**PCIG Consulting**

# Video Consultation Policy

**Version:** **1.0**
**Date:** **30 March 2020**

**This template is for use by Practices to Comply with the GDPR requirement to have a policy regarding processing of patient data. The template is Generic in design as PCIG Consulting have clients across the UK, local sharing arrangements and area specific sharing or processing will need to be added by the practice.**

**Change Control**

| Version | To | Change | Date |
|---|---|---|---|
| 1 | | New Policy | 30/03/2020 |
| | | | |

**Chapelgreen Practice**

# Video Consultation Policy

## Document History

| | |
|---|---|
| Document Reference: | |
| Document Purpose: | Video Consultation Policy |
| Date Approved: | |
| Version Number: | 1.0 |
| Status: | FINAL |
| Next Revision Due: | March 2021 |
| Developed by: | Paul Couldrey – IG Consultant |
| Policy Sponsor: | Practice Manager |
| Target Audience: | This policy applies to any person directly employed, contracted, working on behalf of Chapelgreen Practice or volunteering with the Practice. |
| Associated Documents: | All Information Governance Policies and the Information Governance Toolkit, and Data Security and Protections Toolkit 2020 |

## 1.0 Introduction

1.1 This policy is intended to identify how Chapelgreen Practice will administer video consultation (Video Consultation Appointments (VCA)) especially as a response to the current COVID-19 pandemic.

1.2 Video Consultation Appointments (VCA) is an alternative way to provide outpatient appointments. VCA offers another way to consult with a patient by video either at their home, or at any other appropriate location, with the aim to reduce patient travel and the associated expense. VCA is an option for those patients deemed clinically appropriate by their Clinician, if also accepted by the patient, to replace their existing face to face appointments. Use of VCA within the relevant services is about offering patients a choice of receiving their consultations differently.

## 2.0 Purpose

2.1 To ensure that Chapelgreen Practice and it's staff comply with legislation and NHS standards in respect of information security and the requirements of the NHS in respect of securing personal data and Chapelgreen Practice use of VCA.

## 3.0 Statement of Intent

3.1 It is intended that Chapelgreen Practice complies with NHS and legal requirements for the VCA and the policy is written in accordance with NHSE Using Online Consultations in Primary Care toolkit (September 2019), found here: -

https://www.england.nhs.uk/wp-content/uploads/2019/09/online-consultations-summary-tocolkit-for-practices-dec-2019.pdf

3.2 The benefits of using VCA are:-

- Ability to pick up on visual cues and carry out a visual examination
- May offer advantages in building rapport and facilitating understanding through non-verbal communication compared to other remote consulting methods
- May be used for ward rounds in a care home, housebound patients, supporting members of your MDT visiting patients. Clinicians can see and update patient records in real time
- Support PCN working

However, the Risks are: -

- Relies on the doctor and patient being available at the same time, hence may not be exempt from long waiting times or delays
- Problems with the technology can disrupt the consultation.
- Patients and the practice require the right equipment with the appropriate IT infrastructure

- Patients may need to download an app and use some of their data allowance to undertake a video consultation

3.3 NHSX are encouraging the use of videoconferencing to carry out consultations with patients and service users. This could help to reduce the spread of COVID-19. NHSX have advised that it is acceptable to use video conferencing tools such as Skype as well as commercial products designed specifically for this purpose – a short Data Protection Impact Assessment should be completed if this is a new way of working. (APPENDIX A Template)

## 4.0 Process

- Appointment should be booked with patient asking them to opt into VCA at time of making the appointment see 4.1
- The process requires anyone using the service to prove their identity and restrict access only to authorised users, helping to ensure a confidential and secure service.
- Where patients have consented to carers, parents or relatives communicating with the practice using online consultations, they should have a separate identity verification process and be granted authorisation by proxy. The patient proxy verification should meet the same standards as used for patient identity verification see 4.2.
- A consent should be obtained from the patient during the VCA to record the consultation (verbal consent will suffice).
- Post-consultation procedure: including the right of the patient to view the consultation, actions agreed, next-steps and advice should be given clearly before the termination of the VCA.
- Storage and erasure: VCA forms part of the Medical Records and as such should stored as per other patient medical records in accordance with the practice Records Management Policy.

