CYMORTH LLYWODRAETHU GWYBODAETH AR GYFER GOFAL SYLFAENOL

INFORMATION GOVERNANCE SUPPORT FOR PRIMARY CARE

IG Guidance on

Patient Consultations via Video Conferencing

Introduction

Information governance is a framework which supports how organisations and individuals manage the way information is handled. It applies to sensitive and personal information of employees, patients and service users. It is about setting a high standard for the management of all information and giving organisations the tools to achieve that standard.

The use of personal or confidential patient information should always be limited to the minimum required to meet the specific purpose. Approved processes, systems and applications should be used where it is appropriate to do so.

This guidance is aimed at Primary Care Service providers who will be utilising video conferencing services (VCS) for patient consultations.

There has been a vast expansion in the use of VCS to aid communications as part of responding to the Covid-19 pandemic, and to support a reduction in face to face attendance within primary and secondary care. As Primary Care Service providers are settling into new ways of working, it is important to review the use of VCS and ensure that the chosen solution is used appropriately and securely to support the provider's business need. Risks and risk mitigation should be carefully considered as part of the ongoing VCS use.

Staff are expected to use their professional judgement in the management and use of video conferencing solutions.

Choosing the video conferencing solution

Primary Care Service providers should consider their choice of video conferencing solution carefully. The NHS Wales approved solutions are:

- NHS Wales Video Consulting Service (Attend Anywhere) – suitable for patient consultations;
- Microsoft Teams - suitable for business related calls and can be utilised for patient related consultations. This application has the facility to record consultations where considered necessary. See NHS Wales Microsoft 365 Acceptable Use Policy for Primary Care Service Providers.

These solutions are hosted and managed for NHS organisations at an All-Wales level; appropriate governance processes have been undertaken.

Other video conferencing solutions are available but have not been assured on an All-Wales basis, however it is understood that some have by the local health boards. Therefore, if the Primary Care Service provider chooses an alternative to those detailed here, the organisation should ensure that the health board or practice have undertaken appropriate due-diligence and assurances relating to the security of the data solution and the information governance requirements prior to use.

Where either an all NHS Wales assured product or locally assured organisational implemented product are not available and there is a **significant and serious** need to complete a VCS based consultation or discussion, where there is **absolutely no viable alternative available** and the risk to an individual or patient has been considered to be higher than the governance risk, free consultation services such as WhatsApp and/or Facetime can be utilised. Primary Care Service providers should however consider these risks carefully and only do so for exceptional one-off circumstances. Users of such solutions should ensure that

the storage of audio and video recordings is turned off due to the lack of security and risk of loss of information.

Equipment

It is recommended that wherever possible appropriate and approved organisational owned devices are used to ensure the security and integrity of data systems.

Use of own equipment

It is not advisable for health professionals to use their own personal devices for the management of patient information. However, we appreciate that there may be extenuating circumstances when staff are required to work remotely and who will be relying on the use of their own device and access to the network through MFA.

The ICO recommend this approach is captured in an appropriate policy, therefore the Primary Care Service provider is encouraged to develop and implement a Bring Your Own Device (BYOD) Policy. See the National Cyber Security Centre (NCSC) website for further guidance. A BYOD guide is also available on the ICO website, we understand this is being reviewed however the principles will still apply.

Where there is **no other practical alternative** staff should ensure:

- The device is appropriately maintained, and appropriate software updates and patching have been applied;
- The device is not jailbroken or any other tampering that alters the product's security;
- The device is appropriately protected with anti-virus products;
- The device is kept secure with strong passwords or bi-metric access controls;
- No personal/confidential data is stored or recorded on personal devices;
- Home internet connections are secure (i.e. use a virtual private network (VPN)) and avoid using public WIFI.

Working from home

VCS provides the opportunity for workforces to carry out their work away from their normal business premises such as home working. Where staff are working from home the organisation should ensure that:

- The home environment is appropriate for carrying out a video consultation i.e. consultations can occur privately;
- Health and Safety of employees has been considered and an appropriate workspace is available.

It is recommended to complete a home risk assessment for any member of staff working from home. See IG Guidance on Remote Working for General Practice Staff; including Working from Home for further information.

General principles of video consultation

There are several general principles that should be followed when using remote consultation, these include:

Confirm the patient's identity

The health professional should request re-assurance that they are talking to the correct patient. They must confirm the patient's identity before commencing the consultation. It is extremely important that the questions posed:

- Do not guide the individual in any way;
- Do not accidently disclose information to the patient before their identity is verified;
- Include a range of at least 3 questions in addition to demographic information;
- Are not easy to obtain answers to or guess.

