accuRx DPIA Template: GP Practices and other providers using accuRx Desktop

Submitting Controller Details

Name of controller	T HODSON
Subject/title of DPO	Use of AccuRX at the surgery
Name of controller contact / DPO (delete as appropriate)	Thomas.hodson1@nhs.net

Step 1: Identify the need for a DPIA

Summarise why you identified the need for a DPIA.

The aim of the accuRx platform is to improve communications between healthcare staff and patients to improve outcomes and productivity.

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.

Please see here for demonstrations of all the features in accuRx Desktop.

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

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.

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

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.

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.

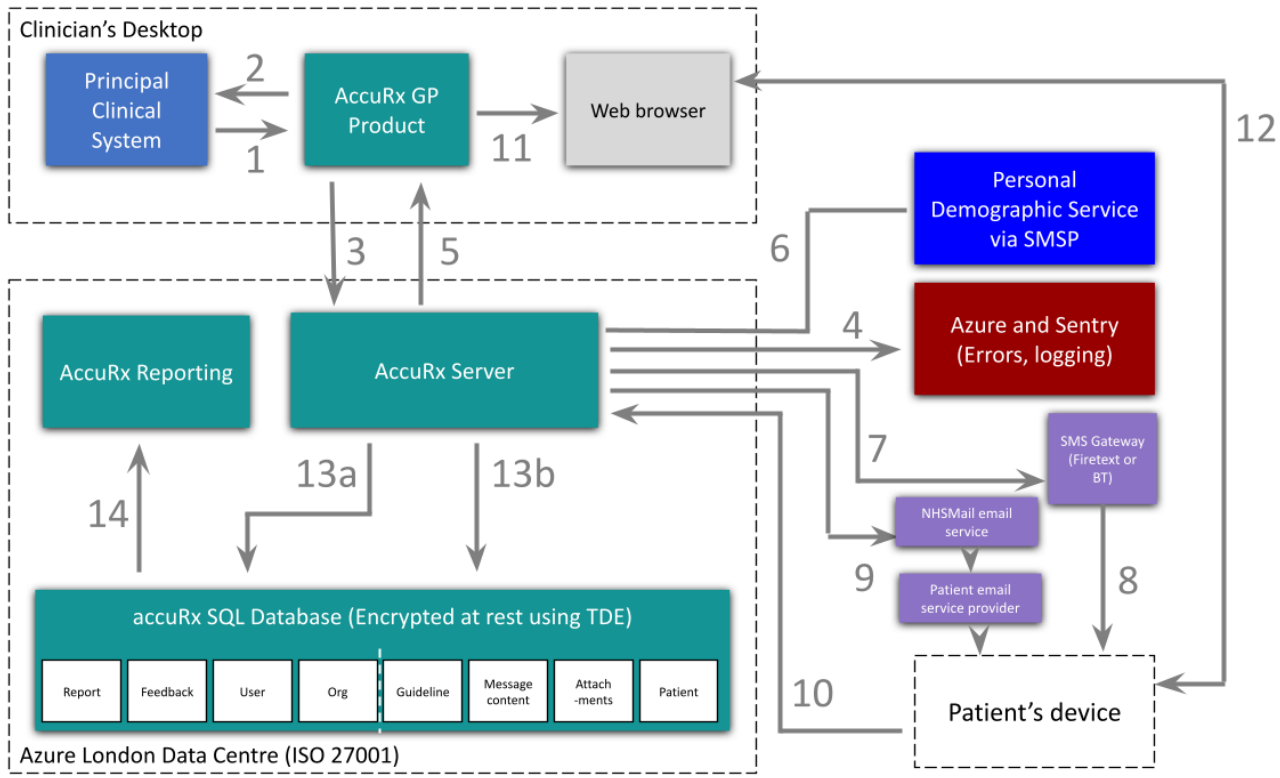
Patient images received can be "logically" deleted: i.e. resulting in the underlying data being marked in such a way that it is no longer visible to any user of the record.

accuRx follows NHS Digital IG requirements, which require them to keep a photo for audit trail purposes, even if the user has deleted the file within accuRx. accuRx can only physically (i.e. permanently and completely) delete a photo from the audit trail that they hold in response to a validated instruction from the data controller or to court orders or other legislative circumstances. A validated instruction for physical deletion of any communication using accuRx (including photos) requires the signature of an organisation's Caldicott Guardian or Privacy Officer, co-signed by a senior clinical representative, in line with GP-IG-11-4 in the NHS Digital IG requirements.