4.1 Patient Verification

Measures to verify the patient is registered at the practice and their details match those recorded in the clinical system, on calling (VCA) the patient – if the patient is well and able to speak to the clinician directly then you should first undertake a basic identification process. Ask the patient their full name, date of birth and full address. Once they have completed this, explain how the consultation will be managed and that whilst the call is not recorded a written record of the consultation will be recorded in the notes as it would if they were in attendance, ask them to confirm they are happy to continue with the discussion and record that decision. You can then continue and undertake the consultation over VCA. Verification also includes:

- Patient information and contact details being matched against the patient record
- Use of NHS Spine integration for patient matching
- Checking details with patients and visual ID check where possible.
- Physical checking of photo ID by practice staff for initial use on VCA

4.2 Process for Speaking to a Family Member or Proxy

If you call the patient and a family (or proxy) member answers, it is advisable in the first instance to ask whether the patient can speak to you. If they are able to, complete the outlined identification checks with the patient and then ask them who the family member is and ask if they are happy for the consultation to be completed with the family member/proxy on their behalf, as the patient may struggle in any number of ways (hearing, retaining information, understanding etc) and normally would attend an appointment with the family member who leads the discussions.

If the patient cannot verify their identify prior to you talking to a family member – due to them not being well enough or not having capacity – then the clinician should record this and act in the best interest of the patient. It is likely to be in the best interest of the patient that the consultation goes ahead. Ask the family member who they are and if they can verify the patient's identity. The clinician should record within the notes that the consultation took place within the patient's involvement and record the reason for this.

4.3 Multiple Staff in the room

If you have another member of staff in the consultation room with you when conducting a VCA, ensure the patient is made aware of this and they are happy to proceed.

## 5.0 SMS message template to patients

Many practices now use SMS text messaging to communicate with their patients. This might be to remind their patients about an appointment that has been booked, or to tell them that their prescription is ready to collect. As part of your plan to promote online consultations to patients you could add a line onto these standard texts, reminding patients about online consultations.

Template text:-

"Did you now know you can contact your GP using online consultations [or video consultations], please visit our website www.chapelgreenpractice.co.uk and you will have a response within 48 hours"

"Did you know you can now save yourself time waiting on the phone and consult with your GP online [or via video], please visit our website www.chapelgreenpractice.co.uk ."

"By having an online consultation with your GP, you may be able to pick up your prescription directly from your local pharmacy without having to come into the practice. For more information visit www.chapelgreenpractice.co.uk "

## 5.1 Telephone message template to patients

Many practices use a call waiting function for when patients phone the practice or are on hold. As part of your plan to promote online consultations to patients you could add a recorded message, reminding patients about online consultations

Template Text

”This is Dr Kemp, if you are ringing to book an appointment or speak to a GP, we have a quick, convenient and easy way to get help to you. Go to our website and click Doctorlink. This will allow you tell us about your problem or question. The information you give will be reviewed by our practice team, who will get back to you promptly, usually within 48 hours. If you need to be seen, the doctor will arrange this. If you are unable to access our website a relative or friend can help you. Otherwise, please hold for reception, who will ask you the same questions as the online system.”

“Thank you for calling Chapelgreen Practice. If you are ringing to book an appointment or speak to a GP, you may wish to try our online consultation service [or video consultation service]; a quick, convenient and secure alternative to visiting the practice. You can access this via the practice website, where you will be asked to fill in an online form and we will get back to you within 48 hours with the next steps.”

## 6.0 Security of Corporate Information

6.1 In order to ensure adherence to the General Data Protection Regulation (GDPR) the following guidelines must be followed:

- As a general principle of good practice, patient or staff identifiable information should not be stored on a mobile computer and certainly must not be stored on one unless it is encrypted to the standards required in the Encryption Policy
- **Under no circumstances should any patient based personal information be stored on any device other than equipment provided by THE PRACTICE e.g. laptop or digital camera. Mobile phones containing cameras, personal or work provided will not be used to take or store patient images or to transmit such images. Similarly no patient information will be stored on personally owned equipment such as iPods, PDA, Satellite Navigation Devices etc**
- If Patient Confidential Data (PCD) must be stored on a mobile computer, then the general principles about sensitive information given above must be followed
- PCD obtained through work must only be stored on computers, electronic equipment or electronic media that are the property of Chapelgreen Practice and therefore are subject to the policies and procedures of THE PRACTICE
- Loss of a mobile computer holding confidential information must be reported through the Incident Reporting mechanism as soon as possible. Chapelgreen Practice has responsibility for informing staff or patients if their personal information has been disclosed unlawfully

