Upwell Health Centre and Welle Ltd (Pharmacy)

Video, Photography and Audio Recording Protocol

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Author | Next Review | Notes |
| 1 | Emma Cooper, Kafico Ltd |  | New Draft |
| 1.2 | Emma Cooper, Kafico Ltd |  | Feb 20 Amendment to length of time CCTV is retained for based on DPO event process review |
| 2 | Emma Cooper, Kafico Ltd |  | Dec 20 - Complete redraft based on new guidance during pandemic |
| 2.1 | Emma Kitcher, Kafico Ltd. | March 23 | No amendment. |
| 2.1 (March 23) | Emma Kitcher, Kafico Ltd | March 24 | Annual review performed. No changes. |

**Contents**

[1. INTRODUCTION 2](#_Toc97534551)

[2. QUICK REFERENCE POINTS 2](#_Toc97534552)

[3. KEY DEFINITIONS 3](#_Toc97534553)

[4. SCOPE 3](#_Toc97534554)

[5. KEY LEGISLATION / FRAMEWORK 4](#_Toc97534555)

[6. APPROVAL OF SOFTWARE AND HARDWARE 4](#_Toc97534556)

[7. PATIENT VIDEO CONSULTATIONS AND PHOTOGRAPHS 4](#_Toc97534557)

[8. PATIENT VIDEO CONSULTATIONS: WORKING FROM HOME 5](#_Toc97534558)

[9. RECORDING VIDEO AND SHARING IMAGES 5](#_Toc97534559)

[10. INTIMATE IMAGES 7](#_Toc97534560)

[11. CHILDREN AND YOUNG PEOPLE 8](#_Toc97534561)

[12. VIRTUAL MEETINGS WITH STAFF MEMBERS OR OTHER PROFESSIONALS 8](#_Toc97534562)

[13. CCTV AND TELEPHONE RECORDING 10](#_Toc97534563)

[14. ACCURACY 10](#_Toc97534564)

[15. RETENTION 11](#_Toc97534565)

[16. SECURITY 11](#_Toc97534566)

[17. RIGHTS 12](#_Toc97534567)

[18. APPLICATION AND AUDIT 12](#_Toc97534568)

[19. APPENDIX A: COMPLIANT RECORDING CHECKLIST 13](#_Toc97534569)

1. INTRODUCTION

This protocol supports staff to manage recording practice so that Upwell Health Centre and Welle Ltd (Pharmacy) complies with the requirements of privacy law and observes the rights and freedoms of data subjects.

Recordings may be used for purposes related directly to the care of the patient, for example, video consultations or as part of the assessment, investigation or treatment of patients’ condition or illness.

They may also be used for “secondary” purposes, such as for training or assessment of healthcare professionals and students or for research.

Whatever the purpose, it is essential that there is a systematic consideration of the rights of individuals and the security of the recording as personal data.

1. QUICK REFERENCE POINTS

* Recordings may be used for care or non care purposes
* Whatever the purposes, data protection and security must be considered
* Privacy law deems recordings more intrusive than photographs which are in turn more intrusive than written notes
* Approved software must be used
* Recording and images should only be captured in limited circumstances and should be based on a particular consideration
* Intimate images or those involving children and young people warrant particular care
* Be aware of your surroundings when discussing sensitive topics via video or telephone call
* Even when carrying out staff meetings, recordings should be used in limited circumstances because employees are deemed ‘vulnerable’ under data protection law
* Recordings and images should be stored securely, for limited periods and should only be attached to a person’s record as an exception
* Group consultations are subject to strict rules and should not be performed without first speaking with DPO

1. KEY DEFINITIONS

**Personal Confidential Information** This term is intended to cover information captured by the Data Protection Act 2018 / GDPR (identifiable information about the living), information covered by the Common Law Duty of Confidence / Tort of Misuse of Private Information and finally, information covered by Article 8 European Convention for Human Rights.

|  |  |
| --- | --- |
| **Recordings** | Originals or copies of audio recordings, photographs, and other visual images of patients that may be made using any recording device, including  mobile phones and CCTV. |

1. SCOPE

See Information Governance Policy for key roles.

All staff, whether management or administrative, who create, receive and use Personal Confidential Information have responsibilities to ensure effective reporting and management of information risk for Upwell Health Centre and Welle Ltd (Pharmacy). Employees have a contractual and legal obligation to read and comply with all company policies and to attend mandatory training to support the appropriate management of information.

