Cheshire and Wirral Partnership
NHS Foundation Trust

Document level: Trustwide (TW)
Code: SOP
Issue number: 29

Video Conferencing Information Governance Guidelines

Lead executive	Medical Director – Effectiveness & Medical Education
Authors details	Information Governance Lead/Data Protection Officer 01244 397384

Type of document	Standard Operating Procedure
Target audience	All CWP staff
Document purpose	To provide staff with guidance for the use of video conferencing platforms whilst maintaining adequate Information Governance requirements.

Approving meeting	Information Governance & Data Protection Sub-Committee	Date 24-Aug-20
Implementation date	24-Aug-20	

CWP documents to be read in conjunction with	
HR6	Mandatory Employee Learning (MEL) policy
IM7	Confidentiality policy
IM1	ICT Acceptable Usage Policy
GR1	Incident Reporting and Management Policy
GR3	Risk Management Policy

Document change history	
What is different?	New standard operating procedure
Appendices / electronic forms	N/A
What is the impact of change?	N/A

Training requirements	No - Training requirements for this policy are in accordance with the CWP Training Needs Analysis (TNA) with Education CWP.

Document consultation	
Clinical Services	Clinical representatives of the Information Governance & Data Protection Sub-Committee
Corporate services	Corporate representatives of the Information Governance & Data Protection Sub-Committee
External agencies	N/A

Financial resource implications	None

External references
Principles of safe video consulting in general practice during COVID-19. Royal College of

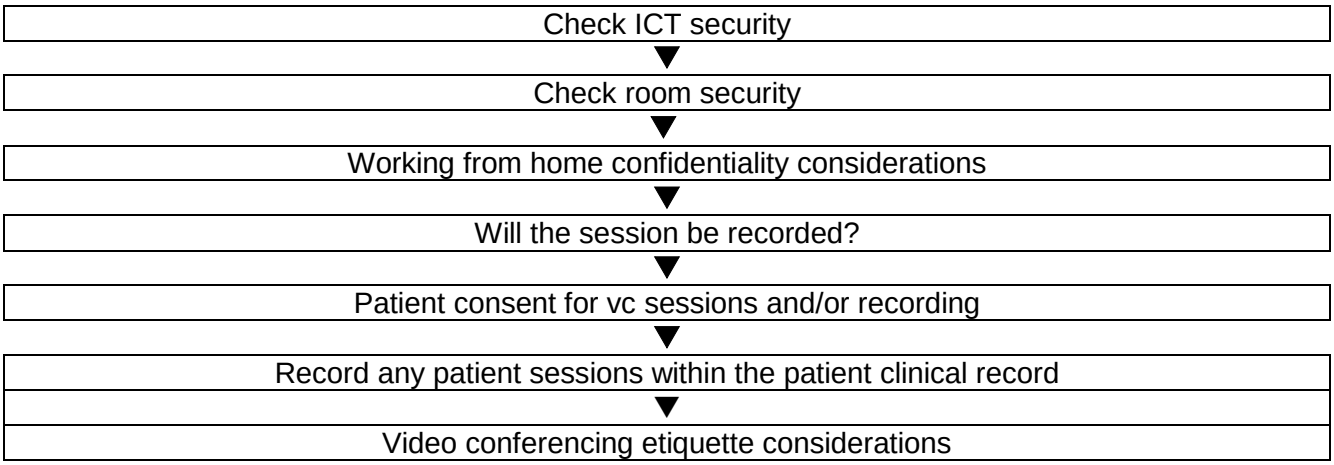
General Practitioners.

