Organisation Name: Woodlands Medical Practice

Audio, Visual and Photography Policy (England)

Version	Edited by	Date issued	Next review date
1.0	Fiona Butcher	13.05.2026	1.04.2027

Position	Named individual
Information Governance Lead	Dr Zammad Chishti
Data Protection Officer	Fiona Butcher
Practice Manager	Fiona Butcher

Overview for all staff

- All staff have a legal duty to act in patients' best interests when creating, using, or handling recordings for clinical, teaching, or publication purposes, and to maintain patient confidentiality.
- Remote consultations are generally unsuitable when an intimate examination is required; patients should be seen in person or referred as appropriate.
- Patient consent for audio or visual recordings must be obtained on arrival at the practice and not at the start of the consultation.
- Covert recordings by clinicians should only occur in exceptional circumstances when no alternative means of obtaining information exist.
- Images sent by patients during remote consultations must be stored solely on organisational systems and never on personal devices.
- Audio-recording meetings may be appropriate in some circumstances as this ensures an accurate and reliable record of discussions.

Table of contents

1 Introduction

1.1 Policy statement

The term 'recordings' will be used throughout this policy and refers to audio recordings, videos, photographs and any other type of visual image of patients made by using any recording device, including mobile phones. Whilst this policy is predominantly for staff, guidance is also provided for patient expectations.

It is the duty and legal obligation of all staff to act in the best interests of patients when making recordings for the purposes of clinical assessment, teaching or publication or when handling such recordings. All staff are under a legal duty to keep patient records confidential.

The GMC guidance titled Making and using visual and audio recording of patients advises that when making or using recordings, patients' privacy and dignity must be respected. All clinical recordings are subject to this policy, irrespective of who owns the equipment or the materials on which they are produced.

This policy is to be read in conjunction with CQC GP mythbuster 100: Online and video consultations and receiving, storing, and handling intimate images and the following organisation's policies:

- Accessible Information Standard Policy
- Communication Policy
- Confidentiality and Data Protection Handbook
- Disciplinary Policy and Procedure
- Portable Device Policy
- Staff Induction Policy
- Vehicle Travel Policy
- Work Related Events Policy

Any breach of this policy may lead to disciplinary action and has the potential for prosecution and referral to the Information Commissioner's Office (ICO). Staff must ensure that all processes comply with both the Data Protection Act 2018 and Data (Use and Access) Act 2025.

1.2 Status

In accordance with the Equality Act 2010, we have considered how provisions within this policy might impact on different groups and individuals. This document and any procedures contained within it are non-contractual, which means they may be modified or withdrawn at any time. They apply to all employees and contractors working for the organisation.

2 Compliance and guidance

2.1 Protecting data

Data protection guidance to support audio recordings and video filming is at Annex A. Guidance should also be sought from the Confidentiality and Data Protection Handbook.

2.2 Communication standards

Effective communication between clinicians and patients is essential to good care as advised within the GMC's professional standards on Communication.

Further reading can be found in the organisation's Communication Policy.

2.3 Safeguards for patients accessing online and video healthcare

There are additional potential patient safety risks with phone, video and online consultations. Should there be any concerns relating to any safeguarding issues, staff must adhere to the organisation's Safeguarding Handbook and also seek advice from the Safeguarding Lead.

2.4 Consent for audio and visual recordings

Consent requirements including consent for recording digital images and/or video can be found at Annex B and the consent form for video and/or audio recordings is at Annex C.

Further guidance can be sought from the organisation's Consent Guidance.

2.5 Register of audio and visual recordings

All recordings are to be added to the Recordings Register that is at Annex D.

2.6 Use of mobile phones and smart devices within the organisation

Mobile phone guidance for audio and video use to support both clinical and general business use is at Annex E.

The personal use of mobile phones and smart devices, i.e., smart watches, smart glasses and other emerging technologies is detailed at Annex F.

2.7 Patient expectations for filming and recording within the organisation

Information detailing patient requirements when using audio recording and video filming within the organisation is detailed at Annex G.

A supporting poster is available and is to be placed in patient facing areas to further explain the reasoning why recording is only permitted within a consulting room to ensure other people's confidentiality is not compromised.

2.8 Practice telephone use and expected standards

The practice phones are only to be used for business purposes and personal use is strictly prohibited except in the event of an emergency.

The guidance at Annex H details telephone use and the required standards including answerphone messaging, telephone audits, staff requirements when dealing with a medical emergencies and the governance actions needed to inform callers that the conversation is being recorded.

2.9 Triage and consultations

Patients telephoning the organisation to request an urgent or same day appointment with a clinician are initially managed using telephone triage. Guidance on the process including the actions required for telephone consultations can be found at Annex I.

When patients contact the organisation by online means, then the process is detailed at Annex J. All patient requests will be triaged by either a GP or AHP who will decide what the required course of action. Further questions are ordinarily asked to ascertain the appropriate care navigation including prioritisation.

The GMC remote consultation flow chart illustrates the factors that this organisation should consider when determining if it is appropriate to use a remote method for the provision of healthcare.

2.10 Undertaking video consultations

It is commonplace for trainee GPs to undertake video consultations as part of their training. While it is not mandatory for a GP registrar to record their consultations, there are instances when recording a consultation can provide educational value.

Annex K provides stepped recommendations for video consultations.

2.11 Retention periods

Retention periods for all types of records are detailed in both the NHS England Record Management Code of Practice and the organisation's Record Retention Schedule.

2.12 Copyright

All recordings remain the copyright of this organisation, and this must be protected on further use of the recordings such as sharing images for publication. Staff must ensure that the copyright always remains with the organisation and not the publisher.

2.13 Research

For recordings made solely for the purposes of research, the consent form should be signed, and the research work must have organisation approval. All research projects using clinical recording must be registered with the Data Protection Officer.

Further reading can be found in the Research Guidance Document.

