




## Data Protection Impact Assessment for GP Practice Use

DPIA Title:	DPIA to support the implementation of the AccuRx platform to aid SMS and video consultations in GP Practices
IG Validation	Liz Griffiths, Information Governance Business Partner – Primary Care
Date of IG Validation	06/08/2020
Data Protection Officer consulted (date):	06/08/2020
Data Protection Officer comments:	Formally approved for practice use
Data Protection Officer signature:	 Hayley Gidman
Caldicott Guardian consulted (date):	14 <sup>th</sup> April 2025
Caldicott Guardian comments:	None
Caldicott Guardian signature:	
SIRO approval (date):	14 <sup>th</sup> April 2025
SIRO comments:	None
SIRO signature:	

What is the process under consideration?	Guidance
<p>AccuRX is an NHS Digital-approved solution developed to ensure anyone involved in a patient's care can easily communicate with everyone else involved in that patient's care, including the patient. AccuRX offers two products:</p> <p>1.) <b>Chain SMS</b>, a desktop-based software that integrates with EMIS and TPP SystmOne and can be used by practices to communicate with patients via SMS.</p> <p>2.) <b>AccuRX Fleming</b>, a web-based product that can be used by any NHS staff member to send a text message to a patient, or to conduct a video consultation. It uses the NHS Personal Demographic System (PDS). AccuRX Fleming does not link with the GP Practice System of Choice as Chain SMS does, and can be used on a mobile, desktop or any device connected to the internet.</p> <p>This Data Protection Impact Assessment is to provide assurances on the use of AccuRx products for video consultations between healthcare staff and patients given the high level of special categories of data being used. AccuRX Fleming can be initiated via a secure URL by healthcare or social care staff. Patients do not need to download an app or create an account.</p> <p>The purpose of using video consultations on the AccuRx platform is to minimise face-to-face contact between healthcare staff and their patients as <u>advised by NHS England on 5<sup>th</sup> March 2020</u> as a response to the COVID-19 pandemic and to ensure the continuous delivery of healthcare. For scenarios beyond COVID-19 where a face-to-face consultation cannot be achieved or at the request of the practice/patient, this will be a valued source of doctor/patient consultation.</p> <p>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 will be carried out in the same way as if a face-to-face consultation had occurred.</p>	<p>Present a brief outline of the processing/scheme/project – i.e. the name of the project, reason for sharing data, etc</p>

Will the process necessitate the use/processing/collection/sharing of any personal or pseudonymised data?	
<p>Yes – AccuRX will process personal data.</p> <p>The personal data, including special categories of personal data, includes but is not limited to the following data relating to patients of the GP Practice (the Data Controller) namely:</p> <ul style="list-style-type: none"> <li>• Patient demographic details (name, address, date of birth, gender)</li> <li>• NHS number</li> <li>• Contact telephone number</li> <li>• Email address</li> <li>• Content of the communications with – or regarding - patients sent via AccuRx (which may include patient images or clinical documents)</li> <li>• Other types of data that may from time to time be required to provide the service.</li> </ul>	<p>Personal data - Any information relating to an identified living person ('data subject') by way of an identifier such as a name, address, date of birth, NHS Number.</p> <p>Pseudonymised data - Personal data which has undergone pseudonymisation, which could be attributed to a natural person by the use of additional information, i.e. local identifier which would then be reidentified if needed.</p>
What are the responsibilities linked to the processing? (i.e. who is the data controller, any possible data processors, and joint data controllers)	
<p>The GP practice remains the data controller, and AccuRx the data processor, as per AccuRx's existing <a href="#">Data Processing Agreement</a>. The video consultation service is hosted by Whereby (sub-processor) who are fully compliant with GDPR. The video and audio communication are only visible to participants on the call and is not recorded or stored on any server. The connection prioritises 'peer-to-peer' between the healthcare professionals and patient's phone and follows <a href="#">NHS best practice guidelines</a> on health and social care cloud security.</p> <p>The data controller's and data processor's responsibilities, in line with processing personal data under the GDPR and Data Protection Act 2018, are stipulated within the Data Processing Agreement between AccuRx and the GP practice.</p>	<p>Definition: Data Controller - Natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.</p> <p>Definition: Data Processor - Natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.</p>

