10th Dec 2020

DPIA: Patient Triage

Submitting Controller Details

Name of controller	St. Neots Surgery
Subject/title of DPIA	AccuRx Patient Triage
Name of controller contact / DPO (delete as appropriate)	Dr.William Davies GP IT Lead & Caldicott Guardian and Clinical Safety trained

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 patient-initiated messaging feature is designed to enable patients to request and receive support relating to their healthcare concerns.

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.

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.

The AccuRx patient-initiated messaging feature allows patients to request and receive support relating to their healthcare concerns. They can make requests to the relevant Healthcare Organisation, at a time convenient to them, for support in relation to their healthcare conditions.

Provision of information by the patient allows the Health or Care Professional dealing with the request to triage requests effectively and make informed decisions about how best to respond - the response could be information or advice, an offer of a consultation, provision of a repeat prescription, test results, or a referral to other services.

This enables the healthcare professional to have an informed view of the patient's current circumstances before deciding to proceed with either (1) a message follow-up, (2) a phone call follow-up, (3) a video-call follow up or (4) an email.

User Flow

- Patient is directed from their GP website to accuRx site
- They then get directed to a number of options to submit a request to the practice
- Before they can submit their request, they must enter: ~dob, ~surname, ~forename, gender, ~postcode, plus contact details including phone number
- The number the patient puts in will be sent a secure code via SMS, and the patient is asked to enter this code into the webpage before proceeding. If they cannot do this, they can still submit their request. The patient is not given information as to whether the practice 'recognises' them / as to whether their details are correct
- The practice automatically uses all this information to search for the patient on PDS
- Practice is able to view all incoming requests, including those which have not been matched to a patient on PDS
- Any match(es) are displayed to the practice staff as either exact or suggested or unmatched
- IF the submitted information matches a single patient, AND the contact number submitted is consistent with that on PDS, AND the patient has successfully submitted the secure code sent to this number (i.e. they have passed a two factor authentication process), it's an exact match, and the patient's request will be displayed to the practice as under the patient's information/ record
- IF the submitted information matches a single patient but the submitted contact number does not match that on PDS, OR if the submitted information and contact number do match to a unique patient, but they have not successfully entered the secure code sent to the contact number listed on PDS, it's a suggested match, and displayed to the practice as such. The practice will be prompted to verify the identity of the patient before proceeding with their request
- IF the submitted information does not match a single patient (i.e. it matches multiple),

OR no patient is found on PDS using the submitted information, it's unmatched, and displayed to the practice as such. The practice will be prompted to verify the identity of the patient before proceeding with their request

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 in this case is:

- Patient data (typically name, identifiers, contact details [mobile], demographic data [DoB; gender], message content (including images), documents/notes, survey responses, metadata)

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 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.

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.

The patient has complete control over how much or how little information they want to provide to the healthcare professional, since it is a form that they are manually inputting. The patient consents by clicking on the link that submits their message to the healthcare professional. Crucially, they have the right to object by simply not submitting a message to the healthcare professional.

Prior to using any AccuRx product and therefore accessing the patient's response, the healthcare professional must agree to an acceptable use policy.

The nature of the relationship with the individuals participating in patient initiated message is that of a healthcare professional providing direct care to 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 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 GPs and 7 patients on this product. Furthermore, AccuRx has also engaged patients and Information Governance leaders on our 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 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.

Patient Triage

Communications between the patient and healthcare professional are encrypted in transit via HTTPS and responses are encrypted at rest via TDE. Patients are also asked to input their DoB, Surname, Forename, Gender, Postcode plus phone number to verify their identity via an SMS Two-Factor Authentication.

The practice is able to view all incoming requests, including those which have not been matched to a patient on PDS. Any match(es) are displayed to the practice staff as either exact or suggested or unmatched.

IF the submitted information matches a single patient, AND the contact number submitted is consistent with that on PDS, AND the patient has successfully submitted the secure code sent to this number (i.e. they have passed a two factor authentication process), it's an exact match, and the patient's request will be displayed to the practice as under the patient's information/ record.
IF the submitted information matches a single patient but the submitted contact number does not match that on PDS, OR if the submitted information and contact number do match to a unique patient, but they have not successfully entered the secure code sent to the contact number listed on PDS, it's a suggested match, and displayed to the practice as such. The practice will be prompted to verify the identity of the patient before proceeding with their request.

