Data Protection Impact Assessment (DPIA)

Submitting controller details

Name of controller	Greystones Medical Centre	
Subject/title of DPO	Security and IG of photos and storage	
Name of controller contact	Greystones Medical Centre	

The aim of the service is to improve communication between healthcare staff and patients to improve outcomes and productivity. The patient image feature is designed to enable patients to attach images to provide clinicians with additional information to inform their care. An example use case would be for remote consultations where video quality may not be optimal and patients want to show a particular area(s) of concern to the clinician, for example, a rash or a skin mole.

The need for a DPIA is the processing, on a large scale, of special categories of data, which in this case is patient images for the purposes of providing direct healthcare.

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

User Flow

The healthcare professional:

1. Opens up the patient that they would like to request the image from
2. Patient demographics are automatically populated from their record (name, NHS no., DoB, sex, mobile no.)
3. Types a message requesting the image from the patient, with specific details included as applicable
4. Confirms that they would like to allow the patient to respond to the message with their image attachment or with a text message (this adds a link to the bottom of the SMS message, enabling a patient to use that link to submit their image)
5. This sent message is then available to view in the patient's SMS history within the AccuRx window

The Patient:

6. Receives an SMS from their healthcare professional asking them to complete a response form. This SMS contains confirmation that the form is operated by AccuRx (with a link to the AccuRx website where the privacy policy can be found)

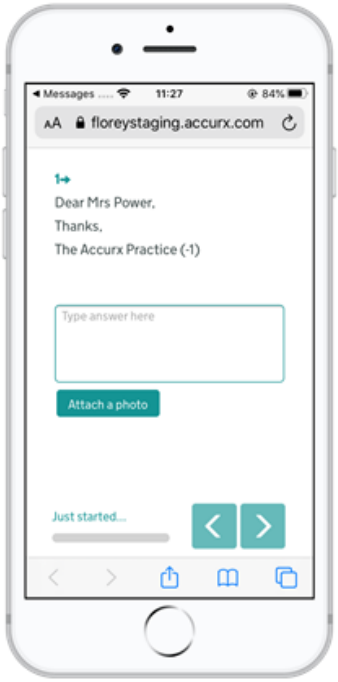
7. The response form states that *"By submitting an image, you consent to your practice receiving and storing that image to help deliver your care"*

8. Patient confirms that they are happy to proceed by clicking "Yes"

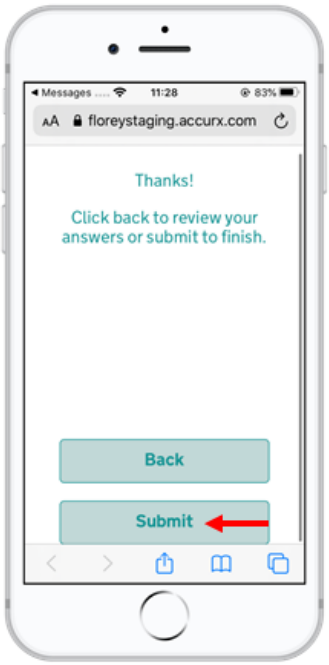
9. Enters their date of birth to verify that the correct patient has received the correct link

10. Is then shown the message from the healthcare professional requesting the image

11. Adds any descriptive detail relating to the image into the free-text box



12. Clicks "attach photo" and then "choose a photo" to upload a photo from their device
13. Reviews their response to the healthcare professional and clicks "Submit"