<p>What governance measures are in place to oversee the confidentiality, security, and appropriate use of the data?</p>	<p>Governance measures may include compliance with the Data Security and Protection Toolkit, having IG, data security and data breach policies and procedures in place, 95% minimum staff compliance with IG training.</p> <p>Note that “All organisations that have access to NHS patient information must provide assurances that they are practising good information governance and use the Data Security and Protection Toolkit to evidence this by the publication of annual assessments” (<a href="https://www.dsptoolkit.nhs.uk/Help/Attachment/5">https://www.dsptoolkit.nhs.uk/Help/Attachment/5</a>)</p>
<p>All computer equipment used in the GP Practice must comply with security requirements and adhere to the NHS standards for encryption. As the URL generated is unique for each consultation and all participants are visible in the consultation, no third party can 'listen in'. All communication between the healthcare professional's browser, or the patient's browser, and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure web socket traffic or secure WebRTC). No demographic information (such as names of the participants) is collected or stored by Whereby.</p> <p>AccuRX submitted to the Data Security and Protection Toolkit DSPT in 2018/19 and submitted to Standards Exceeded on 28/07/2020 for the 2019/20 DSPT. They also hold both the Cyber Essentials and Cyber Essentials Plus certification. AccuRx data is encrypted in transit via HTTPS and encrypted at rest via TDE.</p> <p>The data processing agreement outlines the AccuRX responsibilities to ensure there are adequate technical and organisational controls in place to secure communications and protect patient confidentiality.</p>	

## DATA, PROCESSES AND SUPPORTING ASSETS

<p>What is the data processed?</p>	
<p>The Personal Data, including Special Categories of Personal Data, includes but is not limited to the following data relating to <b>Patients of the Data Controller</b>, namely:</p> <p>Patient demographic details (name, address, date of birth, gender)</p>	<p>List the data collected and processed, i.e. name, address, date of birth etc.</p>

<ul style="list-style-type: none"> <li>• NHS number</li> <li>• Contact telephone number</li> <li>• Email address</li> <li>• Content of the communications with – or regarding - patients sent via AccuRx (which may include patient images or clinical documents)</li> <li>• Other types of clinical data that may from time to time be required to provide the patient with the most effective service, such as copies of x-rays/images/key diagnostics.</li> </ul>	
<p>How does the life cycle of data and processes work?</p>	
<p>When using the AccuRx platform, the healthcare professional:</p> <ol style="list-style-type: none"> <li>1. Logs in with NHSmail Single Sign-on (SSO)*</li> <li>2. Is associated with the organisation returned from SSO</li> <li>3. Is approved if the associated organisation matches an approved list of NHS and social care provider organisations</li> </ol> <p><i>*(If healthcare professional does not have an NHSmail account, they can create an AccuRx account using a verified *.nhs.uk email account from an approved list of NHS or social care provider organisation domains)</i></p> <ol style="list-style-type: none"> <li>4. Looks up a patient by NHS number and date of birth via the AccuRx integration with the Personal Demographic Service (PDS)</li> <li>5. Receives a return of that patient's name, gender, and the last three digits of the patient's contact number only if the PDS search is an exact match</li> <li>6. Verifies that the patient details returned are correct</li> </ol> <p><b><u>Text Messaging</u></b></p> <p>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.</p> <p><b><u>Files and Documents</u></b></p> <p>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</p>	<p>Present and describe how the product generally works (from the data collection to the data destruction, the different processing stages, storage, etc.), using for example a diagram of data flows (add it as an attachment) and a detailed description of the processes carried out.</p>

document is accessible for 14 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.

### **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 medical records and any agreed actions are carried out.

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

Whereby are based in Norway. All communication between the healthcare professional's browser, or the patient's browser, and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure web socket traffic or secure WebRTC). Furthermore, the video consultation connection prioritises 'peer-to-peer' connections between the healthcare professionals 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 healthcare professional and patient are using their computer devices in the European Economic Area (EEA), 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.

The only data related to the call that may be stored by Whereby is metadata to provide additional context about the way their service is being used. The usage data may include the participant's browser type and version, operating system, length of call, page views and website navigation paths, as well as information about the timing, frequency, and pattern of the service use. The IP address of call participants may also be stored as part of this usage data. No other personal information of call participants is collected or stored by Whereby.