1. KEY LEGISLATION / FRAMEWORK

* UK GDPR / Data Protection Act 2018
* Caldicott Principles
* Human Rights Act 1998
* GMC: Making and using visual and audio recordings of patients
* Various ICO Codes of Practice
* Key principles for intimate clinical assessments undertaken remotely in response to COVID-19 (RCGP)

1. APPROVAL OF SOFTWARE AND HARDWARE

* Photography or video recording should only be undertaking using software that has been issued by your IT provider
* Use of personal devices, in exceptional circumstances, must be approved by the DPO
* CCTV Providers must be notified to and approved by the DPO

1. PATIENT VIDEO CONSULTATIONS AND PHOTOGRAPHS

* Group consultations are subject to strict rules and should not be performed without first speaking with DPO
* Before implementing remote consultation software, you should check with your DPO as to whether the software has been approved for use
* When undertaking remote consultations for Upwell Health Centre and Welle Ltd (Pharmacy), the following steps should be taken to mitigate risks to patient data.

**Before the consultation**:

* Ensure you only have the patients clinical record open and close all others.
* Ensure the room is clear and the door is closed to avoid the consultation being overheard
* Check all equipment is working.

**During the consultation**:

* Ensure recording is off
* Ask the patient to confirm their identifiers and match them to their clinical record
* Ensure the patient is in a private space

**After the consultation**:

* Add consultation notes to the patient’s clinical record in the same way as a face-to-face consultation

1. PATIENT VIDEO CONSULTATIONS: WORKING FROM HOME

* There may be times where it is necessary work from home. You should ensure that you adhere to the same guidelines as above with the additional measures:
* Where provided, use a VPN token
* Close all other windows and programmes whilst undertaking a consultation
* Do not leave yourself logged in and lock the device when leaving it, even just for a few minutes.
* Ensure the room is clear and the door is closed to avoid the consultation being overheard

1. RECORDING VIDEO AND SHARING IMAGES

* The session should only be recorded in ***limited*** circumstances, for example, if you would have recorded it in a face-to-face scenario.
* It is necessary for clinicians to determine on a case-by-case basis whether such recordings are **necessary and justified**
* If you can demonstrate that the request is necessary and justified for the purpose of providing healthcare to the patient, images can be requested.
* If in a live video consultation, you can ask them to show the area if they are comfortable to do so.
* If you need a clearer image, you can also request that they take a photo of the area and send it across to the practice.

You should:

* Consider on a case-by-case basis whether a photograph or recording is needed. For example, because you want to get a second opinion.
* Consider whether the same result be achieved without asking the patient to send the photograph or being recording
* It is advised that where possible, a secure method such as AccuRx, TPP Airmid App or other reviewed apps such as Hospify are used to ensure that photographs are encrypted in transit.
* Where this is not possible, patients can be asked to email in the photograph, however they must be made aware there is a risk of interception due to the email not being encrypted.
* Consider which inbox will the photograph be sent to and ensure that only those with a ‘need to know’ are able to access the inbox (shared inboxes are discouraged)
* Ensure photos are deleted from the inbox as soon as they are added to the clinical system
* We advise that, in order to minimise the risk of identification in the event of interception, patients should be asked to only include their NHS number in the subject line / body of the email. They should not provide their name, DOB and / or address as identifying means.
* You do not need consent to process the images (although the patient should be fully informed), however, given that photographs and recordings are inherently more intrusive than a written account, particularly with intimate images, the level of distress must be considered.
* With each consultation you must:
* Explain why the image or recording will be helpful
* Provide different options available such as a face to face if uncomfortable with taking photos and sending it through or being recorded
* Explain who will see the image or recording – where uploaded to the patients record there is a chance that any healthcare professional involved in the patient's care will see the image
* How the image or recording will be used and whether it is being stored
* Make it clear to patients they do not have to share a photo or be recorded, and that refusal will not result in being unable to access care.
* If they feel it is important to send the photo through but do not want it uploaded to the medical record, consider whether the photo is necessary or whether a detailed description would suffice.
* In these instances, you can assure the patient the photo will be deleted once viewed and not added to their medical record.
* If the patient objects to showing the area in a video consultation or sending a photograph in this does not mean the virtual consultation needs to end. You should ask them about the area such as what it feels like and size and then discuss alternatives such as a face-to-face appointment.
* Sometimes a patient may send in an image without being asked. Where this happens, you should contact the patient to obtain context for the disclosure and confirm that they do not object to the image being saved to their record.