Annex A – Data and its protection

Storing and disposing of recordings

The GMC explains in its guidance titled Making and using visual and audio recordings of patients that recordings made as part of the patient's care will form part of the medical records and must be treated in the same way as other medical records. Should a recording be made for secondary purposes, staff must ensure that there is an agreement about the ownership, copyright and intellectual property rights of the recording.

Recordings are to be retained in accordance with NHS England's Records Management Code of Practice and the organisation's Record Retention Schedule.

For further detailed information, see the organisation's UK GDPR Policy and ICO guidance.

Receipt and transferring data

When the patient has chosen to capture and transfer images, issues of device usage/transfer and data protection/information governance are not relevant until the image has been received by the healthcare professional.

Once received, any onward data transfer and storage should meet data protection regulations and information governance requirements. Issues of consent will differ and will relate to any onward transfer, storage and use of the images only once they have been received. Consent is required to be recorded for every single transmission.

Sending sensitive information via NHS mail

Should any image be forwarded by email, the clinician must request that it is sent to their secure and encrypted @nhs.net or @nhs.uk email address.

If a clinician needs to forward or respond to an email that contains sensitive information, they can do so, even to a non-secure email address. However, they must always evaluate whether the email platform is the most appropriate method to communicate such data.

For further detailed information, refer to NHS England's Guidance for sending secure email (including to patients).

Sending sensitive information via a mobile phone

Emails may need to be accessed by a mobile phone although, should the email then need to be forwarded, this should only happen providing the following can be confirmed:

- It can be guaranteed that all PID can be encrypted
- Bluetooth is disabled and will not be utilised to make the transfer of the images
- Images can be downloaded using a wireless network provided the network conforms to the required level of encryption
- It is acceptable to transfer data from a mobile device using a cable between the device and a desktop PC if the PC is not used as a storage device

In circumstances when a secure transfer cannot be guaranteed, data should be anonymised as a solution and then safely transferred.

Data Protection Impact Assessment (DPIA)

It is considered best practice to undertake DPIAs for any existing audio visual or photographic procedures to ensure that this organisation meets its data protection obligations. DPIAs are classed as “live documents”, and processes should be reviewed continually. As a minimum, a DPIA should be reviewed every three years or whenever there is a change in a process that involves personal data.

For further detailed information and a DPIA template, see the organisation’s UK GDPR Policy.

Reporting data breaches, incidents and weaknesses

At this organisation, if a member of staff becomes aware of a data breach, they are, when possible, to contain the breach and advise their line manager immediately. The reporting of any losses, theft or damage to documentation or computer assets should be made at the first possible opportunity and with a degree of urgency. This should then be reported to the Information Governance Lead and/or the Data Protection Officer.

Information to be provided will include details of the losses or incidents and a detailed description of the data lost using the appropriate breach reporting form. Near misses and possible weaknesses will also be reported through this method.

For further detailed information, see the organisation’s Information Governance Breach Reporting Policy.

Standards and expectations

All staff must adhere to the National Data Guardian 10 Data Security Standards. The standards outline the value of the safe, secure, appropriate and lawful sharing of data.

Annex B – Consent

About

The GMC guidance titled Making and using visual and audio recordings of patients details that staff at this organisation must obtain the patient's consent to make a recording that forms part of the investigation or treatment of a condition or contributes to the patient's care.

Staff must explain to the patient why a recording would assist their care, what form the recording will take and assure them that the recording will be stored securely. Furthermore, whenever practicable, staff should explain any possible secondary uses of the recording in an anonymous or coded form when seeking consent to make the recording. Staff must record the key elements of the discussion in the patient's medical record. Patients must be advised that they have the right to withdraw consent at any time.

Video recordings would ordinarily only be required for clinicians in support of training, although this is not an explicit requirement, merely viewed to be a useful tool. Consent is to be sought, and this is to be made upon arrival at the practice as opposed to when in the consultation room. This is to allow the patient to fully consider the request and also so that the patient does not feel pressured or obliged to agree. To further support the decision, a notice is to be placed in the reception/waiting room areas that advises patients that consultations may be recorded and for what purpose, i.e., GP training.

Following the appointment, the patient is to be advised to return to the reception to sign the consent form confirming that they are content that the recording can be used for its intended purpose.

The consent form for video and/or audio recordings can be found at Annex C.

Further information on consent can be found in the organisation's Consent Guidance. Furthermore, detailed guidance including some wording for a waiting room notice can be found in NHS England's Southeast Thames Valley and Wessex GP school guidance titled Guidance for recording consultations in General Practice.

Capacity

Should a clinician judge that an adult patient lacks capacity to decide upon an investigation or procedure that involves a recording, they must adhere to GMC guidance and obtain consent from someone who has legal authority to do so on the patient's behalf before making the recording.

In a situation when no individual has legal authority or when treatment must be provided immediately, recordings may still be made providing they form an integral part of an investigation or treatment that is being provided.

For further detailed information, see the organisation's Mental Capacity Act Policy and the CQC About the Mental Capacity Act guidance.

Consent for children and young people

The GMC advises that children or young people under 16 who have the capacity and understanding to give consent for a recording may do so but clinicians must encourage them

to involve their parents in decision making. When a child or young person cannot understand the nature, purpose and possible consequences of the recording, staff must obtain consent from a person with parental responsibility to make the recording.

For further detailed information, see the organisation's Consent Guidance and the CQC's GP mythbuster 8: Gillick competency and Fraser guidelines.

Disclosure and use of recordings

In its guidance titled Recordings made as part of a patients care, including investigation or treatment of a condition, the GMC stipulates that recordings made as part of the patient's care form part of the medical record and should be treated in the same way as written material in terms of security and decisions about disclosures. Therefore, staff must adhere to the GMC's Confidentiality: good practice in handling patient information guidance.