### **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**

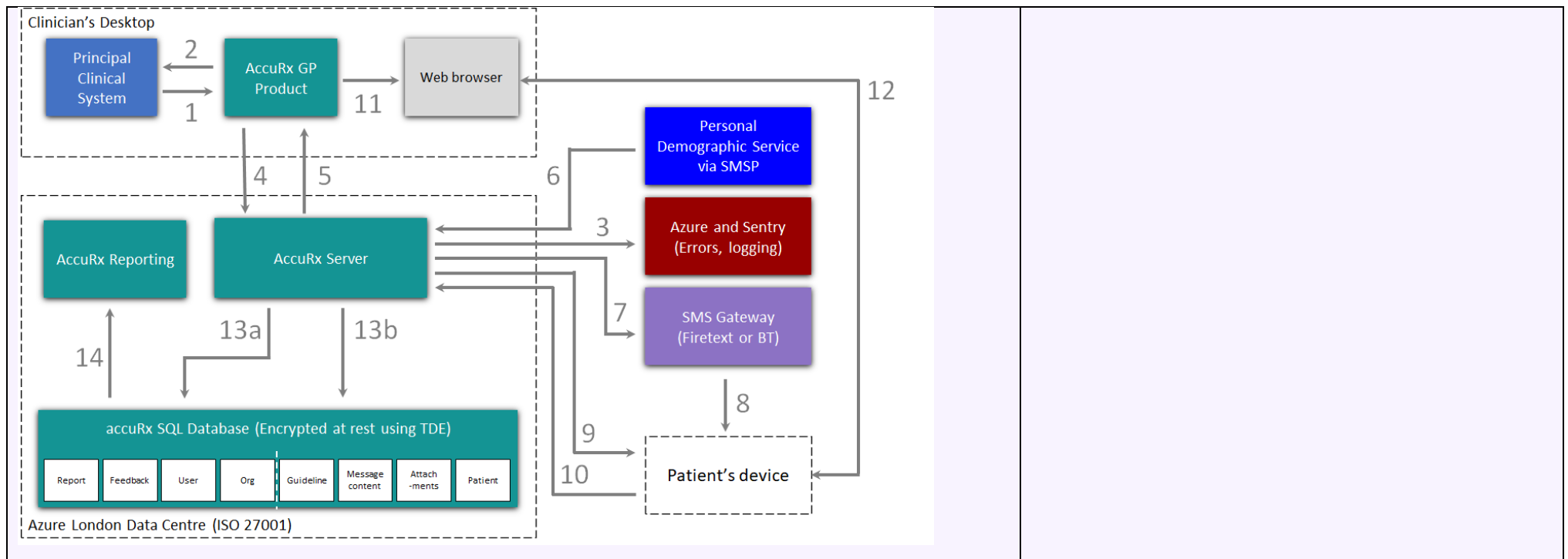
Patients may be asked to submit an image (or multiple images) to the GP practice. The data is collected via a secure web-based form which is accessed via a unique link that the healthcare professional sends to the patient via SMS.

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. However, 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 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 IG Lead, co-signed by a senior clinical representative.

### **Healthcare Messenger**

AccuRx allows GPs to communicate with other healthcare professionals and patients via email, with and about their patient’s care.

The diagram below is an extract from the AccuRX data flow map, obtained from AccuRX which visually showcases the mapping of the data flows.



Number	Data description	Data processed	Method of processing	
1	Principal Clinical System to AccuRx GP Product	<ul style="list-style-type: none"> <li>• Patient demographic details (name; date of birth; gender; NHS number; mobile number; email address)</li> <li>• User ID</li> <li>• User Role (GP, nurse etc)</li> <li>• Organisation (Practice details)</li> </ul>	IM1 API (local to machine)	
2	AccuRx GP Product to Principal Clinical System	<ul style="list-style-type: none"> <li>• Patient demographic details (name; date of birth; gender; NHS number; mobile number; email address)</li> <li>• Content of the communications with – or regarding - patients sent via AccuRx (which may include patient images or documents)</li> </ul>	IM1 API (local to machine)	
3	AccuRx Server to Azure and Sentry	<ul style="list-style-type: none"> <li>• Errors, exceptions, logs (from Principal Clinical System or Chain, to increase stability)</li> </ul>	Https to accuRx specific Azure and Sentry (Slack API URL)	
4	AccuRx GP Product to AccuRx Server	<ul style="list-style-type: none"> <li>• Patient demographic details (name; date of birth; gender; NHS number; mobile number; email address)</li> <li>• Content of the communications with – or regarding - patients sent via AccuRx (which may include patient images or documents)</li> <li>• User ID; User Role (GP, nurse etc); Organisation (Practice details)</li> <li>• Feedback from clinicians (with user and organisation)</li> <li>• Report (tool open/close, advice used, workflow started etc)</li> </ul>	Https with 30 character authentication key installed into machine registry by admin at practice	
5	AccuRx Server to AccuRx GP Product	<ul style="list-style-type: none"> <li>• User and organisation settings (to configure localisation of guidelines, enable extra features)</li> <li>• Download new version of AccuRx GP Product (auto-update)</li> </ul>	Https with 30 character authentication key installed into machine registry by admin at practice	
6	PDS via SMS to AccuRx Server	<ul style="list-style-type: none"> <li>• AccuRx matches ODS code associated with patient to ODS code of user sending patient SMS for data validation</li> </ul>	SMSP interface	
7	AccuRx Server to SMS gateway (Firetext or BT)	<ul style="list-style-type: none"> <li>• Mobile number and SMS message contents (including links to secure web-based patient-response forms)</li> </ul>	Https to Firetext/BT API with unique API key	
8	SMS gateway (Firetext or BT) to Patient's device	<ul style="list-style-type: none"> <li>• SMS message contents (including links to secure web-based patient-response forms)</li> </ul>	SMS	
9	AccuRx Server to Patient's device	<ul style="list-style-type: none"> <li>• Email with link to video consultation</li> </ul>	Email	
10	Patient's device to AccuRx Server	<ul style="list-style-type: none"> <li>• 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)</li> </ul>	Https	
11	AccuRx GP Product to GP Web Browser	<ul style="list-style-type: none"> <li>• Link to video consultation</li> </ul>	Https	
12	GP Web Browser to Patient Web Browser	<ul style="list-style-type: none"> <li>• 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)</li> </ul>	HTTPS and TLS/Secure WebsocketTraffic/Secure WebRTC	
13	AccuRx Server to AccuRx SQL Database	<ul style="list-style-type: none"> <li>a) Feedback and Reports with user/organisation</li> <li>b) Patients (mobile/NHS Number) and SMS message</li> <li>NB: a) and b) aren't linked by any form of ID or foreign key</li> </ul>	Https	
14	AccuRx SQL Database to AccuRx Reporting	<ul style="list-style-type: none"> <li>• Returns list of users, organisations</li> <li>• Aggregate level data (for example, advice usage, tool usage, features used)</li> </ul>	Https with authentication provided by Azure (so only accessible to company employees 2FA)	
What are the data supporting assets?				
GP Practice System of Choice (EMIS/SystemOne), desktop computer or mobile device (laptop, tablet, smart phone), secure internet network, AccuRX platform, Whereby, GP servers such as Microsoft Azure				List the data supporting assets (operating systems, business applications, database management systems, office suites, protocols, configurations, etc.)