1. INTIMATE IMAGES

* An intimate image is breasts, genitalia, or perianal areas but it can also be an area that a patient views as intimate based on their beliefs, culture or personal experience.
* You can request intimate images, but further consideration should be taken regarding whether they are necessary.
* Consider each patient individually and be transparent with them, ask them if they are comfortable with showing an intimate area in a remote setting.
* Make it clear that they can be offered a face-to-face consultation if they wish and refusing to take a photograph / show the area on camera will not affect their access to care.
* Where a photograph of an intimate area is required, since this may cause more harm if a breach were to occur, practices may wish to destroy these particular images and write a detailed description in the records, rather than uploading to the record
* determining whether to keep any photograph or recording, a clinician should undertake a brief risk-benefit evaluation to determine whether the risk to any future distress is outweighed by the need to retain a particular image in order to understand why they gave the advice they did.
* For intimate areas it is unlikely the need to retain would outweigh the risk to future distress if there were a breach which is why we advise deleting these once a detailed description is taken.

1. CHILDREN AND YOUNG PEOPLE

* Where a photography is necessary in relation to a child you should ask the parent/s to explain to the child why the image is necessary and determine whether the child finds this acceptable.
* If the child / young person does not want the image taken this should be respected and alternative route sought to provide care.
* Do not undertake sexual health remote consultations with children under 16 unless in exceptional circumstances – for example, they are self-isolating due to COVID-19 symptoms.

1. VIRTUAL MEETINGS WITH STAFF MEMBERS OR OTHER PROFESSIONALS

* Where there is need for a virtual meeting with other healthcare professionals to discuss patients or other confidential matters such as HR issues - only approved software should be used and advice should be sought from your DPO
* In any circumstances, video is more intrusive than audio recording, which in turn is more intrusive than written notes and there is greater risk of misuse or harm.
* To comply with data protection law, data collected must be limited to 'what is necessary': if there is a less intrusive alternative that meets business needs, that option should be used. If written notes would have been sufficient for a face-to-face meeting, then that method should suffice for remote working.
* But there may be exceptions. For example, recording might be justified if:
  + there is a particular need for a verbatim account;
  + Considerations of language difficulties or an attendees’ disability.
* Regardless, there may be a less intrusive alternative, such as audio recording or a nominated note taker
* Even where an employee agrees, the imbalance of power between employers and employees should be considered and less intrusive routes pursued where possible
* Confidential meetings therefore should only be recorded in very limited circumstances and the chair should undertake a brief risk-benefit evaluation to determine whether the risk to any future distress is outweighed by the need to make the recording
* Explain why the meeting is being recorded
* Provide various options available such as switching off cameras or exiting and requesting a copy of the recorded meeting to review later
* You cannot record without the agreement of those present
* Explain who will see the recording
* How the image will be used and whether it is being stored
* Refer to the privacy policy
* Remind parties of confidential nature of content

,

* Before the meeting starts you should ensure you are in a room where you cannot be overheard and that your equipment is working correctly.
* Once the meeting begins you should introduce yourself and ask each of the other participants to do the same.
* If you do not recognise any of the participants and nor do other participants, ask them to identify themselves in an appropriate way such as showing their Staff ID card to the camera.
* Do not start discussing confidential matters until you are satisfied everyone within the meeting is intended to be there
* Recordings must be stored securely for a defined, limited time and destroyed in accordance with documented protocol

1. CCTV AND TELEPHONE RECORDING

* The appropriate lawful basis for recordings for CCTV or telephone recordings is likely to be “legitimate interests” since the activity is routine for many businesses and public-sector organisations.
* Upwell Health Centre and Welle Ltd (Pharmacy) has carried out a ‘legitimate interests’ assessment for these activities that is held by the Data Protection Officer.
* It is essential that the purpose for processing is specified and that any further uses are compatible with the original purpose.
* All recording activities must be notified to DPO and logged in the Processing Activities Log.
* Where recordings have the potential to be used for secondary purposes or further purposes than can be anticipated such as research or discussion at MDT, it is best practice to make the individual aware for this prior to the recording.
* It is important to minimise the personal data and the privacy intrusion when recording.
* The ICO CCTV guidance, for example, indicates that using audio on CCTV is often not necessary for the desired purpose and the same principle should be applied to all recording.
* Consider the length of recording, the information captured, placement of recording devices (i.e. do we need CCTV only in the waiting room or also in the corridor) so that you are capturing only what is necessary for the purpose
* All reasonable steps should be taken to ensure that data subjects are aware that both outbound and inbound calls are being recorded
* Some providers allow granular options to switch off recording – find out what these are and use them as appropriate

1. ACCURACY

* Every reasonable step must be taken to ensure that all recordings are accurate and of good quality
* You should regularly check that the date and time stamp recorded on images and audio recordings are accurate (for example, when the UK switches between summer and winter time)
* You should ensure that recordings are appropriately labelled to avoid mismatches with the other records
* Old hardware resulting in poor recordings should be replaced to avoid issues with data quality