Equality Impact Assessment (EIA) - Initial assessment	Yes/No	Comments
Does this document affect one group less or more favourably than another on the basis of:		
- Race	No	
- Ethnic origins (including gypsies and travellers)	No	
- Nationality	No	
- Gender	No	
- Culture	No	
- Religion or belief	No	
- Sexual orientation including lesbian, gay and bisexual people	No	
- Age	No	
- Disability - learning disabilities, physical disability, sensory impairment and mental health problems	No	
Is there any evidence that some groups are affected differently?	No	
If you have identified potential discrimination, are there any exceptions valid, legal and/or justifiable?		
N/A		
Is the impact of the document likely to be negative? - If so can the impact be avoided? - What alternatives are there to achieving the document without the impact? - Can we reduce the impact by taking different action?	No N/A N/A N/A	
Where an adverse or negative impact on equality group(s) has been identified during the initial screening process a full EIA assessment should be conducted. If you have identified a potential discriminatory impact of this procedural document, please refer it to the human resource department together with any suggestions as to the action required to avoid / reduce this impact. For advice in respect of answering the above questions, please contact the human resource department.		
Was a full impact assessment required?	N/A	
What is the level of impact?	N/A	

Contents

Quick reference flowchart for information governance video conferencing procedure

For quick reference the guide below is a summary of actions required.



1. Introduction

This standard operating procedure is to provide staff with guidance to ensure that all staff are aware of their information governance responsibilities when utilising any of the Trust's video conferencing platforms ensuring compliance with the principles of Data Protection Legislation. In particular the Trust must ensure the protection of confidential information.

The Senior Information Risk Owner (SIRO) is accountable for the Trust's Information Risk Management. The SIRO must have assurance that we undertake formal processes for the use of video conferencing platforms. Video conferencing platforms must be fully risk assessed and consider the controls and assurance for all aspects of process. Data Protection Impact Assessments, which are a requirement of the General Data Protection Regulation 2016, have been completed and approved by the Caldicott Guardian for each of the Trusts external facing video conferencing solutions.

Video conferencing (VC) services provide the ability to conduct real time video meetings that can cover one to one or one to many site locations. VC technology has become more refined over the past decade, with the benefits of high definition (HD) quality images, clearer digital sound and interaction with other collaborative tools. Some of the key benefits of a video conferencing service are:

- saving time - reduces unproductive time spent for travelling to and from meetings
- the ability to quickly organise real time face to face meetings for critical decision making
- saving money - reduction for travel and expenses costs
- environmental benefits - a reduction of CO2 emissions

VC services are extensively used within the NHS, providing assistances for day to day collaboration, especially in the areas of health management and diagnosis by medical professionals and medical training. It is also a main technology tool to assist administrative and support functions and senior management teams within NHS organisations.

2. Scope

This procedure is applicable to all staff, including contractors, temporary / agency staff and volunteers who utilise video conferencing platforms.

3. Procedure

The following guidelines have been taken from Principles of safe video consulting in general practice during COVID-19, Royal College of General Practitioners.

3.1 Security

If you are working from home and using your own equipment, check your internet access is secure (eg use a virtual private network (VPN) and/or if possible avoid public Wi-Fi), and make sure any security features are in use.

During COVID-19, you can use your own devices to support video conferencing for consultations, mobile messaging and home working where there is no practical alternative. Reasonable steps to ensure using your own devices is safe include setting a strong password, using secure channels to communicate, eg tools/apps that use encryption, and not storing personal/confidential information on

the device, unless absolutely necessary, and that the appropriate security is in place. Safeguard personal/confidential information in the same way you would with any other meeting.

3.2 Room security

Do not leave video conferencing equipment unattended or "in conference" in locations that are isolated. Only videoconference with known and approved site(s) and with location's permission. Ensure room and content security. For example, do not leave confidential information on whiteboards or documents which could be viewed. Clear room of any confidential information on completion of a VC session.

3.3 Working from home

If you are working from home ensure your VC session cannot be overheard by other members of your household and be aware that open windows could enable conversations to be overheard by neighbours or passers by.

3.4 Recording sessions

Some VC platforms enable recording of sessions. If the Microsoft Teams platform is being used it is possible that participants who hold an nhs.net email account are able to record the session. If they do begin to record, the host will receive an immediate notification and they are able to stop the recording. A notification appears at the top of the screen for all participants if video recording has commenced. During meetings it is recommended that participants assume that a session will be recorded and safeguard information as they would normally do during meetings.