## Fundamental principles

### PROPORTIONALITY AND NECESSITY

Are the processing purposes specified, explicit and legitimate?	
Yes - the purpose of processing personal data in this manner is to deliver safe and effective direct care in situations where a normal face-to-face consultation cannot occur. Consultation is for medical purposes and the patient can dissent at any stage by either not clicking on the link to the video consultation or leaving the video consultation.	Explain why the processing purposes are specified, explicit and legitimate. How is the legal basis being specified?
What is the lawful basis for processing the data?	
<p>The lawful basis for processing the data is the provision of direct patient care, which is defined under Articles 6 and 9 of the General Data Protection Regulations (GDPR) and aligned through the Data Protection Act 2018. Article 6 defines the legal basis with article 9 a requirement when using special categories of data.</p> <p><b>Article 6</b></p> <p>- 6(1)(e) processing is necessary for the <b>performance of a task carried out in the public interest</b> or in the exercise of official authority vested in the controller.</p> <p><b>Article 9</b></p> <p>- 9(2)(h) – Processing is necessary for the purposes of preventative or occupational medicine, for assessing the working capacity of the employee, <b>medical diagnosis, the provision of health or social care or treatment or management of health or social</b></p>	What is the legal basis for processing the data? – direct care, legislation, or consent, (do not forget, consent should be a last resort and only used if there is no direct care or legislation in place). Remember to identify which Article 6 or 9 conditions will be used and if there is supporting legislation, what that legislation is, including the specific section of the legislation which supports the use of data for this purpose.

<p><b>care systems</b> and services on the basis of Union or Member State law or a contract with a health professional.</p>	
<p>Is the data collected adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed ('data minimisation')?</p>	
<p>To facilitate effective direct care needs of the patient all clinical information will need to be accessed. However, to ensure only data that is necessary for the purpose that they are processed is accessed, the video and audio is not retained by AccuRx or Whereby. Non-identifiable usage data is retained for service evaluation and improvement.</p>	<p>Need confirmation in here that there is no personal data being processed that is not absolutely necessary for the purpose of the project. Is any information being collected that is not required to complete the project?</p>
<p>Is the data accurate and kept up to date?</p>	
<p>The consultation will be summarised onto the electronic primary care record of the patient, in exactly the same way as is done with face-to-face or telephone consultations. Healthcare professionals should ensure that this is done as soon as possible if not contemporaneously. It remains the responsibility of the GP Practice, in their role as data controller, to ensure records are maintained accurately and kept up to date at all times. They must therefore have robust Data Quality procedures implemented with all staff trained on how and when to update records, and regular audits must be undertaken to ensure the practice records remain accurate and up to data.</p>	<p>Describe what steps are taken to ensure the quality of the data. Need confirmation here of who will check the data is accurate and what process is in place to ensure the data is kept up to date.</p>

## What is the storage duration of the data?

The video and audio are not retained by AccuRx or Whereby. However, in the video consultation the healthcare professional must update the observations and outcome of the consultation in the same way as a face-to-face consultation is updated in the patient's electronic primary care record and any agreed actions must be carried out. Any images, documents and messages between the patient and clinician and personal data processed as a result of the video consultation, is retained within the patient's electronic primary care record as per the NHS Records Management Code of Practice for Health and Social Care 2016. Information stored in the patient's primary care records are retained for the lifetime of the patient and then 10 years after death.