The GMC further advises in its cross-speciality guidance titled Making and using visual and audio recordings of patients that anonymised or coded recordings may be disclosed for use in research, teaching or training, or other healthcare-related purposes without consent. In deciding whether a recording is anonymised, clinicians should bear in mind that apparently insignificant details may still be capable of identifying the patient. Clinicians should be particularly careful about the anonymity of such recordings before using or publishing them without consent in journals and other learning materials, whether they are printed or in an electronic format.

Clinicians may only use an approved encrypted app that has been designed for video or audio recording, and the recording can only be stored on the server for the shortest of either:

- Six months
- On completion of the GP resident doctor's placement

After this period, the recording will be deleted.

All recordings are to be added to the Recordings Register at Annex D.

The organisation will provide a dedicated recording device. Personal smartphones or tablets should not be used for recording purposes unless it is under the sole condition that any recording will be both encrypted and transcribed near-instantly to a secure, remote server.

All such recordings will be deleted from any phone, tablet, or personal online cloud storage.

For further reading, refer to the organisation's Confidentiality and Data Protection Handbook and also the Caldicott and Confidentiality Policy.

Patient's request for copies

Patients and their parents/carers have the right to obtain copies of the clinical notes under the Data Protection Act 2018. The normal rules for a subject access request apply and the Subject Access Request Policy should be followed when dealing with a request of this type.

For further information, refer to the organisation's Access to Medical Records and Online Services Policy.

Consent for publication

If a recording is to be used in any type of public media, staff must obtain the patient's consent in writing using the consent form This is regardless of whether the patient will be identifiable from the recording.

The GMC advises that if a clinician wishes to publish a recording of a patient that was made as part of their care and consent was not obtained at the time the recording was made, then consent must be obtained. If the recording is anonymised, it is good practice to seek consent prior to publication.

Covert recording without consent

Covert recording should ordinarily not be undertaken unless in exceptional circumstances and when there is no other way to obtain information.

Examples of this could include:

- When it is necessary to investigate or prosecute a serious crime
- Should there be a need to protect someone from serious harm, such as if there are grounds to suspect a child is being harmed by a parent or carer

Before any covert recording can be carried out, authorisation must be sought from a relevant body in accordance with the law. In any situation when covert surveillance is proposed, the clinician should discuss this with an experienced colleague and/or seek independent expert advice. Patients should be informed of any use of CCTV.

For further information, refer to the organisation's CCTV Monitoring Policy.

Annex C – Consent form

Patient consent for recording digital images and/or video

Patient details			
Surname		**Forename**	
Title		**Date of birth**	

We are hoping to make video/digital recordings of some of the consultations between patients and [insert clinician name] whom you are seeing today. The recordings are used by [doctors training to be a GP to review their consultations with their trainers]. The recording is ONLY of you and the clinician talking together. Intimate examinations will not be recorded, and the camera/recorder will be switched off on request.

All recordings are carried out according to guidelines issued by the General Medical Council and will be stored securely in line with the UK General Data Protection Regulation (UK GDPR). They will be deleted within six months of the recording taking place.

You do not have to agree to your consultation with the doctor being recorded. If you want the camera/recorder turned off, then please inform the reception team. This will not be a problem and will not affect your consultation in any way. But if you do not mind your consultation being recorded, please sign below. Thank you very much for your help.

I have read and understood the above information and give my permission for my consultation to be recorded.

To be valid, both Parts A and B are to be completed by either patient or the person accompanying the patient

A. BEFORE CONSULTATION

Signature of the patient

Patient's name		**Date**	
Signature			

Signature of person accompanying patient to the consultation:

Patient's name		**Date**	
Relationship		**Signature**	

B. AFTER CONSULTATION

After seeing the clinician (delete as appropriate)

- I am still willing for my consultation to be used for the above purposes
- I no longer wish for my consultation to be used for the above purposes

Signature of the patient

Patient's name		**Date**	
Signature			

Signature of person accompanying patient to the consultation:

Patient's name		**Date**	
Relationship		**Signature**	

CLINICIAN DETAILS

Name		**Date**	
Signature		**GMC No.**	

Annex D – Recordings register

Date/time of the recording	Patient identifier	Responsible Person	Comments, i.e., disposed of or released to patient	Date of erasure of recording

Annex E – Mobile phone use for business purposes

Clinical use

This organisation will follow the UK Guidance on the Use of Mobile Photographic Devices in Dermatology when using a mobile device to make a recording of any type. The guidance covers the following:

- The benefits and risks of using mobile devices
- Data protection and confidentiality issues
- Taking patient images with mobile devices
- Standards on consent, use of mobile devices and the safe transfer and storage of images captured with mobile devices.

At this organisation, staff are reminded that the transferring of images via mobile devices must only be done using the Pando app. The BMJ's Medical photography using mobile devices guidance details the key principles of medical photography, including lighting, focus, location and severity, colour, perspective and positioning.

Camera usage and video recordings

While the use of mobile devices for clinical photography can be extremely beneficial, in terms of patient care this will also present risks.

Any decision to take clinical videos or photographs must be based on clinical judgement in the interest of patient care. Due to the ease with which images can be captured, staff are to be mindful that this could offer the potential for a breach of confidentiality. To maintain the confidence of patients, a careful approach must be taken within the organisation or immediately outside the premises so that no patient can be identified as having attended.

There may be times that remote consultations take place, and patients will send images to the organisation for diagnosis and treatment. These images are only to be stored on organisation systems and not personal mobile phones.

Receiving images directly from patients (not via video consultation)

There may be times that remote consultations are taking place and patients will send images to the organisation for diagnosis and treatment. These images are only to be stored on organisation systems and not personal mobile phones.

As a general principle of good practice, patient or staff identifiable information should not be stored on a mobile computer unless it is encrypted to the standards required in the organisation's Portable Device Policy.

Should a patient be requested to submit an image directly to the organisation, they should do so using the process detailed on the organisation's website. This includes completing an e-form and uploading a photograph.

