Using Video Conferencing for Patient/Service User Consultations

This short guide provides guidance on the Information Governance issues associated with remote consultations using video conferencing applications such as FaceTime® and/or Skype®.

Privacy considerations

- Before implementing videoconferencing for use in remote consultations, you should conduct a Privacy Impact Assessment (see Additional Support below). This will provide assurance that use of such solutions will be secure and that the privacy of service users will be maintained.
- Once you are satisfied that any privacy risks associated with the use of your chosen video/teleconferencing solution(s) have been appropriately mitigated, it is recommended that you pilot usage before rolling it out more widely. This will enable both service users and staff to provide valuable feedback that may help to improve both the user experience and security.
- No solution is ever infallible in terms of security but it is important to assess risks, take steps to reduce them and ensure that patients are fully aware of them.

Policy considerations

- The use of a patient consent form as provided at Appendix 1 is strongly recommended. It is best practice to obtain parental consent for service users under 16 though this is not required where you assess a young person to have the capacity to decide this for him/herself and they have requested that parents should not be involved.
- Whilst videoconferencing can bring great benefits (e.g. convenience, less travel, cost savings etc.) to both patients and healthcare professionals, it should be offered to patients as a choice, rather than a requirement. You should make it clear that you cannot provide any guarantees as to the quality or security of the service; neither can you provide any support to resolve technical issues. Patients should be made aware that they will need to have a good quality internet connection in order to get the most out of such solutions.
- Decisions about whether or not video/teleconferencing is a suitable form of communication should be made on a case-by-case basis. Staff are expected to use their discretion and professional judgement when making such decisions. A clinical risk assessment should be undertaken before using videoconference solutions for care purposes.
- You should NOT use video/teleconferencing to discuss matters that may cause a patient distress or anxiety, or to discuss matters of particular sensitivity (e.g. informing a patient that they have been diagnosed with a terminal illness or potentially stigmatising condition).
- Initial consideration should be given as to whether the VC resolution (e.g. full screen HD) is a priority. You should also bear in mind that the quality of a videoconference will depend on the quality and resolution of webcams and strength of the internet connection of each of the parties to a videoconference, and ask yourselves whether your chosen solution(s) is fit for the intended purpose.
- Which capabilities are of greatest importance will depend on intended use. Image quality and resolution may be important when making any clinical physical assessment of a condition as the displayed image may not be of sufficient detail, e.g. for visual identification of topical problems. Uninterrupted streaming may be a paramount factor for interactive talking therapies but a lower image resolution may be acceptable.
- If you choose to use free solutions you will seldom have any contract or service level agreement in place with the provider. You will not therefore, in most instances, have any

recourse to legal action. The use of video/teleconferencing solutions for communicating particularly personal confidential or sensitive data is NOT recommended in such circumstances, as you will have no 'control' over the data being processed over the internet.

Fair processing considerations

- Service users should be made aware that no communication over the internet is entirely secure. However, the security risks associated with using such solutions for routine non-confidential/sensitive patient discussions have been assessed by your organisation and have been considered to be relatively low.
- You should publish guidance on the secure use of your chosen solution(s) or point patients to guidance that already exists.

Security considerations

- Only initiate via an outgoing call to a patient/service user (to ensure verification of identity) or via a trusted third party service provider which operates a robust authentication process.
- You **MUST** only use corporate devices or personal mobile devices that have been protected by adequate security. This is typically achieved through network security controls and the use of Mobile Device Management solutions.
- Where there is a separate video conferencing login, you must use **STRONG PASSWORDS** when activating their chosen videoconferencing account.
- You **MUST** ensure that you download all necessary updates for your chosen video conferencing solution(s) as they become available - these updates can contain important security patches.
- You must **NOT** use such solutions to share files that contain personal confidential and/or sensitive data. Care must be taken not to bypass or jeopardise established formal communication policies and protocols for secure communications.
- Both service users and staff should be made aware of the need to discuss personal confidential or sensitive matters in a private space (i.e. where others cannot overhear).

Records management considerations

You **MUST** ensure that relevant outcomes are recorded within the patients' electronic record. Video consultations should **NOT** be recorded, unless the patient provides explicit consent to live recordings.

Can I use such solutions to communicate with colleagues?

Yes, but unless you have obtained explicit patient consent you should not discuss patient information in a manner that can be used to identify them.

Additional Support

The Information Commissioner has published guidance on conducting Privacy Impact Assessments which is available at https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
The GMC have published guidance on video and audio recordings at http://www.gmc-uk.org/Making_and_using_visual_and_audio_recordings_of_patients.pdf_58838365.pdf
The IGA aims to become the authoritative source of IG advice and guidance and publishes a wide range of materials at http://systems.hscic.gov.uk/infogov/iga

Appendix 1

Patient consent form for video/teleconferencing			
People are increasingly asking our staff to contact them via online services such as FaceTime® and Skype® as this can save them time and expense. As such, we are offering the choice of being contacted via such services in order to discuss routine matters of care. You are under no obligation to use such services and you can still be seen in person by booking an appointment the usual way. If you are interested there are some risks and required practice associated with using such online services that you should be aware of.			
Potential risks: • Such online services transmit data across the internet in an encrypted format; whilst this is a reasonably secure means of sending data, it is by no means 100% secure. • Poor quality internet connections can often interfere with the quality of the video conference. • Some of the free services offered by FaceTime® and Skype® are not governed by a contract or service level agreement. We cannot therefore make any warrantees or guarantees as to the quality or security of the service.			
These risks can be reduced by:			
• You will be called for your videoconference or be provided with instructions for joining via a trusted service provider. Do not attempt to call our organisation directly.			
• Please use the fastest connection you have available (mobile or broadband) and the device with highest resolution/quality webcam/rear facing camera. • To ensure that FaceTime® and Skype® are not used to discuss matters that are particularly personal confidential or sensitive in nature to you, the professional involved may not be able to fully disclose sensitive aspects of your case. In these cases please do not probe for an answer that may be inappropriate to deliver remotely. • Ensure that you have a safe, quiet, confidential place that is free from interruptions for your consultation.			
• You should set your **PRIVACY PREFERENCES** for receiving communications. For example, when using Skype® you can set your preferences as follows: When logged into Skype® on a Windows device, click Tools > Options > Privacy and on an Apple Mac device, click Preferences > Privacy.			
• If you wish to record the session with your own applications or another device, we request that you inform our staff in advance please.			
Service User Confirmation:	I confirm that I have been made aware of the potential risks and I am happy for those directly involved with the provision of my care to contact me using Skype® or FaceTime® (delete as appropriate).		
Name:		**Date of birth:**	
Skype® ID or FaceTime® mobile number / email address:			
Patient Signature:			
Date:			