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. It is not routinely possible for AccuRX to access patient photographs and images, however as with other record systems, AccuRX are required to be able to access patient data in exceptional circumstances to fulfil legal obligations as a data processor, such as assisting the GP Practice as data controller in providing subject access and allowing data subjects to exercise all of their rights under GDPR/DPA18. If such access is required only designated AccuRX staff can access the data stored on the London Microsoft Azure Data Centre servers. Extensive controls are in place, a full audit trail is kept, and no staff member would view any patient images as part of this process.

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.


Ideally there will be a list here of all the data assets being processed, how long they will be held for, where the timescales have come from (i.e., Information Governance Alliance code of practice for records management). This should be stated for each organisation that holds the data.

Records Management Code of Practice for Health and Social Care 2016: <https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/codes-of-practice-for-handling-information-in-health-and-care/records-management-code-of-practice-for-health-and-social-care-2016>

## CONTROLS TO PROTECT THE PERSONAL RIGHTS OF DATA SUBJECTS

How are the data subjects informed of the processing?	
<p>It is the responsibility of every GP Practice to ensure that as data controllers, they inform their patients under the 'Right to be Informed' detailed in the Data Protection Act 2018. They must ensure the use of AccuRX is detailed in their practice privacy notice and uploaded both to the website and within practice. Any easy-to-read privacy notices, notices produced in other formats or notices translated into other languages, must also contain this information. Practices may wish to produce information leaflets on the use of AccuRX or signpost patients to the AccuRX website for additional information, but the information cascaded to patients must be transparent, easy to understand and specific. AccuRX have a data security and privacy notice on their website which must also be referenced:</p> <p><a href="https://www.accurx.com/data-security-and-privacy">https://www.accurx.com/data-security-and-privacy</a></p>	<p>In here you would expect that privacy notices are made available to the data subjects and information and advice, perhaps even leaflets, about how data subjects can access privacy notices.</p>
If consent is your lawful basis how is the consent of data subjects obtained?	
<p>Consent is not the lawful basis – any patient who does not wish to consult with their clinician via AccuRX would simply not access the link provided and make their preferences to the GP Practice</p>	<p>If consent is not your legal basis, then this should say not applicable. If consent is the legal basis, then this should advise how the consent is obtained, what information is given to the data subject when obtaining consent about what data will be used and for what purpose, how the consent is recorded and what information is given to the data subject about how they can withdraw their consent.</p>
How can data subjects exercise their rights of access and to data portability?	

<p>The GP Practice will process any subject access requests made by patients adhering to the practice Subject Access Request policies. Any information updated into the records following an AccuRX consultation will form part of the release of records and will also adhere to the stipulations of the AccuRX data processing agreement. Patients have the right to request their information in any accessible format in relation to their right to data portability and it is the practice responsibility to meet their requested format as far as practically possible.</p>	<p>Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests</p>
<p>How can data subjects exercise their rights to rectification and erasure?</p>	
<p>Under Article 16 of the GDPR data subjects have the right to have inaccurate data rectified. The GP Practice in their role as data controller must ensure that they have robust policies in place to ensure patients can request rectification of their information and forms part of the Data Quality process each practice must implement to ensure records are accurate and kept up to date. In relation to erasure, this must only be done in cases where clinical validation has been received and only when full assessment has been undertaken and must only be done on a case-by-case basis.</p>	<p>Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests</p>
<p>How can data subjects exercise their rights to restriction and to object?</p>	
<p>A data subject can exercise their right to restrict and to object only in certain cases but when the legal basis relies on public task, carrying out the data processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller those rights will apply. It is harder to restrict or object when the purpose meets direct care purposes however the data subject must give specific reasons why they object to the processing of their data and the reasons need to be based on their particular situation. The GP practice must clearly detail the rights and freedoms of the individual in the practice privacy notice</p>	<p>Need confirmation in here that all data controllers involved in the project have local processes in place to respond to data subjects' individual rights requests</p>
<p>If there is a Data Processor involved, are the obligations of the processors clearly identified and governed by a contract?</p>	