Multi-factor authentication

Data security requirements may include the use of multi-factor authentication (MFA).

When no work phone has been provided, the use of a personal phone for this purpose will be authorised by the practice and may be a requirement of the employee's role. This is a requirement in England. Further reading can be sought from NHS England's Multi-factor authentication (MFA) policy.

Recordings during a meeting

There may be circumstances when it is appropriate or deemed to be useful to audio-record a general meeting or a meeting with a member of staff. Recording a meeting is a reasonable request as it provides guarantees that all notes can be relied upon for accuracy.

While any recording is to ordinarily ensure that there is a confirmed record, accuracy is especially important when there is a lot of information being discussed, for example at a practice meeting or within a staff specific setting such as when it is disciplinary, grievance or performance related.

Before any recording commences, the following should be discussed and agreed:

- Agreement to record should ordinarily be obtained although it should be noted that having agreement to record is not an absolute requirement, e.g., for operational need or purpose
- The recording device will be identified, and no covert recording can be made by any of the attendees
- If for disciplinary, grievance or performance purposes, a copy of the recording should be offered to the staff member involved. This must be an accurate copy and not have been amended
- Staff should be assured that it is in their best interests as the record of the meeting will be accurate, fair and that there can be no misunderstandings at a later point
- The recording will not be shared to third parties unless this is an absolute requirement
- Should it be agreed that the meeting will be recorded, it is unlikely that a second means of minuting will be required. Therefore, it is essential to ensure equipment is fully functioning before the meeting begins and should include:
    - Power sources are fully charged
    - Sound is adequate throughout the room
    - All attendees are positioned so that they can be heard

Use of technology when driving

Only 'hands free' telephone calls may be made while driving for work purposes. Under no circumstances should the driver use their mobile phone or other smart device by any other means for any other purpose other than in this mode. If the employee's vehicle does not have this function, then they should find a safe place to park to make calls or to check messages.

Employees should understand that the law requires drivers to have proper control of their vehicle at all times. Individuals can be prosecuted for careless, inconsiderate or dangerous driving.

With the introduction of the Corporate Manslaughter and Corporate Homicide Act 2007, the organisation also faces greater accountability for its employees including in the case of allowing them to drive unsafe vehicles.

Further information can be found in the organisation's Vehicle Travel Policy.

Personal use

Mobile phone use, including the use of smart devices, is detailed at Annex F.

Annex F – Mobile phones and smart devices in the workplace

Use of personal mobile phones

Personal mobile phone usage is permitted solely for business purposes during the working day. If it is necessary to make or answer a personal call, then this should be done in a private area, and any personal calls or texts are to be made during breaks or lunch breaks.

From a customer service perspective, mobile phones should not be visible as this could be seen as *'their needs are not as important as your social life'* irrespective of need or whether the employee only uses a mobile phone in an emergency or for business purposes. Therefore, phones are to be kept in a safe and private location during the working day, e.g., a locker, bag or desk drawer. This will also reduce any risk of an opportunistic theft.

Ordinarily there is no reason for non-clinical use for video recordings within the organisation apart from team meetings taking place regularly by video link.

Social functions

During a work-related social event such as Christmas party or a fund-raising event, under no circumstances should any images be taken and uploaded to social media that could identify the organisation, practice premises, patients or staff without the express permission of the management for images of the organisation or premises, and/or the persons who are pictured.

Further reading can be found in the organisation's Work-Related Events Policy.

Smart devices

There are emerging 'smart' technical products that need to be considered for use within a general practice setting due to data protection law and the stringent requirement to maintain patient confidentiality.

A smart device is any personal or work-issued equipment capable of recording, capturing, storing or transmitting audio, visual or other data. This includes, but is not limited to, smart glasses, smart watches, body-worn cameras and similar emerging technologies.

The following standards are to be adhered to:

- Staff are not to use personal devices, including smart wearable technology, to record, monitor, live stream or transmit audio, video or images in the workplace or during work-related activities unless expressly authorised

- The use of personal smart wearable devices for recording or data capture during working time is strictly prohibited unless:

    - It has been formally approved by the Information Governance Lead; and
    - There is a clear and lawful basis for processing the data; and
    - Appropriate privacy information and safeguards are in place

- A smart wearable device, such as a smartwatch, may be worn but it must have the recording function disabled during working time or in specified work activities when there is a risk to confidentiality, data security or professional standards

  It should be noted that clinicians must still adhere to the 'bare below the elbow' principles as detailed within the Uniforms, Dress and Appearance Policy and as such may only wear one plain band ring and must not wear a wristwatch (including smartwatches) in the clinical area

- Smart wearable devices and technologies with intended capacity to covertly audio or visually record are not permitted for use as there is no reason for them to be within a general practice workplace. They do not conform to data protection and UK GDPR law. Examples of these would be smart glasses, or recording devices that are designed for another purpose, such as a pen, USB plug, air freshener or other 'spying' resources

- All staff members are responsible for ensuring that personal devices used during working time do not compromise information security, privacy or the organisation's reputation

While ordinarily reasonable adjustments would be considered to support a disability under the Equality Act 2010, smart glasses would not meet this criteria due to the significant data impact, patient safety and potential reputational concern. A BBC article titled Regulator contacts Meta over workers watching intimate AI glasses videos provides an insight into the concerns with this emerging technology.

Any unauthorised recording, transmission or storage of personal data using smart wearable devices may constitute a data protection breach and will be treated as a serious matter, which may lead to potential prosecution, disciplinary action and/or regulatory reporting and in line with the organisation's Disciplinary Policy and Procedure.

When covert recordings are permissible

Covert recording should ordinarily not be undertaken unless in exceptional circumstances and when there is no other way to obtain information. Further information can be sought from Annex B.