- Devices holding sensitive information must be encrypted in order to safeguard the information against unauthorised access. Encryption must be done to the standards currently required by THE PRACTICE
- Sensitive information should be removed from the device as soon as practically possible
- Patient identifiable information on mobile devices should be kept to a minimum i.e. use a hospital/NHS number instead of a name wherever possible, this is to reduce the risk of breach of confidentiality if the device is lost or stolen.
- Information stored on laptops should be regularly backed up and the backups held within a secure location. Normally data should be backed up regularly to a secure location on THE PRACTICE's network. **This would involve regular synchronisation of the computer when connected to the network**
- All mobile devices must be authorised for use by IT Service Provider before connection to either a PC or the network is allowed
- Mobile devices should be password protected to ensure that unauthorised use cannot occur. Passwords should not be shared. If your password is compromised please report immediately to IT Services
- Virus protection software must be installed, active and up to date

## 7.0 Reporting Security Incidents & Weaknesses

7.1 Reporting of any losses, theft or damage to documentation or computer assets will be through Chapelgreen Practice Manager at the first possible opportunity, and with a degree of urgency. This should then be reported to Chapelgreen Practice Data Protection Officer (DPO)

7.2 Information provided will include details of the losses or incidents and a detailed description of the data lost. Any PCD lost will need to be reported to the DS&P Toolkit as a Breach and individual subjects will need to be notified of the losses. Please refer to the Breach Reporting Policy.

7.3 Near misses and possible weaknesses will also be reported through this method.

## 8.0 Dissemination, Implementation and Access

8.1 Dissemination of this policy will be undertaken by publishing on the Intranet.

## 9.0 Monitoring Compliance

9.1 Staff are expected to comply with the requirements set out within the Video Consultation Policy and related policies. Compliance will be monitored by Chapelgreen Practice Manager with reports of spot checks, completion of staff questionnaires, incidents reported, electronic audit trails and submission of the DS&P Toolkit.

9.2 Non-adherence to the Video Consultation Policy and related policies will result in disciplinary action being taken.

## 18.0 References

- Access to Health Records Act 1990
- General Data Protection Regulation 2016
- Data Protection Act 2018
- Crime and Disorder Act 1998
- Human Rights Act 1998
- Common law duty of Confidentiality
- Freedom of Information Act 2000
- Criminal Procedures and Investigations Act 1996
- Regulation of Investigatory Powers Act 2000
- Health and Social Care Act 2001 (Section 60)
- NHS (Venereal Disease) Regulations 1974
- Human Fertilisation and Embryology Act 1990
- Abortion Regulations 1991
- Data Protection Act Policy and Procedures
- NHS Code of Practice: - Confidentiality (Inc Caldicott)
- Children's' Act 2004
- Mental Health Act 2007
- Management of Health and Safety at Work Regulation 1992
- Health and safety (Display Screen Equipment) Regulation 1992
- Manual Handling Operations Regulation 1992
- Midlands and Lancashire Commissioning |Support Unit FAQ and DPIA for Co-Vid 19
- Patient Info.org VCA Guidance
- NHSE Using Online Consultations in Primary Care toolkit (September 2019)

**APPENDIX A**

# DPIA template

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<br>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.<br><br>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.<br><br>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.<br><br>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.<br><br>**Video Consultation *(detailed)***<br>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 SystmOne or EMIS Web profiles; and, an administrator at their GP practice to approve them. This is to prevent people who do not actually and currently work at the provider organisation from accessing the AccuRx system.

Furthermore, patient demographic data is only pulled from either TPP SystmOne or EMIS Web principal care systems. This ensures that a 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 |
|---|---|
| **Principle 1 – (2.21 2.23)**<br>Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –<br><br>(a) at least one of the conditions in Schedule 2 is met, and<br>(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)**<br>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)**<br>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**<br>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)**<br>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)**<br>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)**<br>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)**<br>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.** |

# *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 | Users are authenticated by requiring: NHSmail to register for an account; TPP SystmOne or EMIS Web profiles; and, an administrator at their GP practice to approve them. This is to prevent people who do not actually and currently work at the provider organisation from accessing the accuRx system.<br><br>Patient demographic data is only pulled from either TPP SystmOne or EMIS Web principal care systems. This ensures that a user can only access data of patients registered at their practice.<br><br>Any video consultations are not recorded or stored. | Eliminated | Low | Yes |
| Incorrect patient data selected for SMS | Patient demographic data is only pulled from either TPP SystmOne or EMIS Web principal care systems. This ensures that a user can verify the correct information with the patient before sending | Reduced | Low | Yes |

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

| | | | | |
|---|---|---|---|---|
| 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 |