

DPIA

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

NB: as the data controller, when using AccuRx, it is at your practice's discretion as to whether you complete a DPIA. As a data processor, we cannot complete it for you. However, to be as helpful as we can, we have filled in the key parts of a template DPIA for video consultations using AccuRx.

Submitting controller details

Name of controller	Chapelgreen Practice
Subject/title of DPO	SMS messaging using AccuRx
Name of controller contact /DPO (delete as appropriate)	Chapelgreen Practice DPO Paul Couldrey


Step 1: Identify the need for a DPIA

Explain broadly what the project aims to achieve and what type of processing it involves. You may find it helpful to refer or link to other documents, such as a project proposal. Summarise why you identified the need for a DPIA.

The aim of the service is to improve communications between healthcare staff and patients to improve outcomes and productivity. The video consultation service is designed for mass adoption of remote consultation that doesn't require webcams, implementation managers, patients to register for an account or download an application.

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; and, perform video consultations (which are not recorded or stored) between healthcare staff and their patients.

Please see [here](#) for demonstrations of all the features in Chain.



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? You might find it useful to refer to a flow diagram or other way of describing data flows. What types of processing identified as likely high risk are involved?

The health organisation is the data controller, and AccuRx the data processor, as per [AccuRx's Data Processing Agreement](#).

Video

Consultations

In the video consultation, the clinician will record the observations and outcome of the consultation in the same way as a face-to-face consultation is recorded in the patient's electronic primary care record and any agreed actions are carried out.

The video consultation service is hosted by Whereby who are fully compliant with GDPR. The video and audio communication is only visible to participants on the call and is not recorded or stored on any server. The connection prioritises 'peer-to-peer' between the clinician's and patient's phone and follows [NHS best practice guidelines](#) on health and social care cloud security.

Messaging

The messaging feature allows NHS staff to instantly send SMS text messages to patients. Typical use-cases for this include sending a link to video consultations, advice to patients, notifying a patient of normal results, and reminding them to book appointments.

Patient Responses

AccuRx allows users 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.

Documents

AccuRx have developed a feature that allows healthcare staff to send files or documents (such as sick notes, leaflets, letters, imaging request forms, blood forms, etc.) via SMS to patients. The document is accessible for 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. The user flow is:

1. Click "Attach file" right underneath the "Message text" box in the main UI
2. Once clicked, it will launch the Windows file picker where the user can select a file to attach (file formats supported: .pdf, .docx, .doc, .jpeg, .jpg, .png, .tiff, .tiff.xx2)
3. Once sent, what the patient receives is an SMS to their mobile phone with a link
4. When they click on the link, they will be asked to input their date of birth as identity verification, before being able to access the document

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?

Healthcare staff data (typically name, role, organisation, contact details, identifiers including gender and DoB, messages, metadata, signatures, login and other application-use related data) and patient data (typically name, identifiers, contact details, demographic data, messages content, documents/notes, survey responses, metadata). The video and audio communication of any video consultation is only visible to participants on the call, and is not recorded or stored on any server. The IP address of call participants may be stored as part of metadata stored, however no other personal information of call participants is collected or stored.

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. Users 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.

Video Consultation *(detailed)*

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

[best practice guidelines](#) on health and social care cloud security.

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 call 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.

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 healthcare staff providing direct care to patients. The nature of the relationships with the individuals participating in any video consultations is identical to that of face-to-face consultations between clinicians and their patients. In the video consultation the clinician will record the observations and outcome of the consultation in the same way as a face-to-face consultation is recorded in the patient's electronic primary care record and any agreed actions are carried out.

The use of video consultation via AccuRx is more secure than speaking to patients by phone. The connection prioritises 'peer-to-peer' between the clinician's and patient's phone in line with the principle of data minimisation. Most phones are Voice over Internet Protocol (VoIP). However, phone connections typically include personal information (such as patient phone number). In contrast, the AccuRx video consultation does not use any personal demographic information as it is initiated via a unique URL which does not use any patient or user information. AccuRx specifically selected Whereby services to host video consultations because it fulfilled AccuRx privacy by design requirements in not using any personal demographic data for the calls.

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. The purpose of using video consultations on the AccuRx platform is to minimise face-to-face contact between healthcare staff and their patients as [advised by the NHS](#) in the delivery of healthcare.

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 3,500 GP practices. Over 12,000 video consultations have been completed in the first week of its release. AccuRx has also engaged patients and CCIOs on its Information Governance and Data Protection approach.

Step 4: Assess necessity and proportionality

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

The [lawful bases](#) of healthcare staff using the AccuRx platform for communicating with patients is 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

Users are authenticated by requiring: NHSmail to register for an account; TPP SystemOne 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 SystemOne or EMIS Web principal care systems. This ensures that a user can only access data of patients registered at their practice.

Patient Responses

Patient survey links are sent via SMS directly to a patient's mobile phone. The links are encrypted in transit via HTTPS and responses are [encrypted at rest](#) via TDE. Patients are also asked to input their date of birth as identity verification, before being able to access the survey.

Documents

Links to files or documents sent via SMS by healthcare staff directly to a patient's mobile phone are encrypted in transit via HTTPS and responses are [encrypted at rest](#) via TDE. Patients are also asked to input their date of birth as identity verification, before being able to access the document. The document is only accessible for 14 days.