14. Upon submission, a submission confirmation message will appear

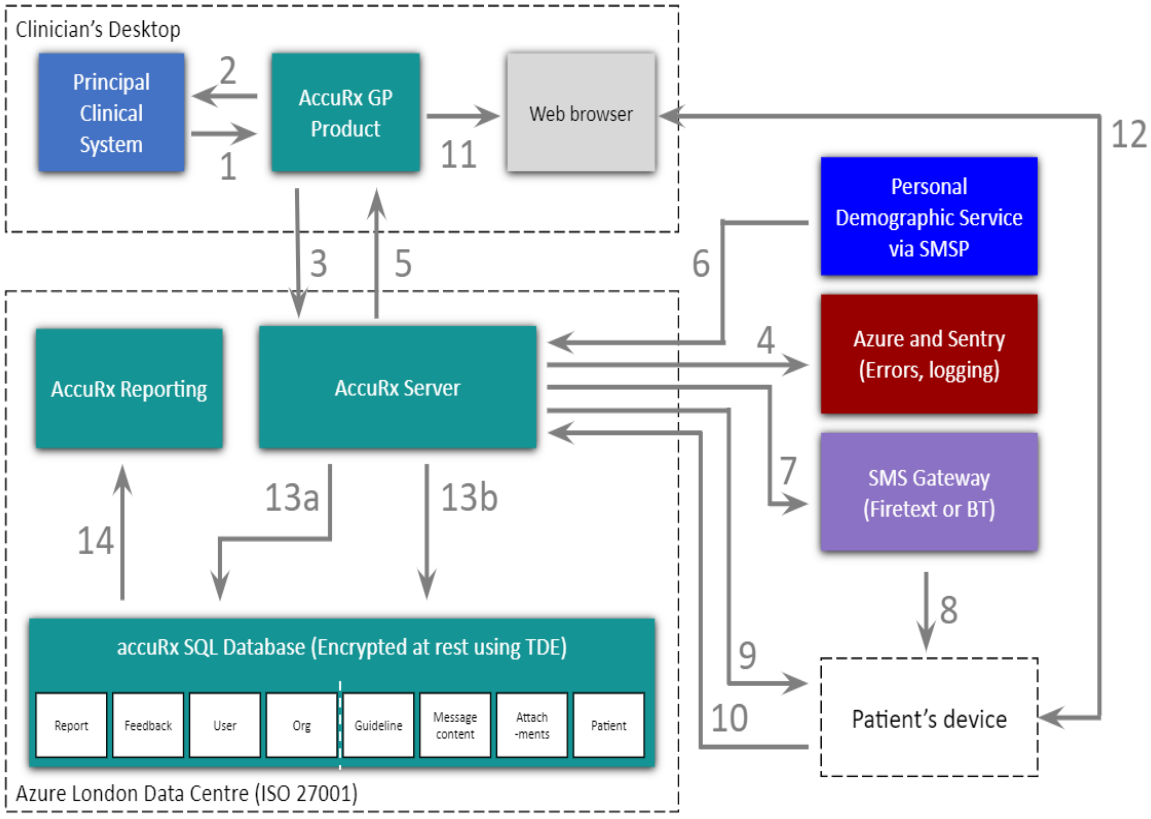
The healthcare professional:

15. Receives the patient's response within the "Patient Responses" section of the AccuRx toolbar
16. Clicks to view the response
17. Clicks the "photo" hyperlink on the Patient Attachment section to view the image in their web browser (or the healthcare professional can download to view outside of the web browser)
18. Clicks "save to record" to save the patient's text and photo response to

their patient record

Data Flows

All data sent is encrypted when in transit (when it is sent) and at rest (when it is stored). The data (including images) is hosted on Microsoft Azure servers in their London Data Centre. AccuRx follows the Microsoft Azure NHS Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services. See here and here for further information.

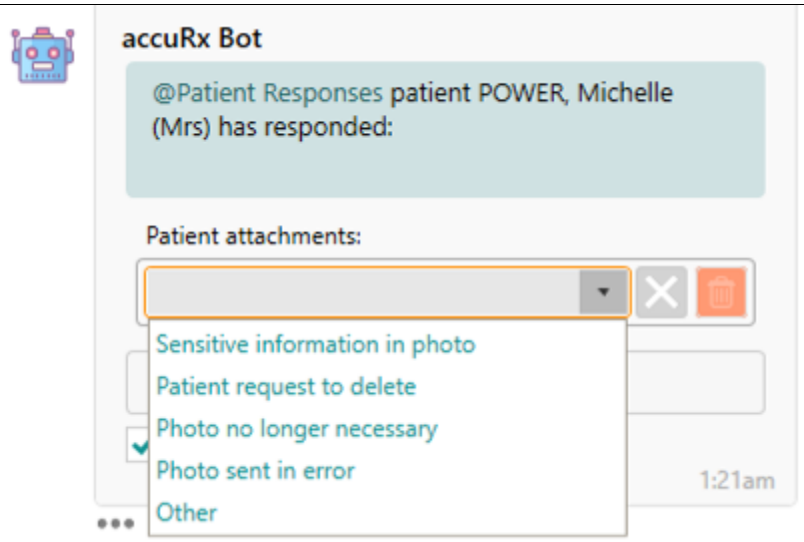


Number	Data description	Data processed	Method of processing
1	**Principal Clinical System** to **AccuRx GP Product**	• Patient demographic details (name; date of birth; gender; NHS number; mobile number; email address) • User ID • User Role (GP, nurse etc) • Organisation (Practice details)	IM1 API (local 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
Not relevant for patient photos feature			
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
Not relevant for patient photos feature			
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)

Data Retention

Patient images - along with other patient data - are kept in line with the Records Management Code of Practice for Health and Social Care 2016. These require us to hold records on behalf of GP practices until 10 years after a patient has died. However, we would delete the data earlier than suggested by this code if we are informed that the condition of Article 9(3) GDPR and s. 11(1) Data Protection Act 2018 no longer applies: "that the circumstances in which the processing of personal data is carried out... [is] by or under the responsibility of a health professional or a social work professional".

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.



However, AccuRx follow 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 court orders or other legislative circumstances. Physical deletion of any communication using AccuRx (including photos) can only be carried out in response to a specifically authenticated and validated request from an organisation's Caldicott Guardian or Privacy Officer, co-signed by a senior clinical representative.

