PCIG Consulting Template

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

Malvern Town Primary Care Network (PCN)

Whiteacres Medical Centre, Malvern Health Centre,
St Saviour Surgery, New Court Surgery

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 Managers
Target Audience:	This policy applies to any person directly employed, contracted, working on behalf of the practices within Malvern Town PCN or volunteering with the practices.
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 practices in the Malvern Town PCN 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 practices in the Malvern Town PCN and the 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 practices in the Malvern Town PCN use of VCA.

3.0 Statement of Intent

3.1 It is intended that practices in the Malvern Town PCN 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.

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

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 practices in the Malvern Town PCN and therefore are subject to the policies and procedures of practices in the Malvern Town PCN
- Loss of a mobile computer holding confidential information must be reported through the Incident Reporting mechanism as soon as possible. Practices in the Malvern Town PCN have 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 practices in the Malvern Town PCN.
- 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 Practice Manager of the individual practice within Malvern Town PCN at the first possible opportunity, and with a degree of urgency. This should then be reported to the 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 [The 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)