IF the submitted information does not match a single patient (i.e. it matches multiple), OR no patient is found on PDS using the submitted information, it's unmatched, and displayed to the practice as such. The practice will be prompted to verify the identity of the patient before proceeding with their request.

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 completing the form and sending it to the healthcare professional. They can dissent at any point by not messaging the healthcare professional.
Principle 2 – (2.2)	Personal data is processed under the lawful basis

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.	of the provision of health care or social care services.
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.	The extent of the patient message purposely has a limit of 200 words per answer in order to ensure the information provided is not excessive and remains relevant to the query.
Principle 4 – () 2.12 Personal data shall be accurate and, where necessary, kept up to date.	The information provided by the patient will give the healthcare professional an up to date view of the patient's circumstances and this can be added into the patient's medical record to ensure an accurate and up to date record is maintained.
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 data is 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 submitting the form to the healthcare professional, after acknowledging that the form will be sent to the healthcare professional. They can dissent at any point by not sending the message.
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.

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.	**Likelihood of harm**	**Severity of harm**	**Overall risk**
Access to Personal data by persons other than the data subject	Low	Significant	Low
Sensitive data being sent via SMS	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 Initiated Messaging - 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 sends a message to the GP practice via clinical or admin request pathways, and describes red flag symptoms / something that warrants more urgent medical attention. This might not be reviewed by the administrators or clinical team for many days (e.g. over the weekend/ out of hours)	Medium	Significant	Low
Any patient can contact any GP practice and submit an admin/ medical request, even if they are not a patient at that practice	Medium	Minor	Low
Malicious use of Patient Triage - a malicious actor could submit a large volume of inbound requests and overwhelm a practice's email inbox / AccuRx inbox	Low	Significant	Low
Malicious use of Patient Triage - a malicious actor could attempt to contact the GP practice pretending to be another individual	Low	Significant	Low
A GP practice could be overwhelmed with more patient initiated requests than they are able to cope with	Medium	Significant	Low
For patient initiated messages that are not matched to a patient via PDS, intercepting staff at the practice could not realise that the patient has not been 'authenticated', i.e. that there is no good reason to believe the patient is who they say they are	Medium	Significant	Low
Email doesn't send for whatever reason and patient is waiting for medical help without knowing that their request has not been received	Medium	Significant	Low
Following submission of an online consultation, the patient condition deteriorates and doctor can't get	Low	Significant	Low

hold of them over phone/video call			
Reception encourages someone that calls to use online service. They struggle to use it and abandon, and are too frustrated/scared/worried to call again to get the help they need	Low	Significant	Low
Patient enters medical request under clinical request, or vice versa	Low	Minor	Low
Patient is unclear when to call 999 /111	Low	Significant	Low
During beta version - user may reply to emails coming into practice email inbox thinking their reply will be sent to the patient. The patient does not receive important clinical information, and the practice does not realise this	Medium	Significant	Low
Patient enters medical request under clinical request, or vice versa	Low	Minor	1
A new patient triage request is not seen in the accuRx Inbox	Low	Significant	2
A patient triage request is not acted on within a reasonable timeframe	Medium	Significant	2
Patient or someone acting on behalf of patient attached intimate photos to Patient Triage request	Medium	Significant	2
A patient is unable to attach an image to their Patient Triage request	Medium	Significant	2
The image quality is not good enough for clinician to identify issue	Medium	Significant	2
A malicious user asks patients to send photos via SMS then deletes these from their record	Low	Significant	2
1. Stored photos/ documents are accessed by an inappropriate / malevolent user or external hacker 2. Stored photos/ documents are accessed by an inappropriate / malevolent accuRx employee 3. Stored photos/ documents are accessed by an appropriate user, but used inappropriately	Low	Significant	2
Patients make errors in their medication requests on Patient Triage	Low	Significant	2