3.5 Patient consultations

The decision to offer a video consultation should be based on the patients need, clinical prioritisation and clinical judgement. There is no need to use video when a telephone call is sufficient. Be aware that patients or their relatives may record the video consultation.

If the Microsoft Teams platform is being used (especially in the case of Group Therapy), it is possible that participants are able to record the video conference. This only appears to be an option if the participant holds an NHS.net (internal) email. If they do begin to record, the host will receive an immediate notification and they are able to stop the recording. During group therapy, the advice would be that this should not be recorded unless consent had been gained from all involved on the call.

If the VC session is in place of a face to face patient consultation, the consent of the patient is implied by them accepting the invitation and entering the video consultation. It is good practice to confirm and record their consent for a video consultation and confirm whether the consultation is being audio or video recorded. If an adult lacks capacity, you 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.

Young people under 16 should be assessed if consulting remotely to assess capacity and safety.

- If the child does have the capacity to consent to a video consultation, then confirm whether they would they like another person (for example, parent or family member) present on the call or not.

- If a competent child wishes to discuss a matter in the absence of a parent, all the usual principles apply in relation to confidentiality.

- Consider the voice of the child, even if children are unable to legally consent to an examination, ask the child if it is acceptable first, they should have as much involvement and say in their care as possible.

- An opportunity to speak to adolescents alone may be more difficult if they are at home. Consider how you will still have these vital conversations.

- For children who do not have capacity to consent, then consent would need to be sought not in the child's best interest. Apply the same principles used in face-to-face practice.

- Document the name and relationship with the adult and/or person(s) present. If a child is the subject of the consultation make sure you see them and that you don't just talk to the adult(s).

- Ask for consent if a trainee, interpreter, chaperone or a multidisciplinary team (MDT) member wants to join the consultation. During an examination, ask others to switch off their camera or leave the room if their presence is not appropriate or the patient does not consent.

Do not record the video or audio of the consultation unless there is a specific reason to do so, and there is explicit and informed consent from the patient, document these discussions and decisions in the clinical record. The process of obtaining and documenting consent should include explaining why a recording will help in providing clinical care, who can access the recording, where and how it will be stored securely, how long it will be stored for and how it will be used (i.e. that the recording will not be used for any other purpose except for direct care without the patient's express permission). If a recording is made this must be stored securely in the patient's clinical record. If recording, confirm when the recording starts and stops.

Confirm the patient's identity if they are not known to you, e.g. check name and date of birth. If you have safeguarding concerns, and the patient is unknown to you, verify their ID, e.g. vouching if you have access to the patient's clinical record, or by asking for photo ID.

Introduce everyone in the room, even those off camera or confirm with the patient that they (and you) are alone. Follow this with:

- checking if the patient or anyone else is recording the consultation
- ensuring you use a private, well-lit room and ask the patient to do the same. You should safeguard personal/confidential patient information in the same way you would with any other consultation
- taking the patient's phone number in case the video link fails

If the connection or video quality is poor, ask the patient to re-book or conduct a phone or face to face consultation as it is possible you could miss something due to technical interference.

It is essential that colleagues are still able to talk to each other and share appropriate information about the people in your care, including with social care. Where possible use the phone, secure NHSmail or MS Teams.

Starting the examination
Setting up Your initial focus should be on the camera position in order that the patient sees your full face and you are in focus. Confirm the patient's location in case you need to send help: they may not be at their home address. Then explain the nature and extent of the examination and seek verbal consent. When talking, look at the camera. When listening continue to look at the camera and screen. Signpost what you are doing when you need to look away to avoid looking uninterested.

Safety netting
Be particularly careful to summarise key points and explain next steps in language that will be clear to the patient:
• Explicitly check understanding.
• Provide clear safety netting instructions.
• Actively signpost for support, e.g. to social prescribing link workers.

Documentation
Make contemporaneous written records in the patient's medical records, as you would in a standard consultation. Do not record the video or audio of the consultation unless there is a specific reason to do so, and there is explicit and informed consent from the patient, document these discussions and decisions in the clinical record. The process of obtaining and documenting consent should include explaining why a recording will help in providing clinical care, who can access the recording, where and how it will be stored securely, how long it will be stored for and how it will be used (i.e. that the recording will not be used for any other purpose except for direct care without the patient's express permission). If a recording is made this must be stored securely in the patient's clinical record. Follow your organisational policy on secure management of patient data. If recording, confirm when the recording starts and stops.

