

| | |
|--------------------|--|
| Name of controller | Queen Camel Medical Centre |
| Subject of DPO | Video consultations using AccuRx |
| Name of DPO | Kevin Caldwell, Somerset CCG somccg.GPDPO@nhs.net |

The use of AccuRx platform for video consultations between healthcare staff and their patients. This 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.

Text Messaging

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

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

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.

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 principal 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.

The purpose of using video consultations on the AccuRx platform is to minimise face-to-face contacts between healthcare staff and their patients as advised by NHS England on 5th March 2020 in the delivery of healthcare.

Views have been gathered from AccuRx users across 3,500 GP practices. Over 1,300 practices have completed 2,000 video consultations in the 48 hours (since March 9th) using AccuRx.

The lawful basis of healthcare staff performing consultations via video 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...’

Data Protection Act:

| Principle | Assessment of Compliance |
|--|---|
| Principle 1 – (2.21 2.23) Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless – (a) at least one of the conditions in Schedule 2 is met, and (b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met | Patient consents to take part in the process by clicking on the link 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. |
| 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. | 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. |
| 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 video and audio is not retained by AccuRx or Whereby. Non-identifiable usage data is retained for service evaluation and improvement. |
| Principle 4 – () 2.12 Personal data shall be accurate and, where necessary, kept up to date. | 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. |
| Principle 5 – (2.20) Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. | The 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. |
| 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 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. |
| 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. 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. |
| 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. | 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. |

| 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 |
| 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 | 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 consultation and joins the call | Remote | Minimal | Medium |

| 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. | Consultation is not video recorded | Eliminated | Low | Yes |
| 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 | 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 | 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 | Eliminated | Low | Yes |
| | 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. | | | |

| Item | Name/position/date | Notes |
|-----------------------------|---------------------------|---|
| Measures approved by: | Partners 07.5.20 | Integrate actions back into project plan, with date and responsibility for completion |
| Residual risks approved by: | Partners 07.5.20 | If accepting any residual high risk, consult the ICO before going ahead |

| | | |
|---|-----------------|---|
| DPO advice provided: | N/A | DPO should advise on compliance, step 6 measures and whether processing can proceed |
| Summary of DPO advice: | | |
| DPO advice accepted or overruled by: | N/A | If overruled, you must explain your reasons |
| Comments | | |
| Consultation responses reviewed by: | N/A | If your decision departs from individuals' views, you must explain your reasons |
| Comments: | | |
| This DPIA will be kept under review by: | Linda Bickerton | The DPO should also review ongoing compliance with DPIA |