uses of the PDS integration.

Healthcare professionals can only access patient data via the Accurx integration with the Personal Demographic Service (PDS) if they either have the patient's NHS number and date-of-birth, or the patient's full name, gender, birthdate and postcode. To ensure accuracy and data minimisation, the only data returned is that patient's name, gender and the last three digits of the patient's mobile. This means that the healthcare professional has the minimum information to verify that this is the correct patient.

Files and Documents

Links to files or documents sent via SMS by healthcare staff directly to a patient's mobile phone are encrypted in transit via HTTPS and responses are encrypted at rest via TDE. Patients are also asked to input their date of birth as identity verification, before being able to access the document. The document is only accessible for 28 days.

AccuMail / Message GP

Healthcare professionals are able to send an email to a patient's GP practice through the Accurx platform. They are only able to do this if the patient's GP practice is currently also using the Accurx platform. The email will be sent to the practice inbox, rather than an individual's inbox.

Video Consultation

Accurx is an NHS Digital approved video consultation provider. The video consultation feature is used in the context of a healthcare professional providing direct care for a patient, as specified by the Acceptable Use Policy. The patient must consent to take part in the process of a video consultation by clicking on the link to join it. They can dissent at any point by either not clicking on the link or by leaving the video consultation.

The video and audio content of the consultation is not retained by either Accurx or Whereby. De-identified usage metadata is retained for service evaluation and improvement. It is the responsibility of the healthcare professional to record the relevant information from the consultation as they would in a face-to-face consultation.

All communication between the healthcare professional's browser, or the patient's browser, and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure websocket traffic or secure WebRTC). No demographic information (such as names of the participants) is collected or stored by Whereby.

Record View

Record View has been developed in response to significant demand from Health and Care Professionals for an efficient way to access the information in Records when providing direct care to a patient.

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

Traditional ways of sharing records - like GPs printing off copies for home visits, clinicians requesting records over the phone with no identity verification, and sending parts of records by email - are unreliable and unsecure.

Existing solutions, such as Summary Care Records ("SCRs") and Local Health and Care Record Exemplars ("LHCRs") have partially helped, but they are hamstrung by constraints (such as dependence on NHS smartcards), lacking awareness of how to access them and limited information available in the record.

Record View aims to address these. Firstly, Record View guarantees ease of access to the Record for Health and Care Professionals by putting patient permission at the heart of the product. Secondly, Record View delivers a more comprehensive set of information, including the patient's immunisation history, the last 2 years' worth of investigations and health status (BMI, smoking and alcohol history).
More broadly, Record View chimes with the NHS Long Term Plan goals to "ensure that clinicians can access and interact with patient records and care plans wherever they are" and "protect patients' privacy and give them control over their medical record" as well as the Caldicott Principle of sharing information when doing so is in the best interests of the patient.
Overall, by providing an alternative way for Health and Care Professionals to view patients' Records, Record View seeks to offer an alternative mechanism for enhancing connectivity between parts of the healthcare system and improving the quality of patient care.

Please also see below for an assessment of compliance against the principles of the Data Protection Act:

Principle	Assessment of Compliance
Principle 1 – (2.21 2.23) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met	Personal data is processed under the lawful basis of the provision of health care or social care services.
Principle 2 – (2.2) Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.	The data is processed in line with the lawful basis above and limited by the instructions given by the data controller to Accurx as a data processor (see the Accurx Data Processing Agreement).
Principle 3 – (3.1) Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed.	Personal data processing in the Accurx platform is completed at the instruction of the data controller only, in line with the organisations' decisions and the actions of the professionals that work for it. Insofar as these professionals are complying with their obligations under UK law and the Caldicott Principles, then processing shall be adequate and minimised.
Principle 4 – () 2.12 Personal data shall be accurate and, where necessary, kept up to date.	Accurx platform users have the ability to modify data, such as contact information. Accurx will react to any instructions to rectify or update any data that is not modifiable by the user through support@accurx.com
Principle 5 – (2.20) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.	The retention period of communications sent in the Accurx platform is set in line with Records Management Code of Practice. Accurx will delete information sooner if instructed by the data controller (we apply the NHS Digital GP IT Futures standard to verifying requests to delete data) or where otherwise legally required to (e.g. due to a court order).
Principle 6 – (2.22& 2.23) Personal data shall be processed in accordance with the rights of data subjects under this Act.	Accurx is committed to promptly assisting data controllers to comply with subject access requests and other actions needed to