Depending on the service provider examples of questions used may include:

- *Please confirm you full name* (Where a patient has an unusual surname or one that can be spelt in different ways i.e. Sean/Shaun please ask the patient to confirm the spelling);
- *Please confirm your date of birth;*
- *Please confirm your full address including postcode* (Ask the patient to spell elements of an address where this is complex);
- *When did you last see a doctor/nurse at this surgery? Which health professional was the appointment with?;*
- *When was your last check up? Which dentist was the appointment with?;*
- *When was your last eye test? Do you wear prescription glasses or contact lenses?;*
- *Which GP Practice are you registered with?;*
- *Do you take any prescribed medicines? Can you tell me what they are?* (If there are a large number of medicines you could ask, please name three?);
- *Where was your last prescription sent?;*
- *Have you had an operation in hospital? Can you remember when and what it was for?*

Note: If the patient makes mistakes in their answers the health professional should be very cautious of the genuine nature of the request and require further identity information before providing access.

Ensure an appropriate setting

Both the health professional and patient should be in a private setting for the duration of the consultation. Patient confidentiality should be treated the same as it would be during an in-person consultation. The health professional should:

- Confirm the patient's location, as they may not be at home, in case you need to send medical help;
- Encourage patients to not join a call in a public space and ensure they maintain their own privacy and security;
- Ensure personal/confidential patient information is safeguarded in the same way you would with any other consultation and ensure that no one else can view or overhear the call without the consent of the patient;

- Conduct the consultation in a well-lit room and ask the patient to do the same. The camera should be positioned so that your full face can be seen, and you are in focus, ensuring you are looking at the camera when talking and listening;
- During any examination, ask others to switch off their camera or leave the room if their presence is not appropriate or the patient does not consent.

Provide Introductions

The health professional should ensure proper introductions are made including:

- Introduce and explain everyone in the room, even those off camera or confirm with the patient that they and you are alone;
- Take or check the patients contact number in case the video consultation fails;
- Check if the patient or anyone else is recording the consultation;
- If the connection or video quality is poor, ask the patient to re-book or convert the consultation to phone or face to face to ensure that you do not miss something due to technical interference.

Key principles for safely assessing patients using video consultation

Assessing patients remotely requires health professionals to make careful judgements that can be more difficult than face to face, the Primary Care Service provider should ensure:

- Staff continue to use their clinical skill and judgement when using VCS to clinically consult remotely, ensuring normal boundaries and thresholds are applied;
- The appropriate triage processes are in place based on clinical judgement;
- Staff are aware that patients or their relative may record the video consultation;

There are several useful remote triage processes relating to remote consultations, examples can be found below:

- BMJ – Covid -19 Remote Consultations
- Healthier Together RCPCH Clinical Pathways – Remote assessment

Consent and remote consultation

By accepting an invitation and entering the video consultation the consent of the patient is implied. It is good practice to confirm and record their consent for a consultation via VCS in the patient record.

If any other party is involved in the consultation i.e. a trainee, interpreter, chaperone or a multidisciplinary team (MDT) member, you should explain their presence in the consultation and request consent for their attendance, as you would during a face to face consultation. Again, their presence should be recorded in the patient record.

The health professional is required to make notes during and/or after the consultation for inclusion in the health record in the same manner as during an in-person consultation.

Any recordings of the consultation by the health professional should form part of the patient record. See IG Guidance on Capturing and Obtaining Clinical Images for further information.

Capacity and consent

Where the patient is a child who lacks capacity to make a decision about taking part in a video consultation with the health professional, the professional will need the permission of someone with parental responsibility.

If an adult lacks capacity, the health professional must obtain consent from someone with authority to act on their behalf for healthcare decisions and/or proceed with the consultation on the basis that it is the patient's best interests to do so.

The same principles used in face-to-face practice should apply:

- Consider the patient, speak directly to them and involve them in their care as much as possible;
- Even when a child has capacity, they may like another person present on the call;
- Consider that adolescents may find it more difficult to have vital conversations when they are at home and family members may be present.

Recording consultations

Organisations should not routinely record the video or audio information relating to consultations. Where there is a specific need or reason to record a consultation, the health professional must ensure that they have obtained explicit and informed consent from the patient. The consenting health professional should ensure that they explain:

- Why a recording is required;
- How it will help in providing clinical care;
- Who can access the recording;
- How and where it will be stored securely;
- How long it will be retained for;
- How it will be used (it is important to note that a recording cannot be used for any other purpose other than those clearly consented to by the patient).

Note: This information may be presented in the form of a privacy notice. Further guidance on informing individuals on how their information is processed can be found on the ICO website.

Where the patient does not consent, a recording should not be made.

Where consent is provided this should be formally recorded in the clinical record. It is good practice to inform the patient when the recording starts and stops.

Patients are able to record their consultations for their own use, health professionals are not required to provide permission when recording occurs, it is however good practice to discuss with patients from the outset of any consultation if they intend to record. Health professionals should be aware of covert recording, however there is limited recourse to stop such practice.

Screen sharing

Many video conferencing solutions include the ability to share your screen. Whilst this can be useful, for example to show a patient a scan or x-ray result, the health professional must ensure that the sharing of the desktop or application is appropriate for the consultation, respecting confidentiality, justified use and appropriate access.

The health professional must take care to ensure that no personal identifiable information of any other individual or any business sensitive information is visible when screen sharing. Screen sharing should only commence once the appropriate file/application has been loaded onto the screen and ceased prior to closing the file/application to ensure that no other information inadvertently becomes visible whilst screen sharing.