An additional type of special category data is being processed (patient images) compared to what is usually processed by AccuRx. The Personal Data, including Special Categories of Personal Data, processed by AccuRx, includes but is not limited to the following data relating to patients of the Data Controller, namely:

- Patient demographic details (name; date of birth; gender)
- NHS number
- Mobile phone number
- Email address
- Content of the communications with – or regarding - patients sent via AccuRx (which may include patient images or documents)
- Other types of data (which may include the patient's GP medical record) that may from time to time be required to provide the Services

Patient images - along with other patient data - are kept in line with the Records Management Code of Practice for Health and Social Care 2016. These require us to hold records on behalf of GP practices until 10 years after a patient has died. However, we would delete the data earlier than suggested by this code if we are informed that the condition of Article 9(3) GDPR and s. 11(1) Data Protection Act 2018 no longer applies: "that the circumstances in which the processing of personal data is carried out... [is] by or under the responsibility of a health professional or a social work professional".

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.

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

The healthcare professional must opt-in to give the patient the option to send an image as a response to the message.

Before opening the message from 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.

The patient consents to take part in the process by clicking on the link that takes them into the healthcare professional's request. They then further consent by uploading their image and sending it back to the healthcare professional. 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." Crucially, they have the right to object by simply not submitting a response to the healthcare professional.

If the patient does decide to respond to the healthcare professional's request with an image, the data processed by AccuRx is encrypted in transit via HTTPS and encrypted at rest via TDE. The viewer of the record has their identity verified by having to log into the EPR System. AccuRx follows the Microsoft Azure NHS Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services. See here and here for further information.

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. The purpose of the patient image feature is to enable patients to attach images to provide clinicians with additional information to inform their care.

Views have been gathered from AccuRx users across 6,500 GP practices. As with all AccuRx products, ongoing feedback is solicited from our 60,000 healthcare professional user base. We've also interviewed 15 users on this. Furthermore, AccuRx has also engaged patients and Information Governance leaders on our Data Protection approach.

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.

Messaging

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 response form 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 response form.

Patient Images

Patients 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.

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	**Patient consents to take part in the process by clicking on the link that takes them into the healthcare professional's request. They then further consent by uploading their image and sending it back to the healthcare professional. 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." They can dissent at any point by not responding to the response form.**
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.	**Image sharing is for medical purposes and the patient can dissent at any stage by either not clicking on the link to the request or not responding to the message.**
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.	**Requests for patient images are based on clinical decisions made by healthcare professionals and are done on a need-only basis to enhance the care being provided virtually.**
Principle 4 – () 2.12 Personal data shall be accurate and, where necessary, kept up to date.	**The ability to view and save (where necessary) patient images will aid this principle by providing the healthcare professional with an enhanced view of the patient's concern and the status of their health at that moment in time.**

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.	**Patient images, along with other patient data, are kept in line with Records Management Code of Practice for Health and Social Care 2016. These require us to hold records on behalf of GP practices until 10 years after a patient has died. However, we would delete the data earlier than suggested by this code if we are informed that the condition of Article 9(3) GDPR and s.11(1) Data Protection Act 2018 no longer applies: "that the circumstances in which the processing of personal data is carried out…[is]by or under the responsibility of a health professional or a social work professional".**
Principle 6 – (2.22& 2.23) Personal data shall be processed in accordance with the rights of data subjects under this Act.	**Patient agrees to take part in the process by uploading an image in response to the healthcare professional, after acknowledging that the request has come from their GP. They can dissent at any point by either not clicking on the link to respond with an image or by not responding to the SMS.**
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 is secure and complies with the NHS standard for encryption. 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. AccuRx data is encrypted in transit via HTTPS and encrypted at rest via TDE.**
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 follows the Microsoft Azure Security and Compliant Blueprint for Platform-as-a-Service web applications, specifically designed for NHS services. This means that AccuRx does not store or directly transfer the Personal Data/Special Categories of Personal Data outside of the EEA without a lawful transfer mechanism. 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 EEA may result in the data being processed outside of the EEA; a patient may be receiving messages whilst outside of the EEA.**

Identify and assess 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**
Access to Personal data by persons other than the data subject	Remote	Significant	Low
Incorrect patient data selected for SMS	Remote	Significant	Low
Sensitive data being sent via SMS	Remote	Significant	Low
Abusive messages are sent to patients by a healthcare professional	Remote	Significant	Low

The integrity of the computers used (how at risk are they from trojans or viruses)	Remote	Minimal	Low
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

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 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.	Eliminated	Low	Yes

Incorrect patient data selected for SMS	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 sensitive data is 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	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 healthcare professional activity for clinical safety purposes.	Reduced	Low	Yes
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
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 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.	Reduced	Low	Yes
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	Yes

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