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

	uphold data subjects' rights (described in Accurx's Data Processing Agreement).
Principle 7 – (2.13 2.14 2.16 2.17 2.18) Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.	Computer equipment in the provider is expected to be secure and complies with the NHS Data Security and Protection Standards, as all NHS organisations are required to - or some similar standard if the provider is outside the NHS. Accurx as a supplier has successfully completed ISO27001 certification, has completed the NHS Data Security and Protection Toolkit assurance (under NHS ODS code 8JT17), and the Cyber Essentials Plus certification. Accurx data is encrypted in transit via HTTPS and encrypted at rest via TDE. A full set technical measures are linked in the Accurx Data Processing Agreement and certificates and credentials are on accurx.com.
Principle 8 – (2.15) Personal data shall not be transferred to a country or territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.	Accurx uses UK data centres for cloud processing only. It follows the Microsoft Azure Security and Compliant Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services. Accurx uses some sub-processors outside the EEA for the purposes of providing online support to its users, and takes measures to minimise and remove any incidental patient data that is processed via these routes. All transfers are conducted under a legal mechanism and additional security measures implemented. The latest description of sub-processors can be found in the Accurx DPA. However, we draw your attention to the fact that that: a healthcare professional who uses Accurx to process patient data using a computer outside of the UK/EEA may result in the data being processed outside of the UK/EEA; a patient may be receiving messages whilst outside of the UK/EEA.

Step 5: Identify and assess risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary. **Note that these are only examples of risks that have been identified. Accurx does not take responsibility for this list being comprehensive.**

Use of the Accurx Platform - Risks

Risk	Likelihood of harm	Severity of harm	Overall risk
Access to Personal data by persons other than the data subject	Low	Significant	2 - Low
Incorrect patient data selected for SMS	Low	Significant	2 - Low
Sensitive data being sent via SMS	Medium	Significant	2 - Low
	Low	Significant	2 - Low

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

A healthcare professional uses the platform for a patient not under their direct care			
A healthcare professional stays logged in so that someone else could use the service under their login	Medium	Significant	2 - Low
Abusive messages are sent to patients by a healthcare professional	Low	Significant	2 - Low
The integrity of the computers used (how at risk are they from trojans or viruses)	Low	Minor	2 - Low

Files and documents - Risks

Risk	Likelihood of harm	Severity of harm	Overall risk
A user inadvertently attaches the wrong document to the message sent to a patient	Medium	Significant	2 - Low
A patient has successfully received the SMS with the document link. When they try to open the link, they are unable to open it	Medium	Significant	2 - Low
A document intended for a patient is opened by someone else	Low	Significant	2 - Low
A patient is unable to open a document after their link has expired	Medium	Significant	2 - Low

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

AccuMail / Message GP - Risks

Risk	Likelihood of harm	Severity of harm	Overall risk
Healthcare professional is not notified of a message not being delivered	Medium	Significant	2 - Low
Healthcare professional is unable to access GP response, resulting in harm to patient	Low	Significant	2- Low
GP does not realise that they have received a healthcare professional initiated message	Low	Significant	2- Low

Video Consultation - Risks

Risk	Likelihood of harm	Severity of harm	Overall risk
The healthcare professional would need to ensure that there was no third-party data visible on desks or screens that could be viewed or captured by the individual in any video call	Low	Minor	2 - Low
A third party is present in the room of one of the video consultation participants without the other participant knowing	Low	Significant	2 - Low
A third party guesses the URL of a video consultation and joins the call	Very Low	Significant	2 - Low

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

Record View - Risks

Risk	Likelihood of harm	Severity of harm	Overall risk
Access to Personal data by persons other than the data subject	Low	Significant	2 - Low
Healthcare professional requests record for wrong patient	Low	Significant	2 - Low
Healthcare professional requests access for a patient not under their direct care	Low	Significant	2 - Low
Patient unable to grant access (e.g. critically unwell)	Medium	Minor	2 - Low
Record View approval is granted by persons other than the data subject	Very low	Significant	1 - Very Low
MFA/unique URL expires prior to patient approval	Medium	Minor	2 - Low
SMS fails to deliver	Medium	Minor	2 - Low
Incorrect telephone number pulled from PDS	Low	Significant	2 - Low