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.

accuMail
accuMail allows GPs to communicate with other healthcare professionals via email, about their patients' care.

Data Flows



Number	Data description	Data processed	Method of processing
1	**Principal Clinical System** to **AccuRx GP Product**	• Patient demographic details (name; date of birth; gender; NHS number; mobile number; email address) • User ID • User Role (GP, nurse etc) • Organisation (Practice details)	IM1 API (local to machine)
2	**AccuRx GP Product** to **Principal Clinical System**	• Patient demographic details (name; date of birth; gender; NHS number; mobile number; email address) • Content of the communications with – or regarding - patients sent via AccuRx (which may include patient images or documents)	IM1 API (local to machine)
3	**AccuRx GP Product** to **AccuRx Server**	• Patient demographic details (name; date of birth; gender; NHS number; mobile number; email address) • Content of the communications with – or regarding - patients sent via AccuRx (which may include patient images or documents) • User ID; User Role (GP, nurse etc); Organisation (Practice details) • Feedback from clinicians (with user and organisation) • Report (tool open/close, advice used, workflow started etc)	Https with 30 character authentication key installed into machine registry by admin at practice
4	**AccuRx Server** to **Azure and Sentry**	• Errors, exceptions, logs (from Principal Clinical System or Chain, to increase stability)	Https to accuRx specific Azure and Sentry (Slack API URL)
5	**AccuRx Server** to **AccuRx GP Product**	• User and organisation settings (to configure localisation of guidelines, enable extra features) • Download new version of AccuRx GP Product (auto-update)	Https with 30 character authentication key installed into machine registry by admin at practice
6	**PDS via SMSP** to **AccuRx Server**	• AccuRx matches ODS code associated with patient to ODS code of user sending patient SMS for data validation	SMSP interface
7	**AccuRx Server** to **SMS gateway (Firetext or BT)**	• Mobile number and SMS message contents (including links to secure web-based patient-response forms)	Https to Firetext/BT API with unique API key
8	**SMS gateway (Firetext or BT)** to **Patient's device**	• SMS message contents (including links to secure web-based patient-response forms)	SMS
9	**AccuRx Server** to **Patient's device** via **Patient email provider**	• Email	Email
10	**Patient's device** to **AccuRx Server**	• User entries in secure web-based patient-response forms including date of birth (to validate user ID), free text replies and attachments (documents and photos)	Https
11	**AccuRx GP Product** to **GP Web Browser**	• Link to video consultation	Https
12	**GP Web Browser** to **Patient Web Browser**	• Video and audio communication – which is not recorded or stored on any server (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)	HTTPS and TLS/Secure Websocket Traffic/Secure WebRTC
13	**AccuRx Server** to **AccuRx SQL Database**	a) Feedback and Reports with user/organisation b) Patients (mobile/NHS Number) and SMS message NB: a) and b) aren't linked by any form of ID or foreign key	Https
14	**AccuRx SQL Database** to **AccuRx Reporting**	• Returns list of users, organisations • Aggregate level data (for example, advice usage, tool usage, features used)	Https with authentication provided by Azure (so only accessible to company employees 2FA)

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 are listed in :

- Healthcare staff 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 call participants may be stored as part of metadata stored, however no other personal information of call participants is collected or stored.

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 follow 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.

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

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 modify the data held about them.

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, who will inevitably sometimes be children and part of other vulnerable groups.

Prior to using accuRx Desktop, the healthcare professional must agree to accuRx's terms and Data Processing Agreement. If they use our Web platform, they also agree to the accuRx Acceptable Use Policy.

This all ensures the use of the platform is to support the care of the patient or management of health services, though it is the data controller's ultimate responsibility to always ensure they have the right legal basis in place.

The accuRx platform is available through the Digital Care Services Catalogue and complies with overarching standards for that, and the specific capabilities listed on the GP IT Futures, and DFOCVC frameworks.

Specific considerations of the context of processing for different features are below.

Video Consultations

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.

Patient Images

The healthcare professional must select a checkbox to give the patient the option to send a response, text and/or image, to the professional's message. This appends a link to a secure web page to the message. This secure web page collects the response.

Before opening the page to respond to the healthcare professional, the patient is informed that the form they are about to complete is operated by accuRx and also have the option to read through accuRx's privacy policy before proceeding. If they choose to proceed, the patient is clearly informed within the message that the healthcare professional has requested the image for a specific purpose. They are then informed in the response form: "By submitting an image, you consent to your practice receiving and storing that image to help deliver your care." Please note this text is not referring to GDPR legal basis consent to process the data, but rather to the organisation making a recording of the patient.