Social media and confidentiality

All personnel owe a duty of confidentiality and should not reveal or disclose any confidential information about patients, the organisation and its business or how the organisation operates. Employees must be mindful of their duty of confidentiality at all times when using mobile phones and smart devices including when using social media for their personal use.

Examples of potential confidentiality breaches:

- Sending a photo that reveals patient information
- Forwarding an image that includes that of a patient within the organisation
- Posting derogatory comments on social media regarding their employer

The BMA offers advice in its guidance titled Ethics of social media use.

Further information can be sought within the organisation's Confidentiality and Data Protection Handbook and also the Communication Policy.

Liability for loss or damage of personal equipment

The organisation will not accept any responsibility or liability for a mobile phone or smart devices that is lost, stolen or damaged while on the organisation's premises or during work time.

To reduce the risk of theft, employees are encouraged to keep doors locked when rooms are not in use, and use cupboards, drawers or lockers to stow away valuable possessions, including mobile phones and smart devices.

Breaches of mobile phone usage

Potential breaches of this policy will be treated very seriously. Any employee found to be in breach of this policy may be subject to action under the organisation's disciplinary policy and procedure.

Annex G – Expectations of patients who audio and video record

BMA guidance

The BMA advises that patients are increasingly asking doctors if they can record or video consultations on their phones or other devices. Its document titled Patients recording consultations provides detailed guidance.

At the end of the consultation, the clinician can ask the patient to provide a copy of the recording, if they wish, so that this can be added to the patient's healthcare record to form a permanent record of the consultation and what was discussed.

Overt versus covert

The differences between overt and covert is that overt refers to actions, behaviours, or expressions that are open, visible and easily observed, whereas covert refers to actions that are hidden, concealed, or subtle. Therefore, an overt recording has been sanctioned, and a covert recording is unknown.

Video and audio recording devices

As technology evolves, there will be new devices and methods that enable high definition video and audio recording.

Staff may encounter patients using commonplace devices within the practice such as a smartphone for audio or video recording purposes and other frequently used devices might include smart watches. However, there are emerging smart wearable and other covert recording devices that make it more difficult to notice that a recording is occurring such as smart glasses.

Patients are requested to ask for prior permission to record their consultation. However, permission will not have been sought if the recording is made in another areas of the practice, such as a waiting room, or at the reception desk.

Should a staff member see a patient making a recording that poses a risk to other patient's confidentiality, then they are to be informed that their actions are inappropriate and that they should cease and delete the recording. Furthermore, they should be told to refrain from making any further recordings explaining other patients' confidentiality may be compromised and that legally, explicit consent must be obtained when recording others.

Should the staff member not feel confident to confront the person making the recording, then they are to escalate this concern to a manager. In all instances, the Practice Manager should be informed as there might be other governance considerations, such as raising this as a significant event.

A poster detailing appropriate and inappropriate use of audio and visual recordings is available and may be placed in a prominent patient facing area.

Annex H – Telephone use, standards and procedures

Acceptable and authorised use

The practice phones are only to be used for business purposes and personal use is strictly prohibited except in the event of an emergency. Calls to premium-rate telephone numbers are also prohibited. Calls to areas outside the UK are blocked. Should it be necessary to call a number, Practice Manager authorisation will be required.

All calls, whether incoming or outgoing, are always to be handled professionally and courteously.

Full information on the use of organisation telephones and call handling procedures can be found in the organisation's Communication Policy.

Assuring telephone standards

At this organisation, telephone calls are recorded as a tool to assist with both responding to any complaint or concern and to support the team by reducing any negative concerns by monitoring the quality of the call. This organisation will undertake a regular compliance audit that involves call monitoring and will provide both feedback and, when required, additional training to ensure that an efficient and excellent service is offered.

There is a set of key standards that it is expected each patient or caller will receive. When auditing the quality of any call, it is expected that the following standards will be met:

Key	Standards	Achieved (Y/N or N/A)
1	Was the call answered?	
2	Was the call answered within the specified number of rings?	
3	Did the staff member identify themselves?	
4	Did the staff member identify the organisation?	
5	Was the staff member friendly and polite?	
6	If the call was not answered, did it go to voicemail?	
7	If so, was the appropriate message left that did not breach any confidence of the intended recipient?	

The management team will monitor, provide feedback and implement any actions as required. This audit will also be discussed within the governance standing agenda at select organisation meetings.

An audit template is available below in the audit and review of telephone recordings section.

Medical emergencies

Calls about emergencies should be made to the local ambulance control and handled in accordance with the current When to call 999 guidance. The call handler will ordinarily need

the ODS code, and they will go through and explain any steps that are to be followed in a calm and professional manner. For further information, refer to the organisation's Medical Emergencies Guidance Document.

Practice answering machine

The answering machine is to be turned on at the close of business daily and switched off at the start of the working day by a member of the reception team. The outgoing message is not to be amended unless authorised by the Practice Manager. Patients are unable to leave messages on the answering machine.

Patients' answering machines

This organisation will not routinely leave messages on a patient's answering machine unless it is deemed urgent. This is to ensure that patient confidentiality is always maintained. If it is necessary to leave a message, the message must be brief and not breach confidentiality. An appropriate example being: "Please call the practice when you are free to discuss your appointment".

It is essential that clinical information, patient-identifiable information, or other sensitive information is not disclosed during the recording of the message.

Notifying callers of any call recording system

Information regarding call recording, including the reason why any call will be recorded, is to be detailed at the following:

- Any incoming call, including any calls using desktop software, mobile apps or an internet browser-based application

- For outbound calls, including telephone consultations, when no automated announcement exists, the caller will inform the recipient by reading a statement which says 'This call is being recorded for safety, security and training purposes'

- A summary of this policy on both the website and within the practice privacy notice

Should a patient request that their call is not recorded, then they are to be advised that it is organisation policy to record all calls to ensure the safety and security of both patient and employee. They are also to be advised that there is no option to switch off the recording facility. If the patient continues to insist that they do not wish the call to be recorded, then they are to be advised that the call cannot continue and that they should contact NHS111 or 999 in an emergency. It should be noted that secret recordings are not permitted.