1. RETENTION

* Recordings should be kept for no longer than necessary their intended purposes
* Consideration around transcription into hard copy (such that it represents a reduced privacy intrusion) should be made
* CCTV is usually wiped over 28 days to 3 months after recording, retention periods beyond this should be discussed with the Data Protection Officer
* Call recordings can be kept up to 7 years to support a negligence claim
* Fair Processing / transparency materials should include information about how long the recordings are retained

1. SECURITY

* Recording activities must be added to the Processing Activities Log and have a risk score attributed
* All physical assets capable of making audio or visual recordings should be added to an asset log so that they can be tracked and returned when required
* All physical assets capable of making audio or visual recordings should have a nominated owner that can monitor associated risk
* All physical assets capable of making audio or visual recordings should be destroyed in line with the Information Lifecycle and Data Quality Protocol
* All physical assets capable of making audio or visual recordings should not be removed from the premises without being signed out on the asset log
* Where audio or video recordings are made, this should be recorded within the main record along with the consent form (barring CCTV and general telephone recording)
* Disclosure of audio of video recordings to third parties must be subject to an Information Sharing Agreement or discussed with the Caldicott Guardian / Data Protection Officer
* Audio or video recording software that is supported by a third-party provider must be subject to a compliant contract that has been reviewed by the Data Protection Officer
* Transfer of recordings must be through encrypted methods in the first instance. Alternative routes must be discussed with the Data Protection Officer
* Recordings, including still images, must not be obtained using personal devices such as mobile phones.
* Recordings must be stored securely in the shared drive and must not be stored in email accounts, personal drives or on personal devices such as mobile phones

1. RIGHTS

* Individuals being recorded must be informed of their rights
* The right to object to being recorded
* The right to withdraw their consent to being recorded
* The right to rectify inaccurate information that has been recorded
* The right to have their recorded information sent to another Controller
* The right to restrict the use of the recording
* The right to request a copy of the information and confirmation that it is held
* The right to be informed about the use, disclosure and retention of the recording
* The right to make complaints

These rights are described in more detail in the Information Rights and Access Protocol.

1. APPLICATION AND AUDIT

Compliance with this protocol will be audited and the results fed into the Plan, Do, Check, Act Cycle described in the Information Risk and Audit Protocol.

* Upwell Health Centre and Welle Ltd (Pharmacy) will list the information rights on our privacy policy
* All staff should be able to recognise and refer information rights requests to the right person
* All staff, visitors and service users should have access to the Data Protection Officer’s contact details to support with rights
* New projects, suppliers or systems must be raised with the Data Protection Officer for review
* Upwell Health Centre and Welle Ltd (Pharmacy) will keep a log of all information rights requests to ensure that we are responding in a consistent and timely way
* Staff must confirm that they have read and understood this protocol
* This protocol will be reviewed annually or sooner in the event of significant learning or change
* This protocol should be read in conjunction with the other protocols in the Data Protection and Security policy suite
* Subject Access Requests are covered in the Disclosures and Access Protocol

1. APPENDIX A: COMPLIANT RECORDING CHECKLIST

|  |  |
| --- | --- |
| I have identified all the recording that happens at our organisation, added it to the Processing Activities Log and shared with our Data Protection Officer |  |
| The entries related to recordings in our Processing Activities Log include a retention period for recordings |  |
| All relevant staff are aware of the requirements about minimisation of data captured as part of recordings |  |
| All physical assets capable of making recordings have been added to an asset log so that they can be tracked and returned when required |  |
| All physical assets capable of making recordings have a nominated owner that can monitor associated risk and usage |  |
| The nominated owner will regularly check that the date and time stamp recorded on images and audio recordings are accurate (for example, when the UK switches between summer and winter time) |  |
| All physical assets capable of making recordings will be destroyed in line with the Information Lifecycle and Data Quality Protocol |  |
| All staff involved with making recordings are aware that that should not be removed from the premises without being signed out on the asset log |  |
| Where recordings are made, this is recorded within the main record along with the consent form (barring CCTV and general telephone recording) |  |
| Disclosure of recordings to third parties is subject to an Information Sharing Agreement or discussed with the Caldicott Guardian / Data Protection Officer |  |
| Audio or video recording software that is supported by a third-party provider is subject to a compliant contract that has been reviewed by the Data Protection Officer |  |
| Transfer of recordings is through encrypted methods in the first instance. Alternative routes will be discussed with the Data Protection Officer |  |
| Staff involved with making recordings, including still images, are aware that they must not be obtained using personal devices such as mobile phones. |  |
| Recordings are stored securely in the shared drive and will not be stored in email accounts, personal drives or on personal devices such as mobile phones |  |
| We are not using old hardware that compromises the accuracy or quality of recordings |  |