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 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 TPP SystmOne. This ensures that a healthcare professional can only access data of patients registered at their practice. Any video consultations are not recorded or stored.	Eliminated	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

Patient Triage- Measures to reduce risk

Risk	Options to reduce or eliminate risk	Effect on risk	Residual risk	Measure approved
A patient sends a message to GP practice via clinical or admin request pathways, and describes red flag symptoms / something that warrants more urgent medical attention. This might not be reviewed by the administrators or clinical team for many days (e.g. over the weekend/ out of hours)	Informing the patient at multiple points before submitting their request that 1. their message will not be read out of hours, 2. that their request may not be read for up to 2 working days within normal working hours, 3. that they should seek more urgent medical help if they need a more urgent response, whether from their practice, NHS 111, or 999. Also 4. Screening for 'Red flag' symptoms, and preventing patients submitting a request if they state that they have any of these; 5. prompting patients upon submission of their request to seek more urgent medical attention if their condition deteriorates.	Reduced	Low	Yes
Any patient can contact any GP practice and submit an admin/ medical request, even if they are not a patient at that practice	Patients' queries are flagged to practice staff as 'unmatched' for patients who's submitted information does not match to a patient registered at that practice. The practice is then prompted to confirm the identity of the patient, and will have access to the	Reduced	Low	Yes

	patient's contact details to let the patient know if they are not registered with that practice.			
Malicious use of Patient Triage - a malicious actor could submit a large volume of inbound requests and overwhelm a practice's email inbox / accurx inbox	Restricting the number of times someone is allowed to submit the form from a particular location.	Eliminated	Low	Yes
Malicious use of Patient Triage - a malicious actor could attempt to contact the GP practice pretending to be another individual	Patients are prompted to submit a phone number upn submission of their request. A 6 digit code is sent via SMS to this phone number, and the patient is prompted to enter this code into the website. If patient requests do not pass this two factor authentication, their request is flagged up to the practice as 'unmatched'. The practice is then prompted to confirm the identity of the patient, and will have access to the patient's contact details to let the patient know if they are not registered with that practice. It is possible that some people will have access to the mobile of the person they are trying to imitate, and will therefore be able to pass the 2 factor authentication. This is deemed an acceptable level of risk.	Reduced	Low	Yes
A GP practice could be overwhelmed with more patient initiated requests than they are able to cope with	Patients are prompted to call practice if they have not heard from practice after 3 days. Offering analytics of demand will help practices match demand to capacity.	Reduced	Low	Yes

For patient initiated messages that are not matched to a patient via PDS, intercepting staff at the practice could not realise that the patient has not been 'authenticated', i.e. that there is no good reason to believe the patient is who they say they are.	1. Patients are clearly displayed as 'unmatched' if they are, and 2. GP staff are then prompted to authenticate the patients' identity if needed. Staff are prompted to have a mitigating course of action for these patients.	Reduced	Low	Yes
Email doesn't send for whatever reason and patient is waiting for medical help without knowing that their request has not been received	Stringent internal testing to ensure 100% reliability before product is live.	Reduced	Low	Yes
Following submission of an online consultation, the patient condition deteriorates and doctor can't get hold of them over phone/video call	Patient is reminded at multiple times throughout the request process 1. how quickly the practice is likely to respond, 2. that this is not a suitable product for urgent medical requests, and 3. that they should escalate their request to 111 or 999 if they need more emergent care, or if they deteriorate.	Reduced	Low	Yes
Reception encourages someone that calls to use online service. They struggle to use it and abandon, and are too frustrated/scared/worried to call again to get the help they need	Practice staff to be encouraged via user guide to only direct patients to complete online requests if they are able to, to call back if they cannot, and for practice staff to fill in online consultation themselves on behalf of the patient where appropriate.	Reduced	Low	Yes
Patient enters medical request under clinical request, or vice versa	All requests will be vetted by staff at the practice, and the staff can escalate these as urgent if needed.	Reduced	Low	Yes
Patient is unclear when to call 999 /111	Information to be provided directing patient to NHS website explaining when to call 111/ 999.	Reduced	Low	Yes
During beta version - user may reply to emails coming into practice email inbox thinking their reply will be sent to the patient.	Emails coming into the practice inbox (for the beta version) have a reminder message at the top not to reply to them. Emails sent to the sending	Reduced	Low	Yes