<p>Data processor obligations are defined within the following contract between the GP practice and AccuRx:</p>  <p>200524_AccuRx_DP A-docx.pdf</p>	<p>If a data processor is involved, this should fully explain who the processor is and what their role is in relation to the processing. Need confirmation that there is a data processing agreement and/or contract in place between the data controller and the data processor which stipulates what the data processor will be doing with the data.</p> <p>If there is no data processor, then consideration should be made to a data sharing agreement being put in place.</p>
<p>In the case of data transfer outside the United Kingdom, are the data adequately protected?</p>	
<p>Whereby are based in the European Economic Area (EEA). All communication between the healthcare professional's browser, or the patient's browser, and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure web socket traffic or secure WebRTC). Furthermore, the video consultation connection prioritises 'peer-to-peer' connections between the healthcare professionals 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 healthcare professional and patient are using their computer devices in the European Economic Area, it is guaranteed that any data hosted on a server is within the EEA in line with NHS best practice guidelines on health and social care cloud security. Not to store or directly transfer the Personal Data/Special Categories of Personal Data</p> <p>However, it is important to note:</p> <ul style="list-style-type: none"> <li>• A clinician 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.</li> <li>• A patient may be receiving messages whilst outside of the EEA.</li> </ul>	<p>This should confirm if any data is being transferred outside of the UK, this includes where servers, for systems being used, are based. If data is being transferred outside of the UK, then strict assurances need to be in place that where the data is being transferred to will meet GDPR compliance and a contract in place.</p>

## Risks

This section allows you to assess the privacy risks, considering existing or planned controls.

Risk Factors to consider:

- Illegitimate access to data.
- Unwanted modification of data
- Data disappearance

## PLANNED OR EXISTING MEASURES

See appendix A for information on working out Risk Likelihood and Severity

#	Risk Ref	Risk Description	Mitigating Control(s)/Actions	Likely	Severity	Score
			(See details below)	(See details below)		
1	Risk of data being shared	Access to personal data by persons other than the data subject.	Consultation is not video recorded, and no personal data is stored by the supplier	Low	Low	Low
2	Risk that devices do not meet required standards	The integrity of the computers used (how at risk are they from trojans or viruses)	Use of devices that complies with NHS standards of encryption	Low	Low	Low
3	Risk of inadvertently sharing other	The healthcare professional would need to ensure that there was no third-party data	Healthcare professionals can view what the patient views in the video consultation. Therefore, any third-party data could be	Moderate	Moderate	Moderate

	personal data via the consultation	visible on desks or screens that could be viewed or captured by the individual	identified and blocked. by the healthcare professional			
4	Risk of third-party presence or coercion	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.	Moderate	Moderate	Moderate
5	Risk of infiltration	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 could immediately see when another participant joins the call and end the call.	Low	Low	Low
6	Risk that key agreements are not in place following the Brexit transition period	As Whereby are sub-processors based outside of the United Kingdom, risk that contracts do not meet UK legislation	When the UK end the transition period, agreements need to be reviewed to ensure they meet legislative requirements when using a non-UK processor or sub-processor for UK data activities	Moderate	Moderate	Moderate
7	Risk of sensitive data sent via SMS	Risk of the practice using the AccuRX SMS service to send non-generic, sensitive information via text	To ensure practice standard operating procedures are implemented, and the standardised templates developed by AccuRX are used to send communications out to patients	Low	Moderate	Low
8	Patients may not use the link correctly	Patients may attempt to respond to the GP question by texting back rather than following the link to respond	To ensure patients are provided with key usage information and an acceptable use policy adopted by the practice to ensure patients understand how to use AccuRX	Low	Moderate	Low

			appropriately. Also, the patient will receive a message informing them they cannot reply via that method and must use the AccuRX link for communicating, sending documents or images.			
--	--	--	---	--	--	--

EXAMPLES of risks - FOR INFORMATION ONLY	
<b>Education</b>	Breach of IG policies and guidance due to lack of visibility, communication, and training
<b>GDPR</b>	Non-compliant with GDPR implementation
<b>Malware</b>	Threat from malicious links/ attachments
<b>Process</b>	Information is lost/ processed in a non-compliant manner due to gaps in processes and poor controls
<b>Purchasing</b>	Limited governance over low spends allows DPIA process bypass
<b>Sharing</b>	Sharing information inappropriately or illegally due to immature technology or understanding of legislation
<b>Supplier</b>	Suppliers breach Privacy Law due to poor information handling practices/ IT security