PAS Integration - Risks

Risk	Likelihood of harm	Severity of harm	Overall risk
More patient data than is necessary is captured and stored on the Accurx platform	Low	Significant	Low
Incorrect or mismatched data is pulled from the patient record and displayed in the patient lists on Accurx Web.	Low	Significant	Low
Data exposed in transit via PAS integration	Low	Significant	Low
Too much data is retained from the PAS integration	Low	Significant	Low

Quick Launch Integration - Risks

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

Risk	Likelihood of harm	Severity of harm	Overall risk
Incorrect data or mismatched data is passed over causing an error	Medium	Significant	Medium

Step 6: Identify measures to reduce risks

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5. Note that these are only examples of risks that have been identified. Accurx does not take responsibility for this list being comprehensive.

Use of the Accurx Platform - Measures to reduce risk

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Access to Personal data by persons other than the data subject	Healthcare professionals are either authenticated by being required to logon via NHSmail Single Sign-on (SSO) and having their associated organisation (in SSO) matched to a whitelist of NHS (or social care) provider organisations; or they have a whitelisted provider organisation address. The PDS search (NHS no and DoB) must return an exact match, so a healthcare professional could not put in random NHS numbers, or search for a patient by name. The only personal data returned from PDS is the name, gender, and last three digits of the mobile number. Name is used to personalise the message and to confirm that the correct patient is chosen. An individual in possession of the NHS no. and DoB would also be in possession of the name and gender. Name, DoB, gender and NHS no. make up the standard set	Reduced	Low	❑

	of demographics. The mobile number is obfuscated except for the last three digits, so that the number can be verified with the patient or another system. Full audit trails are kept of all searches and uses of the PDS integration. Any video consultations are not recorded or stored. Patients flagged as a safeguarding risk on PDS will not be returned in the search.			
Incorrect patient data selected for SMS	Healthcare professionals need to have both the patient's NHS number and date-of-birth to return that patient's name, gender and the last three digits of the patient's mobile. This means that the healthcare professional has the minimum information to verify that this is the correct patient.	Reduced	Low	❑
Sensitive data being sent via SMS	Healthcare professionals have to agree to an acceptable use policy that includes confirming that the service not be used to communicate SMS messages that are sensitive or clinically urgent messages. Full audit trails are kept of all searches and uses of the PDS integration.	Reduced	Low	❑
A healthcare professional stays logged in so that someone else could use the service under their login	The user sessions will be reduced to 12 hours to reduce the likelihood of someone else accessing an open user session. A healthcare professional will be automatically logged out after 12 hours.	Reduced	Low	❑

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

Abusive messages are sent to patients by a healthcare professional	Accurx scans SMSs for abusive content and flags to its Clinical Lead if any are detected. Full audit trails are kept of all healthcare professional activity for clinical safety purposes.	Reduced	Low	❑
The integrity of the computers used (how at risk are they from trojans or viruses)	Use of devices that comply with NHS standards of encryption.	Reduced	Low	❑
A healthcare professional uses the platform for a patient not under their direct care	This is specifically prohibited in the Acceptable Use Policy that all users acknowledge when using Accurx Web for the first time. Audit trails are maintained to allow orgs to investigate misuse of this kind.	Reduced	Low	

Files and documents - Measures to reduce risks

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
A user inadvertently attaches the wrong document to the message sent to a patient	A patient can call the practice if they feel a document sent to them is not fitting with what they expected The file picking UI is the windows file explorer so they will be used to this. Once a file is attached, a new UI element appears showing that a file has been attached alone with the file name and extension Once a file is attached, a cross is present if the user wants to remove the attachment	Reduced	Low	❑
A patient has successfully received the SMS with the document link. When they try to open the link, they are unable to open it	1,2,3) A patient can contact their practice if they are unable to view a document 2) Many smartphones will automatically select the appropriate app to open a file depending on its type	Reduced	Low	❑

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

A document intended for a patient is opened by someone else	1,2) The link is sufficiently long such that it is unlikely a user will be able to 'guess' a URL. It would also be difficult for a user to quickly see the URL on a patient's phone and remember it. 1,2) If an unintended party has obtained the URL, there is a further verification step where the patient's date of birth needs to be entered 1,2) The URL expires automatically after 28 days to further reduce risk of unintended viewing	Reduced	Low	❑
A patient is unable to open a document after their link has expired	TBC	Reduced	Low	❑