The patient does not receive important clinical information, and the practice does not realise this.	(accurx.nhs.net) email account will also get an automatic reply, advising that the patient will not receive their sent email.			
Patient enters medical request under clinical request, or vice versa	All requests will be vetted by staff at the practice, and the staff can escalate these as urgent if needed	Reduced	Low	Yes
A new patient triage request is not seen in the accuRx Inbox	- Users are notified on new patient triage requests via a notification banner and red dot containing the number of unread messages - When a user is viewing the inbox, there are additional red dots with numbers inside to indicate unread messages in each folder - Patient Triage requests are visible to all users to ensure messages are not stuck in someone's inbox if they are out of practice on the day	Reduced	Low	Yes
A patient triage request is not acted on within a reasonable timeframe	- Although assignment helps show the practice who is responsible for acting on a patient triage request, all patient triage requests are visible to non-asignees. This was an intentional design decision to ensure that the practice has an overview of all patient triage requests and can monitor any that have not been acted on in a timely manner - The webpage where the patient enters their symptoms has a section where the patient is informed not to use the form for medical emergencies and requests may not be seen for 2	Reduced	Low	Yes

	working days. Patients need to click to confirm they do not have symptoms constituting a medical emergency. - There is an urgent flag that a user can apply to a patient triage request. This turns the patient triage request selection red, adds a red flag icon and indicates to other users that the request is of higher urgency.			
Patient or someone acting on behalf of patient attached intimate photos to Patient Triage request	Patients are prompted not to attach any intimate images, and have to actively consent that they have not done so before submission.	Reduced	Low	Yes
A patient is unable to attach an image to their Patient Triage request	- A patient can discuss the issue by calling the practice - A patient can contact accuRx support, for technical assistance - Practice staff can respond to the Patient Triage request, asking for a photo and sending an SMS to enable this pro	Reduced	Low	Yes
The image quality is not good enough for clinician to identify 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) - Helper text is displayed to the patient to guide them to take a better photo, advising them to (1) use adequate lighting, (2) make sure image is in focus and (3) uses an object for scale	Reduced	Low	Yes
A malicious user asks patients to send photos via SMS then deletes	- Although a user can delete an image from the patient's SystmOne record,	Reduced	Low	Yes

these from their record	they are unable to delete it from the accuRx server. This allows an audit trail of images			
1. Stored photos/ documents are accessed by an inappropriate / malevolent user or external hacker 2. Stored photos/ documents are accessed by an inappropriate / malevolent accuRx employee 3. Stored photos/ documents are accessed by an appropriate user, but used inappropriately	(1), (2) We follow recommended best practice for storing documents and photos, they are encrypted at rest, and noone has direct access to the files; rather - they are only accessible on an individual basis by authenticated practice users through secure channels. (3) Photos can be 'soft' deleted so that users cannot access them going forward. We have logs of photos accessed for >= the past 12 months, and these can be used to inform an audit trail if needed. We encourage submissions to be saved to the patient's record, and provide best practice guidance to users around processing photos.	Reduced	Low	Yes
Patients make errors in their medication requests on Patient Triage	Staff are trained to check medication requests from patients, and should be alert to possible errors. St. Neots Surgery uses the advantage of the customisation to redirect to Airmid/NHS App and SystmOnline	Reduced	Low	Yes

Step 7: Sign off and record outcomes		
Item	**Name/position/date**	**Notes**
Measures approved by:	Dr. William Davies	10th December 2020
Residual risks approved by:	Dr. William Davies	10th December 2020. I am happy that the residual risks are clinically safe (no greater than 2) and have been mitigated as far as practicable.
DPO advice provided:	No further advice required	
Summary of DPO advice:		
DPO advice accepted or overruled by:	N/A	
Comments:		
Consultation responses reviewed by:	N/A	
Comments:		
This DPIA will kept under review by:	Dr. William Davies	