#### Appendix A

<b>Encryption</b>	Means implemented for ensuring the confidentiality of data stored (in the database, in flat files, backups, etc.), as well as the procedure for managing encryption keys (creation, storage, change in the event of suspected cases of data compromise, etc.). Describe the encryption means employed for data flows (VPN, TLS, etc.) implemented in the processing.
<b>Anonymisation</b>	Indicate here whether anonymization mechanisms are implemented, which ones and for what purpose. Remember to clearly distinguish between anonymous and pseudonymous data.
<b>Partitioning</b>	Implementation of data partitioning helps to reduce the possibility that personal data can be correlated and that a breach of all personal data may occur.
<b>Logical Access Control</b>	Methods to define and attribute users' profiles. Specify the authentication means implemented. Where applicable, specify the rules applicable to passwords (minimum length, required characters, validity duration, number of failed attempts before access to account is locked, etc.).
<b>Traceability (logging)</b>	Policies that define traceability and log management.
<b>Archiving</b>	Where applicable, describe here the processes of archive management (delivery, storage, consultation, etc.) under your responsibility. Specify the archiving roles (offices of origin, transferring agencies, etc.) and the archiving policy. State if data may fall within the scope of public archives.
<b>Paper document security</b>	Where paper documents containing data are used during the processing, indicate here how they are printed, stored, destroyed, and exchanged.
<b>Minimising the amount of personal data</b>	The following methods could be used: Filtering and removal, reducing sensitivity via conversion, Reducing the identifying nature of data, reducing data accumulation, Restricting data access

## Physical Security Control

<b>Operating security</b>	Policies implemented to reduce the possibility and the impact of risks on assets supporting personal data.
<b>Clamping down on malicious software</b>	Controls implemented on workstations and servers to protect them from malicious software while accessing less secure networks.
<b>Managing workstations</b>	Controls implemented on workstations (automatic locking, regular updates, configuration, physical security, etc.) to reduce the possibility to exploit software properties (operating systems, business applications etc.) to adversely affect personal data.
<b>Website security</b>	Implementation of ANSSI's Recommendations for securing websites.
<b>Backups</b>	Policies and means implemented to ensure the availability and/or integrity of the personal data, while maintaining their confidentiality.
<b>Maintenance</b>	Policies describing how physical maintenance of hardware is managed, stating whether this is contracted out. Indicate whether the remote maintenance of apps is authorized, and according to what arrangements. Specify whether defective equipment is managed in a specific manner.
<b>Processing Contracts</b>	<p>Regulate the procurement relations via a contract signed intuitu personæ.</p> <ul style="list-style-type: none"> <li>- Require the processor to forward its Information Systems Security Policy (PSSI) along with all supporting documents of its information security certifications and append said documents to the contract. Ensure that the measures pursuant to its PSSI comply with the ICO's recommendations in this respect.</li> <li>- Precisely determine and set, on a contractual basis, the operations that the processor will be required to carry out on personal data: <ol style="list-style-type: none"> <li>1) The data to which it will have access or which will be transmitted to it.</li> <li>2) The operations it must carry out on the data.</li> <li>3) The duration for which it may store the data.</li> <li>4) Any recipients to which the data controller requires it to transmit the data.</li> <li>5) The operations to be carried out at the end of the service (permanent deletion of data or return of the data in the context of reversibility then destruction of data at the processor's).</li> <li>6) The security objectives set by the data controller.</li> </ol> </li> <li>- Determine, on a contractual basis, the division of responsibility regarding the legal processes aimed at allowing the data subjects to exercise their rights.</li> <li>- Explicitly prohibit or regulate use of tier-2 processors.</li> <li>- Clarify in the contract that compliance with the data protection obligations is a binding requirement of the contract.</li> </ul>
<b>Network security</b>	Depending on the type of network on which the processing is carried out (isolated, private or Internet). Specify which firewall system, intrusion detection systems or other active or passive devices are in charge of ensuring network security.
<b>Physical access control</b>	Policies to ensure physical security (zoning, escorting of visitors, wearing of passes, locked doors and so on). Indicate whether there are warning procedures in place in the event of a break-in.

<b>Monitoring network activity</b>	Monitor intrusion detection systems and intrusion prevention systems in order to analyse network (wired networks, Wi-Fi, radio waves, fibre optics, etc.) traffic in real time and detect any suspicious activity suggestive of a cyber-attack scenario.
<b>Hardware security</b>	Indicate here the controls bearing on the physical security of servers and workstations (secure storage, security cables, confidentiality filters, secure erasure prior to scrapping, etc.).
<b>Avoiding sources of risk</b>	Documentation on implantation area, which should not be subject to environmental disasters (flood zone, proximity to chemical industries, earthquake, or volcanic zone, etc.). Specify if dangerous products are stored in the same area.
<b>Protecting against non-human sources of risks</b>	Policies describing the means of fire prevention, detection and fighting. Where applicable, indicate the means of preventing water damage. Also specify the means of power supply monitoring and relief.