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 each other regarding patients) for the provision of healthcare or social care services.

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?

Views have been gathered by accuRx from its users across 6,500 GP practices. As with all accuRx products, ongoing feedback is solicited from our 75,000 healthcare professional user base. We've also interviewed >100 users directly on this product. Furthermore, accuRx has also engaged patients and Information Governance leaders (including Dame Fiona Caldicott and her panel, Dr Neil Bhatia, the Joint GP IT Liaison Committee and several central body IG teams) on various elements of our IG and data protection approach.

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 expected to be 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.

Messaging - Email and SMS

Healthcare professionals are authenticated by requiring: NHSmail to register for an account; TPP SystmOne or EMIS Web profiles; 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 either TPP SystmOne or EMIS Web principal care systems. This ensures that a healthcare professional can only access data of patients registered at their practice.

Patient Responses

Patient survey links are sent via SMS directly to a patient's mobile phone. The links 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 survey.

Patient Images

Patient can upload an image via the secure patient-response form via their mobile phone. Images are encrypted in transit via HTTPS and responses are encrypted at rest via TDE. The patient clicks on a link SMS that takes them into the healthcare professional's request for an image. The response form states on the first page that "By submitting an image, you consent to your practice receiving and storing that image to help deliver your care."

Files, documents or forms

Links to files, documents or forms 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

The interface only allows healthcare professionals to contact other people with nhs.net, gov.uk, nhs.uk, and pnn.police.uk domains, for the provision of direct care. nhs.uk email domains can be recipients too; there is a warning in the product when the recipient is from an organisation not on the allow list. This means that no other individuals who do not fall within these domains are able to access the interface or receive a message.

Patient Triage ('Online Consultation')
For organisations activating the accuRx Patient Triage feature, we have created a full DPIA Template for this available here.

Video Consultation

The patient consents to take part in the process by clicking on the link to the video consultation. They can dissent at any point by either not clicking on the link to the video consultation or leaving the video consultation.

The video and audio is not retained by accuRx or Whereby. Only de-identified usage metadata is retained for service evaluation and improvement.

With regards to the sub-processor, Whereby are based in the European Economic Area (EEA). All communication between the user's browser, or the patient's browser, and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS or TLS or secure webstock 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 UK or 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.

Please also see below for an assessment of compliance against the principles of the Data Protection Act, based on the use by healthcare providers, in line with the terms of using accuRx's services.

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 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.**

Risk	Likelihood of harm	Severity of harm	Overall risk
Access to Personal data by persons other than the data subject	Low	Significant	Low
Incorrect patient data selected for SMS or email	Low	Significant	Low
Sensitive data being sent via SMS or email	Low	Significant	Low
Abusive messages are sent to patients by a healthcare professional	Low	Significant	Low
The integrity of the computers used (how at risk are they from trojans or viruses)	Low	Minor	Low

Patient Responses - Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	Likelihood of harm	Severity of harm	Overall risk
A patient attempts to respond to the GP question by texting back rather than following the link	Medium	Significant	Low
A patient is unable to respond due to not being able to open the link	Medium	Significant	Low

A patient enters a clinically urgent response to a user's question	Low	Considerable	Low
A user does not see the patient response	Medium	Significant	Low

Files, Documents or Forms - Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
A user inadvertently attaches the wrong document to the message sent to a patient	Medium	Significant	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	Low
A document intended for a patient is opened by someone else	Low	Significant	Low
A patient is unable to open a document after their link has expired	Medium	Significant	Low

Patient Images - Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
A patient is unable to attach an image to their response	Medium	Significant	Low/Medium
The image quality is not good enough for the clinician to identify the issue	Medium	Significant	Low/Medium
A malicious user is getting patients to send photos via SMS then deleting it from their record	Low	Significant	Low

Patient Triage (Online Consultation) - Risks

Patient Triage ('Online Consultation')
For organisations activating the accuRx Patient Triage feature, we have created a full DPIA Template including a set of risks available here.

Video Consultation - Risks

Describe source of risk and nature of potential impact on individuals. Include associated compliance and corporate risks as necessary.	**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	Low
A third party is present in the room of one of the video consultation participants without the other participant knowing	Low	Significant	Low
A third party guesses the URL of a video consultation and joins the call	Low	Minor	Medium

AccuMail - 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

Step 6: Identify measures to reduce risk

Identify additional measures you could take to reduce or eliminate risks identified as medium or high risk in step 5.