Document in the patient's record that the consultation is via video*, the nature and extent of the examination has been explained to the patient in advance (together with all the other aspects of the consultation) and the patient verbally consented to being examined in this manner. Record discussions and decisions about capacity and consent. Ensure your clinical justification for examination and non-examination is clear. Record who was present for the consultation, you should record their identity, including their designation and the extent of the assessment witnessed, for example 'present for the complete video-linked assessment'.

3.6 Video conferencing etiquette considerations

It is important that all parties feel comfortable with the arrangements in place during video conference meetings. Staff should consider the following:

- Organisers of meetings should ensure that meetings are not unnecessarily long
- Organisers of meetings should allow some time in-between different video conference meetings to ensure adequate break time is allowed for staff

- Everyone join on time
- Activite mute when not talking – chair to do this if people don't
- All need to allow the chair to lead the meeting – will ensure people are invited to speak
- Use the chat bar or hand up function for participants to ask questions or make comments
- Make full use of the 'share screen' option to share agendas and papers
- Re-join on time (all) – when taking breaks

It is now possible to add a custom background to Cisco Webex Meetings, for a full guide on how to add a background please click here. Please ensure that any images you upload of your own are suitable and in line with CWP values for both internal and external Webex meetings.

4. Training

- Raising awareness to fully implement the procedure.
- To publish on the Intranet and communicate via the e-bulletin.

5 Monitoring

For this procedure:

- Staff responsible for undertaking video conferencing are aware of their accountabilities and responsibilities regarding this procedure.
- All staff are aware of relevant procedural documents e.g. ICT Policy, Information Governance Policy, Confidentiality Policy etc..
- Untoward incidents resulting from the use of video conferencing platforms will be logged on DATIX and reported to the Information Governance & Data Protection Sub-Committee

6. Duties & Responsibilities

6.1 Chief Executive

The Chief Executive will assume overall accountability for ensuring that appropriate and effective systems of information governance are in place throughout the Trust.

6.2 Senior Information Risk Owner (SIRO)

The SIRO is an executive director (currently the director of Business & Value) who highlights the impact on Trust strategy of information risks. The SIRO appraises the board of information risks and advises on information risk in the statement of internal control. Information Asset Owners (IAOs) are accountable to the SIRO.

6.3 Caldicott Guardian

The Caldicott guardian is a senior clinician (currently the medical director for Effectiveness and Workforce) who oversees the use and sharing of patient information, championing confidentiality and information sharing within and outside the Trust. The guardian plays a key role in ensuring that the Trust satisfies the highest practical standards for handling patient-identifiable information.

6.4 Information Governance Lead

The information governance lead is accountable for ensuring effective management, accountability, compliance and assurance for all aspects of information governance. They have operational responsibility for the delivery of a sound and effective information governance system.

6.5 ICT Service Support

ICT will provide support to staff in relation to video conferencing platforms via the ICT service desk email: cwp.ictservicedesk@nhs.net Tel: 0800 33 8182

6.6 Service Manager's/or Information Asset Owners (IAO) Responsibilities

Managers/IAO's are responsible for ensuring that their staff are aware of their information governance responsibilities, they have appropriate access to training and support and act in accordance with Trust policies and procedures in all aspects of information governance. Managers must report information incidents in accordance with the Trust's Incident reporting and management policy and recognise and manage information risk according to the Trust's Risk management policy. Managers are responsible for ensuring that contracts for staff or services meet or exceed CWP policies and procedures for information governance.

6.7 Employee's Responsibilities

All CWP employees and employees of partner and sub-contractor organisations must ensure that they undertake mandatory information governance training, access support and abide by all relevant policies and procedures. Information risks must be managed and information incidents reported through the Trust's Incident Reporting and Management Policy (GR1) and Risk Management Policy (GR3).