Video Consultation

The NHS have approved AccuRx's Information Governance approach (see [here](#)) to video consultation. Please also see below for an assessment of compliance against the principles of the Data Protection Act:

Principle	Assessment of Compliance
<p>Principle 1 – (2.21 2.23) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –</p> <p>(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</p>	<p>Patient consents to take part in the process by clicking on the link to the video consultation. They can dissent at any point by either not clicking on the link to the video consultation or leaving the video consultation.</p>
<p>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.</p>	<p>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.</p>
<p>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.</p>	<p>The video and audio is not retained by AccuRx or Whereby. Non-identifiable usage data is retained for service evaluation and improvement.</p>
<p>Principle 4 – () 2.12 Personal data shall be accurate and, where necessary, kept up to date.</p>	<p>The consultation should be summarised on to the electronic medical record as with a face-to-face or telephone consultation. Healthcare professionals should ensure that this is done as soon as possible if not contemporaneously.</p>
<p>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.</p>	<p>The video and audio is not retained by AccuRx or Whereby. However, in the video consultation the clinician may record the observations and outcome of the consultation in the same way as a face to face consultation is recorded in the patient's electronic primary care record and any agreed actions are carried out.</p>
<p>Principle 6 – (2.22& 2.23) Personal data shall be processed in accordance with the rights of data subjects under this Act.</p>	<p>Patient agrees to take part in the process by clicking on the link to the video consultation. They can dissent at any point by either not clicking on the link to the video consultation or leaving the video consultation.</p>
<p>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.</p>	<p>Computer equipment is secure and complies with the NHS standard 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 user's browser, or the patient's browser, and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure websocket traffic or secure WebRTC). No demographic information (such as names of the participants) is collected or stored by Whereby.</p>
<p>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.</p>	<p>Whereby are based in the European Economic Area (EEA). All communication between the user's browser, or the patient's browser, and Whereby's service is transmitted over an encrypted connection (secure web traffic using HTTPS and TLS or secure websocket traffic or secure WebRTC). Furthermore, the video consultation connection prioritises 'peer-to-peer' connections between the clinician's and patient's phone over connections via their servers. In some cases, due to NAT/firewall restrictions, the encrypted data content will be relayed through Whereby's TURN server, but never recorded or stored. In such cases, as long as both the clinician and patient are using their computer devices in the European Economic Area, it is guaranteed that any data hosted on a server is within the EEA in line with</p>

[NHS best practice guidelines](#) on health and social care cloud security.

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	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 user	Remote	Significant	Low
The integrity of the computers used (how at risk are they from trojans or viruses)	Remote	Minimal	Low
The clinician would need to ensure that there was no third-party data visible on desks or screens that could be viewed or captured by the individual in any video call	Remote	Minimal	Low
A third party is present in the room of one of the video consultation participants without the other participant knowing	Remote	Significant	Low
A third party guesses the URL of a video	Remote	Minimal	Medium

consultation and joins the call			
---------------------------------	--	--	--

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	<p>Users are authenticated by requiring: NHSmail to register for an account; TPP SystemOne 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.</p> <p>Patient demographic data is only pulled from either TPP SystemOne or EMIS Web principal care systems. This ensures that a user can only access data of patients registered at their practice.</p> <p>Any video consultations are not recorded or stored.</p>	Eliminated	Low	Yes
Incorrect patient data selected for SMS	<p>Patient demographic data is only pulled from either TPP SystemOne or EMIS Web principal care systems. This ensures that a user can verify the correct information with the patient before sending</p>	Reduced	Low	Yes

	<p>an SMS.</p> <p>Users 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.</p> <p>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.</p>			
Sensitive data being sent via SMS	<p>Users 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.</p> <p>Full audit trails are kept of all user activity for clinical safety purposes.</p>	Reduced	Low	Yes
Abusive messages are sent to patients by a user	<p>AccuRx scans SMSs for abusive content and flags to its Clinical Lead if any are detected.</p> <p>Full audit trails are kept of all user activity for clinical safety purposes.</p>	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

The clinician would need to ensure that there was no third-party data visible on desks or screens that could be viewed or captured by the individual in any video call	Clinicians can view what the patient views in the video consultation. Therefore, any third-party data could be identified and blocked by the clinician.	Reduced	Low	Yes
A third party is present in the room of one of the video consultation participants without the other participant knowing	Participants can ask the other participant to scan the room with the camera if either are concerned.	Reduced	Medium	Yes
A third party guesses the URL of a video consultation and joins the call	Each URL generated is completely unique, rendering it almost impossible to guess by a third party. They would also have to guess it at precisely the same time other participants are in the virtual meeting room. Even if they did both of those (incredibly unlikely) things, participants can immediately see when another participant joins the call and end the call.	Eliminated	Low	Yes

Step 7: Sign off and record outcomes

Item	Name/position/date	Notes
Measures approved by:	Blake Foster, Practice Manager	Integrate actions back into project plan, with date and responsibility for completion
Residual risks approved by:	Justin Croft, Caldicott Gaurdian	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:	Blake Foster, Practice Manager	The DPO should also review ongoing compliance with DPIA