## Organisational Control

<b>Organisation</b>	Specify whether a person is responsible for the enforcement of privacy laws and regulations. Specify whether there is a monitoring committee (or equivalent) responsible for the guidance and follow-up of actions concerning the protection of privacy.
<b>Policy</b>	Set out important aspects relating to data protection within a documentary base making up the data protection policy and in a form suited to each type of content (risks, key principles to be followed, target objectives, rules to be applied, etc.) and each communication target (users, IT department, policymakers, etc.).
<b>Managing Privacy risks</b>	Policy describing processes to control the risks that processing operations performed by the organization pose on data protection and the privacy of data subjects (building a map of the risks, etc.)
<b>Integrating privacy protection in projects</b>	Existence of a policy designed integrate the protection of personal data in all new processing operations.
<b>Managing personal data violations</b>	Existence of an operational organization that can detect and treat incidents that may affect the data subjects' civil liberties and privacy.
<b>Personnel management</b>	Existence of a policy describing awareness-raising controls are carried out with regard to a new recruit and what controls are carried out when persons who have been accessing data leave their job.
<b>Relations with third parties</b>	Existence of a policy and processes reducing the risk that legitimate access to personal data by third parties may pose to the data subjects' civil liberties and privacy.
<b>Supervision</b>	Existence of a policy and processes to obtain an organization able to manage and control the protection of personal data held within it.

## Severity Definitions

Severity	Description
Negligible severity	<p>Data subjects either will not be affected or may encounter a few inconveniences, which they will overcome without any problem.</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>- physical : transient headaches</li> <li>- material : loss of time in repeating formalities or waiting for them to be fulfilled, receipt of unsolicited mail (e.g.: spams), reuse of data published on websites for the purpose of targeted advertising , etc.,</li> <li>- moral : mere annoyance, feeling of invasion of privacy without real or objective harm (commercial intrusion), etc.</li> </ul>
Limited severity	<p>Data subjects may encounter significant inconveniences, which they will be able to overcome despite a few difficulties</p> <p>Examples :</p> <ul style="list-style-type: none"> <li>- physical : minor physical ailments (minor illness due to disregard of contraindications), defamation resulting in physical or psychological retaliation, etc.</li> <li>- material : Unanticipated payments (fines imposed erroneously), denial of access to administrative or commercial services , Receipt of unsolicited targeted mailings likely to damage the reputation of data subjects, etc.</li> <li>- moral : minor but objective psychological ailments, feeling of invasion of privacy without irreversible damage, intimidation on social networks, etc.</li> </ul>
Significant severity	<p>Data subjects may encounter significant consequences, which they should be able to overcome albeit with real and serious difficulties</p> <p>Examples:</p> <ul style="list-style-type: none"> <li>- physical : serious physical ailments causing long-term harm (worsening of health due to improper care, or disregard of contraindications), iteration of physical integrity for example following an assault, an accident at home, work, etc.</li> <li>- material : misappropriation of money not compensated, targeted, unique and non-recurring, lost opportunities (home loan, refusal of studies, internships or employment, examination ban), loss of housing, loss of employment, etc.</li> <li>- moral : serious psychological ailments (depression, development of a phobia), feeling of invasion of privacy with irreversible damage, victim of blackmailing, cyberbullying and harassment, etc.</li> </ul>
Maximum severity	<p>Data subjects may encounter significant, or even irreversible, consequences, which they may not overcome</p> <p>Examples :</p> <ul style="list-style-type: none"> <li>- physical : long-term or permanent physical ailments, permanent impairment of physical integrity, death</li> <li>- material : financial risk, substantial debts, inability to work, inability to relocate, loss of evidence in the context of litigation, loss of access to vital infrastructure (water, electricity), etc.</li> <li>- moral : long-term or permanent psychological ailments, criminal penalty, abduction, loss of family ties, inability to sue, change of administrative status and/or loss of legal autonomy (guardianship), etc.</li> </ul>

Severity	Description
Negligible likelihood	<p>It does not seem possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in a room protected by a badge reader and access code).</p>

In accordance with the <b>Risk Treatment Process</b>	
Score	Risk Class
1	Negligible
2	Limited
3	Significant
4	Maximum

Limited likelihood	It seems difficult for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in a room protected by a badge reader).
Significant likelihood	It seems possible for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in offices that cannot be accessed without first checking in at the reception).
Maximum likelihood	It seems extremely easy for the selected risk sources to materialize the threat by exploiting the properties of supporting assets (e.g.: theft of paper documents stored in the public lobby).

		Severity			
		Negligible (1)	Limited (2)	Significant (3)	Maximum (4)
Likelihood	Maximum (4)	Medium (4)	High (8)	Very High (12)	Very High (16)
	Significant (3)	Medium (3)	High (6)	High (9)	Very High (12)
	Limited (2)	Low (2)	Medium (4)	High (6)	High (8)
	Negligible (1)	Low (1)	Low (2)	Medium (3)	Medium (4)