AccuMail / Message GP - Measures to reduce risks

Risk	Options to reduce or eliminate risk	Effect on risk	Residual Risk	Measure approved
Healthcare professional is not notified of a message not being delivered	Failed delivery receipts will be available in the Accurx ChainWeb Dashboard' where users view delivery receipts for SMS.	Reduced	Low	❑
Healthcare professional is unable to access GP response, resulting in harm to patient	Only users with an NHS mail account can use this feature and it is reasonable to expect that they will check their NHS mail inbox as part of their regular workflow, this is also currently how a healthcare professional may receive a message from the GP.	Reduced	Low	❑
GP does not realise that they have received a healthcare		Reduced	Low	❑

professional initiated message	Healthcare professionals can only send a message to GPs who are already using (and therefore understand) the Accurx email feature. The GP will receive a notification saying that they have received an email. All approved users are able to access the practice email inbox and see when a reply has been received. A healthcare professional will not be able to initiate a message into a GP practice if the practice is not using Accurx and will see the following message 'this feature is not available for this patient.'			

Video Consultation - Measures to reduce risks

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
The healthcare professional would need to ensure that there was no third-party data visible on desks or screens that could be viewed or captured by the individual in any video call	Healthcare professionals can view what the patient views in the video consultation. Therefore, any third-party data could be identified and blocked by the healthcare professional.	Reduced	Low	❑
A third party is present in the room of one of the video consultation participants without the other participant knowing	Participants can ask the other participant to scan the room with the camera if either are concerned.	Reduced	Medium	❑

A third party guesses the URL of a video consultation and joins the call	The URLs generated use the same approach as encryption so they are statistically impossible to guess. If a third party managed to defy those odds, the other participants would know immediately that someone else has joined the consultation such that they can end the call before any breach of sensitive data.	Reduced	Low	❑

Patient Response - Measures to reduce risks

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
A patient attempts to respond to the professional's question by texting back rather than following the link	If a patient does not respond to an important query, the clinician can still contact them through usual methods such as a phone call. Many phones do not allow reply e.g. Android 10 disables any text input and displays the message "Sender doesn't support replies". iOS 13 allows text input but provides a failure message "Not Delivered" along with a red "!" icon. The SMS sent to the patient contains the message "To respond, please follow this link: ..." The SMS sent to the patient contains the message "please do NOT text back a reply to this message".	Reduced	Low	❑
A patient is unable to respond due to not being able to open the link	1,2) A patient can contact the professional using usual methods e.g. telephone 1,2) A user can contact the patient using usual methods e.g. telephone	Reduced	Low	❑

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

	1) A patient can open the link on their computer browser and respond using this. In the initial SMS sent to the patient, we have the message "if you do not have access to the internet..."			
A patient enters a clinically urgent response to a user's question	The nature of the response is likely to be aligned to the question asked by the user/clinician. They will use clinical judgement to assess whether a question is best asked face-to-face vs telephone vs single patient response. If a patient is concerned, they can still contact the professional using existing methods e.g. telephone call. Following submission of the answer, the patient is informed "Your response may not be viewed immediately. For urgent queries, please call reception".	Reduced	Medium	❑
A user does not see the patient response	This is mitigated against because the response is delivered to the NHS Mail inbox of the user, and this is made clear to them next to the Patient Response toggle: "The patient's response will come back to [user email address]"	Reduced	Low	❑

Record View - Measures to reduce risks

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
Access to Personal data by persons other than the data subject	Healthcare professionals are either authenticated by being required to logon via NHSmail Single Sign-on (SSO) and having their associated organisation (in SSO) matched to a whitelist of NHS (or social care) provider organisations; or they have a whitelisted provider organisation address.	Reduced		

	The PDS search (NHS no and DoB) must return an exact match, so a healthcare professional could not put in random NHS numbers, or search for a patient by name. The only personal data returned from PDS is the name, gender, and last three digits of the mobile number. Name is used to personalise the message and to confirm that the correct patient is chosen. An individual in possession of the NHS no. and DoB would also be in possession of the name and gender. Name, DoB, gender and NHS no. make up the standard set of demographics. The mobile number is obfuscated except for the last three digits, so that the number can be verified with the patient or another system. Full audit trails are kept of all searches and uses of the PDS integration. The patient's GP will have access to an audit trail of: which healthcare professionals requested access to their patient's record, when and from what organisation. Healthcare professionals cannot send the MFA SMS to a number other than that returned directly from the PDS search.			
Healthcare professional requests record for wrong patient	In the SMS sent to the patient that includes the unique code, there is an alert to say "If this is unexpected, please click [on link]." The link will alert the healthcare professional that	Reduced		