Procedures for managing and releasing call recordings

When a telephone system allows telephone conversations to be recorded, the following should be noted:

- All recordings will be stored securely with access to the recordings controlled and managed by the Information Governance (IG) Lead or any other persons authorised to do so

- Access to the recordings is only allowed to satisfy a clearly defined business need and reasons for requesting access must be formally authorised by only the IG Lead. All requests for call recordings should include the following information:

    - The valid reason for the request
    - Date and time of the call if known
    - Telephone extension used to make/receive the call
    - External number involved if known
    - When possible, the names of all parties to the telephone call
    - Any other information on the nature of the call

- The browsing of recordings for no valid reason is not permitted

- UK GDPR allows persons access to information that the organisation holds about them, and this includes recorded telephone calls. Therefore, the recordings will be stored in such a way to enable information to be retrieved

- Requests for copies of telephone conversations made as data subject access requests under UK GDPR should be notified in writing as per the organisation's Access to Medical Records Policy and, subject to assessment, the requestor will be provided with access to the recording. It would be best practice to discuss any such data request with the IG Lead and/or the Data Protection Officer (DPO)

- All reasonable attempts will be made to confirm that the identity of the individual making the subject access request matches the identity of the caller. If in doubt, the final decision will be made by the DPO

- In the case of a request from an external body in connection with the detection or prevention of crime, e.g., the police, the request should be made in writing and forwarded to the IG Lead who will liaise with the DPO to agree an appropriate course of action

- When there is agreement to provide a copy of any recording, this will be provided in a format the organisation can reasonably expect the requester will be able to use. The organisation will consider the individual's preference versus the practicality and cost of preparation. Formats are likely to include WAV, MP3 or another digital format or transcript

- Any recordings released to other services or users of the organisation must be kept securely and in compliance with this policy. Once the recording has been used for the agreed purpose, it must be deleted

Further sharing of any call must be authorised by the IG Lead.

Audit and review of telephone recordings

The audit and review of telephone recordings may be used to:

- Check for mistakes

- Facilitate staff training, coaching and support

- Prevent, detect, investigate and prosecute fraud

- Verify what was said if there is a dispute or complaint
- Protect from abusive behaviour, coupled with monitoring language and tone
- Monitor the quality of call handling and customer service and to ensure the information provided is consistent and accurate
- Help to plan and make improvements to the organisation's services
- Verify the details of the call for the purposes of, or in connection with, any legal proceedings
- As evidence within an investigation should a misconduct, performance or capability concern arise

Requests for copies of telephone conversations as part of staff disciplinary processes will only be released with the written agreement of the IG Lead or any other authorised person. The DPO is to be consulted before any approval is granted.

All staff will have telephone consultations audited during their probationary period and annually thereafter.

- Three randomly selected conversations will be listened to and assessed using the audit tool. This number can be increased to five when further clarification of practice is required
- The aim is for all to score at least 80% on the audit. Anyone scoring below this will be informed and then reaudited within three months to monitor for improvement
- Feedback will be provided to individual staff regarding good practice and also any areas for improved practice. Results are to be saved on individual HR records. Any professional practice concerns are to be shared with the Partners
- The collective results of this audit are to be recorded as being one of the annual practice audits
- Any exemplary conversations, likewise, poor conversations can be used for training purposes. The obvious place for this is to be recorded is as a significant event to highlight what went well or what went wrong.

The audit criteria are as follows:

Criteria	Standard
Staff member carries out a full introduction	100%
The identity of the patient is confirmed	100%
The consultation is conducted in a professional manner	100%
Confirm that consent has been given	100%
Confirm that the patient understands	100%
A clear plan in terms of any required next steps including prescriptions and/or reviews has been communicated	100%

Access to the telephone call recording system is logged and is traceable using an identifiable username and secure password. Access and usage may be monitored at any time to ensure adherence with this policy.

Any employee may request to hear call recordings in which they are personally involved. The employee should make a request in writing detailing the reason for hearing the recording to their line manager in the first instance who will escalate the request to an appropriate nominated member of staff for consideration.

Should any recording be released, a record of this is to be logged within the Recording Register as at Annex D. This register is maintained by the Practice Manager and audited by the IG Lead/DPO as required.

For further detailed information, refer to the MDDUS Recording telephone consultations with patients guidance.

Annex I – Telephone triage and consultations

Triage process

Patients telephoning the organisation to request an urgent or same day appointment with a clinician are initially managed using telephone triage. There are several key definitions used with care navigation and triage in a GP setting and as detailed within the NHS England guidance titled Digitally enabled triage.

The clinician triaging will:

- Introduce themselves clearly stating their name and role at the organisation
- Verify the ID of the caller, ensuring that they are the patient, or they have the consent of the person they are calling about. This should include three forms of identity to confirm the ID and can be a combination of name (first and last), telephone number and address
- Explain the purpose of telephone triage
- Ascertain as much information as possible:
    - What is the problem?
    - Where does the problem occur?
    - When does the problem happen?
    - What makes the problem better or worse?
    - What is the time frame for the problem?
- Consider the possible diagnoses based on the information provided
- Formulate an action plan:
    - Advice will suffice
    - Recommend that the patient visits the local pharmacy
    - Advise the patient that a telephone consultation with a clinician is required
    - Advise the patient that a face-to-face appointment with a clinician is necessary
    - It is an emergency situation and an ambulance is required
- End the call by providing an overview of the discussion and the plan, ensuring that the patient (or caller) fully understands what happens next and when to expect a call back from a clinician (if applicable)
- The patient is to be advised that the clinician will attempt to call the patient a maximum of two times during the advised period. If the patient fails to answer the call, the clinician will not attempt a third call
- Advise the patient or caller that if the condition worsens, they should ring back or call 999 (as appropriate)

Further reading:

- NHS England Advice on how to establish a remote 'total triage' model in general practice using online consultations
- CQC report Getting to the right care in the right way – digital triage in health services
- CQC GP mythbuster 77: Access to GP services
- The organisation's Managing Access and Patient Demand Policy

Detailing information within the clinical record

As per all patient interactions, staff must ensure they record all the information gleaned during their telephone call on the patient's healthcare record. Equally, if a patient fails to answer a clinician's call back, this must also be annotated in the individual's healthcare record as it may be needed as evidence if a complaint is raised in the future.

Arrangements for a telephone consultation

At this organisation, clinicians are permitted to conduct telephone consultations with patients. Clinicians are allocated a set number of telephone consultations per session, with each consultation being allocated a set duration.

Telephone consultation process

Prior to calling the patient, the clinician should read the patient's notes on the clinical system, familiarising themselves with the notes made during the triage telephone call and any pre-existing medical conditions.

The clinician is to then telephone the patient and:

- Introduce themselves clearly stating their name and role at the organisation
- Verify the ID of the caller, ensuring that they are the patient, or they have the consent of the person they are calling about. This should include three forms of identity to confirm the ID and can be a combination of name (first and last), telephone number and address
- Explain the purpose of the telephone consultation
- Offer the patient the opportunity to explain what it is they are calling about, using questions and probing as and when required
- Seek clarification for any comments the patient has made, eliciting any relevant information
- Determine what it is the patient would like or thinks they need
- Consider a diagnosis
- Determine what treatment and/or medication is required
- Formulate an action plan, relaying the plan to the patient (or their representative)
- Ensure that the patient (or representative) understands and agrees with the plan

- End the call once assured that the patient is happy, advising the patient to call back or call 999 if their condition worsens (based on the advice given)

Documenting the telephone consultation

The clinician is to document the consultation in the individual's healthcare record ensuring that it is a true reflection of the consultation.

Prescribing by telephone

Clinicians at this organisation who are authorised to prescribe via telephone must adhere to the GMC prescribing guidance.

Risks of telephone consultations

While the GMC acknowledges that good telephone consultations can improve patient access to advice and treatment, clinicians at this organisation must ensure that they fully understand the risks associated with telephone consultations and take the necessary actions to mitigate such risks where possible.

The following are common examples of risks and action should be taken to avoid them:

- Poor information gathering due to the absence of significant questions
- Inappropriate decision-making, such as premature diagnosis
- Confusion due to poor communication
- Unmet expectations due to unclear instructions/advice

Patient failure to answer a call

Patients are to be advised that the clinician will attempt to call them twice during the allocated time frame.

Should the patient fail to answer the call, the clinician will not attempt a third call. The individual's healthcare record is to be annotated to reflect the failed communication attempt(s).

Note:

While medical emergencies should never be booked for a telephone consultation, consideration will always be given should there be a concern as to a patient's deteriorating condition. In this instance, reference is to be made to both the Personalised Care and Safety Netting Policy and the escalation process within the Home Visit Policy.

Rebooking

The clinician is to message the reception team, asking them to contact the patient to arrange a call when the patient can accept a call from the clinician. This will be during the usual times allocated for telephone consultations.

If the reception staff have any concerns, they are to speak to a member of the clinical team to request advice. It is imperative that all contacts and decisions are accurately recorded in the individual's healthcare record.

Annex J – Online triage and consultations

Overview

GP practices in England must keep their online booking open all day during working hours with the detail being specified within the GP contract 2026/27: what you need to know.

Patient services must not be compromised when attempting to reduce footfall within the organisation and, at this organisation, online services will include patients having the ability to:

- Ask questions
- Report symptoms
- Submit an administrative request
- Discuss other information
- Review a known problem or condition
- Upload photos where appropriate

During the consultation, clinicians should ask and record who is in the room with the patient and ask more questions than normal about how the patient is doing generally. If the consultation is with a child, they should try to speak with the child if appropriate. If this is not possible, ask to see the child on the video. After the consultation, a detailed record is required within the patient's notes.

At this organisation, clinicians conduct online consultations with patients by generic email, the NHS App or a recognised secure method of online request. An online consultation enables patients to contact a GP or other health professional over the internet. A patient can ask questions, report symptoms and get advice from their GP and access NHS self-help information, signposting to services and a symptom checker using a smartphone, tablet or computer.

To access their NHS account, a patient will need to set up an NHS App login and prove who they are. The NHS account then securely connects to information from the organisation.

At this organisation, clinicians will adhere to the GMC principles when providing remote consultations to patients.

For further detailed information, refer to NHS England's Online consultation tools guidance and the organisation's Managing Access and Patient Demand Policy

Process

Online consultations are not appropriate for emergencies, and this should be made clear on the organisation's website. The organisation should also provide clarity regarding response times inside and outside of opening hours and how patients should expect a response, e.g., secure online message, phone call, text. The website should also provide information on which providers can be used for online consultations and how best to download the app or link.

A shared inbox should be used to ensure prompt responses to enquiries. The allocation of the right staff capacity (clinical and administrative) to process online consultation workflow should be established and a contingency plan put in place in case of staff absence, holidays,

technical failure and usability/access issues to ensure submissions are responded to in a timely manner.

Using the NHS App:

- Patients click on ‘check your symptoms’ and then ‘Ask Your GP for Advice’
- They fill in the online form with information about their symptoms, conditions or treatment, or those of someone they care for. They can also use it to request help with sick notes or GP letters
- They then submit the online form to their GP organisation where it can be viewed by an appropriate clinician
- The clinician reviews the form and decides on the right care for the patient, whether it is an email with advice or information, setting up a telephone or video consultation or a face-to-face appointment with a professional from the organisation
- If a patient hits a ‘red flag’ they will be directed to seek acute care

Using another type of electronic consultation

- The patient completes the online form via the website and follows the online instructions
- Once received by the organisation, an automated message is sent to the patient by text, email or as a secure online message to confirm that the online form has been received and indicating a likely response time

Verification and authentication

The responsibility for verification and authentication sits with the organisation. The process should require anyone using the service to prove their identity and restrict access only to authorised users, helping to ensure a confidential and secure service.

Organisations should consider if the measures they are using for verification and authentication are sufficiently robust and secure, specifically if the information required could be readily obtained or be available to others, e.g., friends, parents, family. If there are any concerns, the organisation should contact the patient to confirm identity through alternative means.

Responding to an online consultation

Once the form is received by the organisation, this will be securely downloaded into the clinical system to be triaged by the organisation’s staff and can be commented upon as with any other consultation. When responding to the consultation, clinicians should ensure that the patient is informed as to whom they are consulting with online.

Receiving and storing patient images

Staff at this organisation must be aware of the medico-legal issues regarding receiving and storing images, and adhere to the MDU guidance titled Receiving and storing patient images from online consultations.

Clinicians must adhere to the GMC's Good medical practice at Paragraph 9 which states 'you must provide safe and effective clinical care however you assess a patient and if you can't provide safe care through the mode of consultation you're using, you should offer an alternative if available, or signpost to other services'.

Intimate images

The MDU in its guidance titled Receiving and storing patient images from online consultations explains that intimate images (genitalia, anus and breasts) create particular medico-legal risks and in a normal consultation, when an intimate examination is needed, a chaperone would be offered to the patient and as detailed within the organisation's Chaperone Policy.

A further consideration is that taking, sending and receiving intimate images of children under 18 may potentially lead to a criminal investigation. Frail patients and those lacking capacity may need assistance from others in trying to obtain an intimate photograph and this could seriously impact their dignity and be an unreasonable burden on family or carers.

Consequently, when the need to obtain an intimate image arises in a clinical setting, and it is not possible to safely defer the consultation, the question arises as to whether a remote consultation is appropriate. In those circumstances, it should be considered whether the patient should be seen in person or a referral to a specialist colleague made when this is appropriate and necessary.

Making digital consultations work

The organisation should:

- Provide specific training for clinicians in triaging online
- Flag urgent consultations so that they can be prioritised more easily
- Use two-way secure online messaging to clarify information, ask additional questions, check understanding, send leaflets, attachments or request images without having to phone the patient unnecessarily
- Pass the online consultation to the patient's regular GP if appropriate
- If a patient later requires a further consultation, pass this to the clinician who originally dealt with the online consultation
- Optimise the skill mix to distribute work across the team
- Use pre-set messages which can then be customised to save time via the organisation facing portal or saved as an organisation document
- Configure signposting within the system to include local services
- Ensure the use of appropriate response templates to enable appropriate coding outcomes

Further reading can be found in the NHS England guidance titled Online consultation – frequently asked questions and support resources.

Annex K – Recommended guidance for video consultations

Purpose

It is commonplace for trainee GPs to undertake video consultations as part of their training. While it is not mandatory for a GP registrar to record their consultations, there are instances when recording a consultation can provide educational value.

This annex details the stepped recommendations. For further guidance, refer to the RCGP document titled Guidance for GP registrars and GP Educators on recording consultations for GP training purposes.

Patient verification

The clinician must, on calling the patient, verify the identity of the patient and ensure their details match those recorded in the clinical system. If the patient is well and able to speak to the clinician directly then a basic identification process should first be undertaken by asking the patient their full name, date of birth and full address.

Verification can also include:

- Patient information and contact details being matched against the patient record
- Use of NHS Spine integration for patient matching
- Checking details with patients and a visual ID check when possible.
- Physical checking of photo ID by organisation staff for initial use on VCA

Speaking to a family member or proxy

If the clinician calls the patient and a family or proxy member answers, it is advisable in the first instance to ask whether the patient can speak to them. If they are able to, the clinician should 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 the clinician 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.

The clinician should 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 without the patient's involvement and record the reason for this.

Multiple staff in the room

If the clinician has another member of staff in the consultation room with them when conducting a video consultation, they must ensure the patient is made aware of this and be asked to indicate that they are happy to proceed. This should be recorded in the consultation notes.

The process

To ensure compliance with the referenced legislation, the clinician must:

- Explain to the patient the purpose of the request to make the recording
- Ensure the patient understands why the clinician wishes to make the recording
- Ensure consent has been given freely, without influence
- Obtain the patient's signature on the organisation's consent form
- Advise the patient that it is their right to withdraw their consent at any time
- Ensure consent is recorded

Once the clinician is satisfied that the above actions have been completed, they will set the video camera to record and commence the consultation as they normally would. At the end of the consultation, the patient should be offered the opportunity to review the consultation and reaffirm their consent for the recording to be used for the purposes outlined.

For patient agreement, consent is detailed at Annex B.

Equipment

Audio-visual recording or clinical photography is ordinarily to be undertaken using the organisation's camera/digital video recorder/mobile device which is registered in the organisation's Information Asset Register.

When not in use, equipment is stored securely. The Practice Manager or nominated representative will ensure that the video camera or camera is signed out to the relevant clinician or photographer upon request. On completion of the recording, the organisation camera/digital video recorder/mobile device is to be returned and signed in.

Under no circumstances is the organisation's camera/digital video recorder/mobile device to be removed from the premises without prior authorisation from the Practice Manager or their nominated representative. The organisation's camera/digital video recorder/mobile device must be tested prior to use to ensure functionality including the correct date and time on the device being accurate.

Multiple patients' photographs should not be stored on the internal memory of devices. For further information, refer to the organisation's Portable Device Policy.

For further guidance on the required process, refer to the following GMC guidance:

- Recording made as part of a patients care, including investigation or treatment of a condition

- Making and using visual and audio recordings of patients