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 authenticated by requiring: NHSmail to register for an account; TPP SystmOne or EMIS Web profiles; 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	Eliminated	Low	Yes

	from accessing the accuRx system. Patient demographic data is only pulled from either TPP SystmOne or EMIS Web principal care systems. This ensures that a healthcare professional can only access data of patients registered at their practice. Any video consultations are not recorded or stored.			
Incorrect patient data selected for SMS or email	Patient demographic data is only pulled from either TPP SystmOne or EMIS Web principal care systems. This ensures that a healthcare professional can verify the correct information with the patient before sending an 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. Where a link to documents are shared (e.g. to a document), the patient has to verify their identity by typing in the date of birth.	Reduced	Low	Yes
Sensitive data being sent via SMS or email	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. accuRx points orgnaisations using this template to guidance from the NHS IG Panel about the use of email and SMS communications with patients.	Reduced	Low	Yes

	Full audit trails are kept of all healthcare professional activity for clinical safety purposes.			
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	Yes
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	Yes

Patient Responses - Measures to reduce risk

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
A patient attempts to respond to the GP 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	Yes
A patient is unable to respond due to not being able to open the link	1,2) A patient can contact the practice using usual methods e.g. telephone 1,2) A user can contact the patient using usual methods e.g. telephone 1) A patient can open the link on their computer	Reduced	Low	Yes

	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 practice using existing methods e.g. telephone call. Following submission of the answer, the patient is informed "Your message will be reviewed in the next 7 days, for urgent queries, please call reception".	Reduced	Low	Yes
A user does not see the patient response	Colleagues can let each other know about responses that they have acted on. The only user to be notified of a patient response will be the user who sends the question to the patient. All users at a practice can review responses in the shared "Practice inbox".	Reduced	Low	Yes

Files, Documents or Forms - Measures to reduce risk

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
A user inadvertently attaches the wrong	A patient can call the practice if they feel a document sent to them is	Reduced	Low	Yes

document to the message sent to a patient	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			
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	Yes
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	Yes
A patient is unable to open a document after their link has expired	TBC	Reduced	Low	Yes

Patient Images - Measures to reduce risk

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
A patient is unable to attach an image to their response (due to technical or user limitations)	A patient can discuss the issue by calling the practice. A patient can see a healthcare worker face to	Reduced	Low	Yes

	face. In some practices, patients can email in to the practice In addition, the following text is displayed to a patient completing a response to the practice: "If you need to attach an image, the option will be available on the next screen." A header with 'Attach Image' is displayed			
The image quality is not good enough for the clinician to identify the issue	A user can see the patient face to face. A user can contact the patient to retake the photo with advice. A user can send an image in via email (not available at all practices). In addition, helper text is displayed to the patient to guide them to take a better photo: "Please ensure adequate lighting and that the subject is in focus (image has crisp edges). Place a ruler or coin in shot which is useful to assess scale)."	Reduced	Low	Yes
A malicious user is getting patients to send photos via SMS then deleting it from their record	Although a user can delete an image from the patient's EMIS/SystmOne record, they are unable to delete it from the accuRx server. This allows an audit trail of images	Eliminated	N/A	

Patient Triage ('Online Consultation')

For organisations activating the accuRx Patient Triage feature, we have created a full DPIA Template including risks and a set of measures to reduce them available here.

Video Consultation - Measures to reduce risk

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	Healthcare professionals can view what the patient views in the video consultation. Therefore, any third-party data could be identified and	Reduced	Low	Yes

captured by the individual in any video call	blocked by the healthcare professional.			
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	Yes
A third party guesses the URL of a video consultation and joins the call	Each URL generated is completely unique, rendering it almost impossible to guess by a third party. They would also have to guess it at precisely the same time other participants are in the virtual meeting room. Even if they did both of those (incredibly unlikely) things, participants can immediately see when another participant joins the call and end the call.	Eliminated	Low	Yes

AccuMail - 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 professionals can only send a message	Reduced	Low	❑

healthcare professional initiated 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.'			

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes

Measures approved by:	T HODSON	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	T HODSON	If accepting any residual high risk, consult the ICO before going ahead
DPO advice provided:	Via CCG	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:		
This DPIA will kept under review by:		The DPO should also review ongoing compliance with DPIA