	the wrong patient has been contacted. The healthcare professional can only request a record once they have entered both that patient's NHS number and date-of-birth via the AccuRx integration with the Personal Demographic Service (PDS). They only receive a return of that patient's name, gender, and the last three digits of the patient's mobile only if the PDS search is an exact match. This enables them to verify that the details returned of the patient (whose record they would like to access) are correct.			
Healthcare professional requests access for a patient not under their direct care	The healthcare professional can only gain access to the patient record with the explicit permission of the patient. The patient must actively inform the healthcare professional of the unique code they have received verbally.	Reduced		
Patient unable to grant access (e.g. critically unwell)	In instances where the patient is incapacitated and cannot tell the healthcare professional their unique code, the healthcare professional can directly message the GP practice of the patient via AccuRx to request the patient information they need to deliver the appropriate care.	Reduced		
Record View approval is granted by persons other than the data subject	Patient approval to access the record is granted via MFA. Mobile numbers of patients in PDS are updated within 24 hours of it being changed in their GP's system. If the healthcare professional is concerned about this risk, they can ask the patient to	Reduced		

	verbally submit the unique code in person or via AccuRx's video consultation feature.			
MFA/unique URL expires prior to patient approval	The healthcare professional will be able to send a new code to the patient should the original code expire.	Reduced		
SMS fails to deliver	AccuRx provides the healthcare professional with failed delivery receipts so that they are made aware when an SMS is not delivered.	Reduced		
Incorrect telephone number pulled from PDS	Mobile numbers of patients in PDS are updated within 24 hours of it being changed in their GP's system. The healthcare professional can double check with patients if the number pulled from PDS matches that of their correct mobile phone number. In the SMS sent to the patient that includes the unique code, there is an alert to say "If this is unexpected, please click [on link]." The link will alert the healthcare professional that the wrong patient has been contacted. The accuracy in PDS has not been an issue in the 2m video consultations AccuRx have completed (using PDS) to date. In the exception where the number is inaccurate, the patient will not receive the code but there is no breach of data. As the code is verbally confirmed, the clinician cannot access the record.	Reduced		
The integrity of the computers used (how at risk are they from trojans or viruses)	Computer equipment is secure and complies with the NHS standard for encryption. AccuRx has successfully completed NHS Data Security and Protection Toolkit	Reduced		

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

	assurance (under NHS ODS code 8JT17), and both the Cyber Essentials and Cyber Essentials Plus certification. AccuRx data is encrypted in transit via HTTPS and encrypted at rest via TDE.			
Third party access to unique code.	Access to the unique code is only possible if the third party has access to the patient's mobile. The patient's special categories of data is not a risk of being exposed to that third party however, as only the healthcare professional can view the record.	Reduced		

PAS & Quick Launch Integration- Measures to reduce risks

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
PAS: More patient data than is neccessary is captured and stored on the Accurx platform	Accurx is only picking up the information relevant to us, any data that is not being directly used by us for the product is not persisted. It is never stored in any kind of database and is not stored in our audit logs either	Reduced	Low	Yes
Data exposed in transit via PAS integration	The PAS connection is made via the HSCN. Mutual TLS is also used to securely authenticate the client and server to each other, and an additional authentication header is used.	Reduced	Low	Yes
Too much data is retained from the PAS integration	To ensure unneeded data is not inadvertently stored, the raw data Accurx receives is filtered, and only the required data is retained - the rest is permanently discarded.	Reduced	Low	Yes

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

Quick Launch: Incorrect or mismatched data is pulled from the patient record and displayed in the patient lists on Accurx Web.	Accurx platform would fallback to the default page, where users then have to search for the patient manually to ensure they have the right patient	Reduced	Low	Yes

Step 7: Sign off and record outcomes

Item	**Name/position/date**	**Notes**
Measures approved by:		Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:		If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:		DPO should advise on compliance, step 6 measures and whether processing can proceed
Summary of DPO advice:		
DPO advice accepted or overruled by:		If overruled, you must explain your reasons
Comments:		
Consultation responses reviewed by:		If your decision departs from individuals' views, you must explain your reasons
Comments:		

Please note: As the data controller, when using Accurx, it is up to your organisation to complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of this DPIA Template.

This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA