

Guideline

Information Governance - Use of cameras, video and audio recorders on Trust premises (including the use of smart phone and other mobile devices with recording functionality)

Relevant to:

All Trust Staff

Purpose of Guidance:

This guidance sets out the Trust's position in relation to both the use of authorised and unauthorised audio / visual recording devices on the premises by service users, visitors, staff, external agencies such as the police, Media and contractors.

Guidance to Follow:

Photography and video recordings are a valuable part of assessing and evidencing a patient's condition. They are beneficial in areas such as tissue viability, to demonstrate that the condition of a wound has improved, or in areas such as physiotherapy and speech and language therapy to demonstrate improvements of a particular condition over time.

Recordings taken using cameras owned by the organisation which illustrates a patient's condition or an aspect of the treatment, form a part of that patient's health record and are protected in the same way as any other health record. The existence of each photograph or recording must be documented in the patient's health record.

Recordings must be indexed and held in a suitable system to facilitate rapid retrieval at all times.

Acceptable Use

- 1.1 Authorised recording may be made for many purposes including:
 - 1.1.1 Clinical – to record the outward signs of a patient's condition, a medical or surgical procedure being applied to a patient; monitor therapeutic change over time, give feedback, enable patients and their carers/families to observe and learn from their actions/interactions, support training (such as parenting skills) and facilitate clinical involvement of the wider team;
 - 1.1.2 Teaching – to illustrate clinical signs and demonstrate interviewing/ counselling techniques;
 - 1.1.3 Training – to provide on-going training for the clinical team and for clinical supervision purposes;
 - 1.1.4 Research – as a defined aspect of an approved research project or study;
 - 1.1.5 Safeguarding – in some circumstances photographic evidence of injuries and/or bodily condition may be required to assist in a safeguarding investigation.
 - 1.1.6 Incident investigation and feedback – to ensure the correct recording of information in circumstances where there is a requirement to ensure absolute

Guideline

Information Governance - Use of cameras, video and audio recorders on Trust premises (including the use of smart phone and other mobile devices with recording functionality)

accuracy or in feedback meetings where the presence of a minute taker may be insensitive and intrusive;

1.1.7 Administrative support – to allow recording of a meeting without the need for attendance by a minute taker;

1.1.8 Security surveillance – specifically excluded from this policy/procedure. See the Trust CCTV (Closed Circuit Television) Policy

1.1.9 Publicity

1.2 All projects/research involving the recording of patients (visual and auditory) must be registered with the Trust Research and Development and Information Governance functions.

1.3 Copyright of all such records is held by the Trust.

1.4 Store authorisation, and where relevant, consent - with the image.

1.5 Always log and store negatives, master transparencies, original digital camera files and videotapes appropriately. Do not alter digital images in any way before storage. Take special care to protect the image and maintain its integrity and ensure that the quality of a recording (in terms of resolution, colour depth or volume) is adequate for purpose.

1.6 In order to maintain the integrity of images, manipulation may only be carried out to the whole image and must be limited to simple sharpening, adjustment of contrast and brightness and correction of colour balance.

1.7 The quality of the image must not be compromised when photographing or viewing wound assessments.

1.8 It is good practice for patients to see the images taken of them as a means of confirming their consent to the process.

2.0 Consent

2.1 Health professionals should always ensure that they make clear, in advance, if any photographic or video recording will result from a procedure.

2.2 Photographic and video recordings which are made for treating or assessing a patient, from which the patient might be identified, must not be used for any purpose other than the patient's care or the audit of that care, without the express consent of the patient or a person with a lasting power of attorney for personal welfare or parental responsibility for the patient.

2.3 If you wish to use such a recording for education, publication or research purposes, you must seek consent in writing, ensuring that the person giving consent is fully

Guideline

Information Governance - Use of cameras, video and audio recorders on Trust premises (including the use of smart phone and other mobile devices with recording functionality)

aware of the possible uses of the material. In particular, the person must be made aware that you may not be able to control future use of the material once it has been placed in the public domain.

- 2.4 In the case of children, if a child is not willing for a recording to be used, you must not use it, even if a person with parental responsibility consents.
- 2.5 If you need to take photographs or video recordings of a patient lacking the mental capacity to provide consent, the reason for taking the recording must be in the best interest of the patient and documented. Consent may be obtained from someone who holds a power of attorney for personal welfare. It is always good practice to try and discuss with the patient by any means necessary or the next of kin to explain the rationale for making the recordings.
- 2.6 If you wish to make a photographic, audio or video recording of a patient specifically for education, training, accreditation, supervision, publication or research purposes, you must get their written explicit consent (or where appropriate that of a person with parental responsibility) both to make the recording, and to use it. If a patient lacks the mental capacity to provide consent you must not make, or use, any such recording, if the need could be equally well met by recording patients who are able to give or withhold consent.
- 2.7 If this image is to be held by a third party, i.e., training establishment (University) as part of accreditation of a practitioners competence, then it must be provided in line with information sharing agreements, stored securely and used only for the purpose of accrediting a practitioner's competence. Patient's consent must be obtained and in line with Code of Confidentiality there should be '*no surprises*' as to what is being done with the image and who has access etc.
- 2.8 You must make patients aware that they are free to stop the recording at any time and that they are entitled to view it if they wish, before deciding whether to give consent to its use. If the patient decides that they are not happy for any recording to be used, it must be destroyed or deleted. Consent can be withdrawn at any time and this should be documented.
- 2.9 As with recordings made with therapeutic intent, patients must receive full information on the possible future uses of the recording, including the fact that it may not be possible to withdraw it once it is in the public domain.
- 2.10 In the case of minors, the parent or guardian should sign the consent form for education, publication or research purpose unless the minor reaches the age of 16 or is judged to be capable of consenting in their own right during the course of treatment, when new consent is required. If a child is not willing for a recording to be used it must not be used, even if the person with parental responsibility consents. If the recording is part of clinical treatment then those under 16 cannot refuse if parental consent is given in law.

Guideline

Information Governance - Use of cameras, video and audio recorders on Trust premises (including the use of smart phone and other mobile devices with recording functionality)

- 2.11 Photographic and video recordings, made for treating or assessing a patient, and from which there is no possibility that the patient might be recognised, may be used within the clinical setting for education or research purposes without express consent from the patient, and as long as this policy is well published.
- 2.12 In instances where a recording is to be used for more than one purpose explicit consent must be obtained for each purpose. It must be explained that future consent will be sought if at a later stage there is an intention to use the recording for a different purpose.
- 2.13 In all cases of recording, care must be taken to respect the dignity, ethnicity and religious beliefs of the patient.
- 2.14 A model consent form is contained within the Consent Policy at Appendix 7.

3.0 Non-clinical photography

- 3.1 In cases where the patient is incidental to a recording, e.g. where the picture is to illustrate a particular piece of equipment set-up, consent to appear in the recording is still required from any patient or member of the public.
- 3.2 Avoid accidental recording of patients who have not given appropriate consent.
- 3.3 Photography may be permitted in designated areas of the Trust e.g. Maternity where relations and visitors may be allowed to photograph new born babies. Photography should only be allowed when parental consent is obtained and at the discretion of local staff. The confidentiality, privacy and dignity of other service users, staff and visitors must be maintained.
- 3.4 Images of a patient that inadvertently include an image of another patient or patients who have not consented should not be published under any circumstances. Unless detrimental to the care of the subject patient, they should be destroyed.
- 3.5 Freelance professional photographers may sometimes be employed by the Trust to take non-clinical photographs. They may only be used by prior arrangement with the Head of Communications.
- 3.6 Contracts with outside photographers must ensure that they waive ownership of copyright and moral rights in the recordings they prepare, although they may still be allowed to reproduce the recording or image providing permission has been given from the Trust on each occasion.
- 3.7 External agencies (for example media) are not permitted to take photographs or other recordings on Trust premises unless previous arrangements have been made with the Trust Communications Team; these arrangements must comply with the Trust Media Handling Policy & Guidelines for staff and Governors. Such agencies must be accompanied by a member of Trust staff at all times whilst on the premises. If seen

Guideline

Information Governance - Use of cameras, video and audio recorders on Trust premises (including the use of smart phone and other mobile devices with recording functionality)

unaccompanied and recording they should be challenged by staff and asked to produce written documentation to confirm that they have received authorisation to be on site.

- 3.8 It should be noted that modern cameras and mobile phones can capture detailed information at great distances. Take care that any authorised recording is not allowed to capture patient identifiable information that may be visible e.g., on desks, computer screens and wall/notice boards.

4.0 Authorised recording of meetings

- 4.1 You do not need consent to record meetings such as staff meetings / formal meetings as attendees are not attending the meeting in a personal capacity. However, as a matter of courtesy and good practice make attendees aware that the meeting is being recorded.
- 4.2 You must have consent to record one to one sessions, appraisals, sickness, capability, disciplinary or similar staff meetings as these are personal meetings.

5.0 Recording by service users and members of the public

- 5.1 Occasionally service users or other individuals may ask to record a meeting or clinical session to help them retain information or aid their therapy. Section 36 of the Data Protection Act 1998 allows processing of information to take place for domestic purposes. This means the Trust should consider each request on its own merits to establish if it is appropriate to allow the recording to take place. Service users should be invited to record consultations overtly, not covertly. Ask the service user for a copy of the recording which can then become part of their records. Reassure patients that the recordings will be stored securely and only used for agreed purposes e.g., seeking consent or advising as to treatment options. As appropriate, the Trust should offer to make the recording and give a copy to the individual to ensure the copy is accurate and unadulterated. Individuals must give explicit consent, be advised that the recording is for personal use only and advised that the Trust accept no responsibility for the safekeeping of the copy once it has been handed to the individual. The individual must also be advised that the recording must not be used for litigation purposes. This is not permitted under Section 36 of the Data Protection Act 1998.
- 5.2 It may also be considered inappropriate to allow a recording where references may be made to third parties or where visual interaction would not be apparent, for example in an audio recording.
- 5.3 Advise service users that clinical sessions are fully documented and a written copy can be provided to the service user.

Guideline

Information Governance - Use of cameras, video and audio recorders on Trust premises (including the use of smart phone and other mobile devices with recording functionality)

6.0 Covert recording

6.1 The Trust does not encourage the use of covert recording, unless supported by an appropriate authority made out under the Regulation of Investigatory Powers Act 2000 (RIPA). You need this authority to be obtained either in pursuance of a Police led investigation or NHS Protect in the interests of investigating and/or preventing crime e.g., abuse, violence, aggression, systematic theft, fraud and any other criminal or anti-social activity including terrorism, due to the potential to breach the right of individuals to privacy as described in the Human Rights Act.

7.0 Management action in relation to unauthorised recordings

7.1 Under no circumstances should you, as an employee of the Trust, engage in covert recording. You must get permission (in all instances) where it is intended to record. Do not make recordings if you do not have permission.

7.2 If a member of staff is identified as having made an unauthorised recording, then this will be dealt with via the Trust Disciplinary Policy and Procedure (unless it is of a criminal nature, in which case the police should be involved).

7.3 Where photographs or video / audio footage have been taken of a member of staff without their prior consent, staff should be advised of avenues for reprisal that are open to them. This may include instigation of civil proceedings or discussions with their staff association.

7.4 If a service user or other visitor to Trust premises is found to be making a recording without the permission of the Trust, the individual should be advised this may contravene the right to confidentiality of any individuals being recorded and is against Trust policy.

7.5 Any visitor observed making an unauthorised recording of other individuals on Trust premises should be asked to leave. A refusal to leave could result in police involvement.

7.6 If the making of a covert recording, from which individuals can be identified, is discovered after the recording has been made and if it has already been published (for example on Facebook, YouTube) the maker should be requested to immediately remove the recording and notify the Trust when it has been done.

Guideline

Information Governance - Use of cameras, video and audio recorders on Trust premises (including the use of smart phone and other mobile devices with recording functionality)

8.0 Security and storage of recordings

- 8.1 Store recordings securely on a Trust server. Do not store data in a cloud environment such as iCloud , OneDrive, Dropbox, Google Drive and Box (even as a back-up) nor on a standalone device where it is only possible to store data locally.
- 8.2 Recordings may be required to be disclosed under the Data Protection Act or Access to Health Records Act.
- 8.3 Recordings may be held temporarily on Trust owned devices before being uploaded to a secure area of the network or onto one of the approved information assets (e.g., PACS). Ideally, all digital images should be uploaded immediately where possible and deleted from the recording device to prevent any loss of personal data and security incidents. All recordings must be transferred from the device either at the end of each day or immediately upon return to base (if recorded off site e.g., in the patient's home).
- 8.4 Once the data has been transferred to the Trust network device all traces of the data should be immediately removed from the source device.
- 8.5 Personally owned devices, e.g., mobile phones, personal digital cameras, MP3 players, must never be used to take or store images or other recordings.
- 8.6 Data in transit on removable media must be encrypted, handled and stored appropriately and afforded the utmost security and protection at all times.
- 8.7 Any image or recording must be named with the NHS Number of the subject patient. In addition, the patient's name, date of birth and the date the image or recording was made should be recorded. Each image should be assigned a file name by which it can clearly be identified.
- 8.8 Always ensure that recording devices are stored securely when not in use or when taken away from Trust premises and remain vigilant at all times regarding the security and handling of equipment.

Implications of not following the guidance:

Images or recordings may be:

- Destroyed in error
- Inappropriately shared
- Inappropriately disclosed into the public domain e.g. via social media, or file sharing platforms

Useful Contacts:

Beverley Adams-Reynolds

Information Governance Manager

Ext 3210

Guideline

Information Governance - Use of cameras, video and audio recorders on Trust premises (including the use of smart phone and other mobile devices with recording functionality)

Monitoring the Process:

Document review on year one and every three years thereafter unless subject to legislative or changes on best practice.

National Definitions:

Recordings	Music, sounds, or images that have been stored on a record, CD, computer, memory stick, removable data memory cards, etc., so that they can be heard or seen again
Confidentiality	The ethical principle or legal right that an individual will hold secret all information relating to another, unless given consent permitting disclosure
Clinical photography or video	Using stills photography or video equipment to record the outward signs of a patient's condition; or a medical or surgical procedure being applied to a patient
Images	These include both visual (static or moving) and auditory
Analogue	Information is translated into electric pulses
Digital	Information is translated into binary format (zero or one).
Informed consent	A full understanding of the options and implications of decision being made
Copyright	The legal right that grants the creator of an original work exclusive rights to its use and distribution
Information asset	Any data, device, or other component of the environment that supports information-related activities
Information asset owner	A named individual responsible for information assets within a defined area.
Authorised recordings	Recordings made with explicit consent of the Trust or individuals as applicable to the circumstances
Covert recordings	Recording of a location, or the movements or activities of an individual or group where there is no knowledge that the recording may be taking place
Caldicott Guardian	The person with overall responsibility for protecting the confidentiality of person identifiable data.
Senior Information Risk Owner	The person with allocated lead responsibility for the Trust's information risks and provides a focus for the management of information risk at Board level

Guideline

Information Governance - Use of cameras, video and audio recorders on Trust premises (including the use of smart phone and other mobile devices with recording functionality)

Information Governance Manager	The person with responsibility for regulating the use and security of personal information
--------------------------------	--

Reference Material & Associated Documents:

Information Governance Policy - POLCGR017

Information Governance Framework - OTCGR141

Information Governance Strategy - STRCGR013

Information Governance Guidance - Fax - Email - Internet – Telephone - GUCGR022

Document History

Edition No	Reason for change
1	New policy created to ensure that patient information and images remain confidential and to assist with assessment and evaluation of patients conditions though the use of clinical photography. To reduce risks associated with use of cameras.
2	Review and updated into guidance document (archive POLCGR126)

Approval Signatures:

Revision No:	1	ID No:	GUCGR023
Distribution:	Intranet / Q-Pulse		
Date Approved:	September 2016		
Approved By:	Information Governance Group		
Review date:	September 2019		
Author:	Information Governance Manager - Beverley Adams-Reynolds		
Document Owner:	Director of Corporate Governance, Risk, Compliance & Legal - Lynne Stuart		