South East Coast Ambulance Service NHS
NHS Foundation Trust

Patient Photographic and Video Recording Policy

Use of cameras, video and audio recorders (including the use of smart phone and other mobile devices with recording functionality)

Contents

1. Introduction

1.1. South East Coast Ambulance Service NHS Foundation Trust (the Trust) is committed to upholding and maintaining the privacy and confidentiality of its service users. Confidentiality does not only apply to information in written form but also extends to that stored on other media. With the developments in technology over recent years (such as smart phones and other devices which are able to record either audio or visual material, or both), safeguarding the privacy, cultural beliefs and confidentiality of service users is of paramount importance. From here-on, the term "image" relates to any media (i.e. stills or video images, etc). Where the image has been captured on a Trust issued and managed body warn video device this is managed under a separate policy.

1.2. Technological advances in digital photography over recent years have been accompanied by an increase in legislation and guidance covering the security and confidentiality of identifiable information. The Human Rights Act, United Kingdom General Data Protection Regulation (UK GDPR) and Data Protection Act 2018 are all concerned with an individual's right to dignity and privacy. Annual completion of the Data Security & Protection Toolkit provides assurance that the Trust is compliant with its data protection obligations.

1.3. Key elements of this legislation and guidance underline the requirement for patients to be fully informed and give explicit consent where possible, of any record being made of them, including images, together with their intended use, particularly where this may extend beyond the patient care record such as inclusion in personal logbooks, Continued Professional Development (CPD), teaching or publication.

1.4. Additionally, the Confidentiality NHS Code of Practice was issued by the Department of Health in November 2003 and the Confidentiality Policy issued by NHS England and NHS Improvement in September 2019 act as a guide to NHS staff regarding confidentiality and patients' consent to the use of their health records.

1.5. The Confidentiality Code of Practice, Glossary of Terms, states that patient identifiable Information is as follows: Pictures, photographs, videos, audio-tapes or other images of patients.

1.6. A copy of the code of practice and NHS Confidentilaty policy can be found from the following links:

1.7. http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

1.8. https://www.england.nhs.uk/wp-content/uploads/2019/10/confidentiality-policy-v5.1.pdf

1.9. Under Article 15 of the UK GDPR and Data Protection Act 2018 is the data subject access provision, under which a patient or their designated representative (e.g. solicitor) can request copies of their health records, including images. It is therefore essential that any image taken by clinicians from South East Coast Ambulance Service NHS Trust (the Trust) is accessible in order that a copy can be produced for this purpose.

1.10. Any information sharing relating to clinical images or patient data, outside of the provision for direct clinical care must have an agreed legal basis. For example there must be a formal information/data sharing agreement in place to allow for recipients to act as a data processor and receive this information. All agreements will require review by the Head of Information Governance with approval sought by the Caldicott Guardian and SIRO.

1.11. A Trust Patient Photographic and Video Recording Policy is therefore required in order to take account of the above issues and set out clear procedures to ensure that both the Trust and its staff comply with the requirements of appropriate legislation.

1.12. This policy is intended to ensure the protection of both the rights of the patient and the position of the Trust and its staff with regard to appropriate legislation and is thus intended to be helpful rather than restrictive.

2. Responsibilities

2.1. All Trust employees and anyone working for the organisation (e.g., agency staff, honorary contracts, management consultants, voluneteers, etc.) who use and have access to Trust premises and information must understand their personal responsibilities for information governance and comply with UK law.

2.2. All staff with access to confidential information have an individual responsibility and duty to keep that information safe and secure. They must comply with Trust policies, procedures and guidance and attend/complete relevant education and training events in relation to Information Governance annually or as required by the Trust.

3. Aims and Objectives

3.1. Recording of images is a valuable part of assessing and evidencing a patient’s condition, this includes the provision to:

- Provide information on the legal requirements regarding clinical image capture and processing.

- Implement best practices within the Trust involving clinical image capture and processing in line with existing principles and legislation, such as Caldicott Principles, Common Law Duty of Confidentiality, Data Protection Act 2018 and the UK GDPR.

- Provide a framework for when clinical imagery capture and processing can be used and to comply with legislation surrounding clinical imagry.

- Provide assurance that the Trust is compliant with legislation.

- Ensure Patient confidentiality is maintained at all times.

4. Definitions

4.1. **Clinical photography**: The taking of images with respect of the patients condition or injury to record a visual representation of that condition/injury to be viewed by other health professionals.

4.2. **Clinical videography**: As above, but using video recording, instead of still photography.

4.3. **Incident Images**: Any image or video that is captured or processed which relates to the incident, scene, people, documents, animate or inanimate objects with any correlation to the Trusts response or attendance.

4.4. **PCR**: the Patient Clinical Record.

4.5. **ePCR**: Electronic Patient Clinical Record

5. Policy Statement

5.1. Risk management is the responsibility of all Trust staff. Where appropriate, risks and issues will be recorded on the Trust's Risk Register.

6. Arrangements

6.1. Personally owned devices, e.g., mobile phones, personal digital cameras, MP3 players, must never be used to take or store images or other recordings.

6.2. Staff must ensure that image 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. This includes Trust issued mobile phones and iPads/Tablet devices.

6.3. SECAmb will remain the data controller for any Images taken. Where the image contains the patient, patient identifiable information or clinical information this forms part of the patients clinical record which is managed by the Trust on the patients behalf. Where the image is included in an electronic record or is taken explicitly for transmission to another care facility for the provision of direct patient care, the Trust remains responsible for its secure transmission including where it is stored on Trust devices.

6.4. Images 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., ePCR) where this is not an automated process.

6.5. Ideally, all digital images should be uploaded immediately where possible and deleted from the recording device to prevent any loss of personal data and data 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).

6.6. As at July 2021 the current ePCR application only accepts images directly inserted into the clinical records through an approved secure process.

6.7. This section applies where the image is not securely and automatically applied to the patient record or approved Trust system such as the ePCR.

6.8. Once the data has been transferred all traces of the data must be immediately removed from the source device where this is not managed by an automated process. Images must only be held on portable devices for the least amount of time as possible to ensure safe transfer. If staff are using the cut/copy and paste function for this process it is their responsibility to ensure that the image is only copied/pasted to the correct destination.

6.9. The Trust will store images on Trust approved infrastructure / servers and should never be stored on a stand alone device such as a USB memory stick. If there are any concerns regarding how this section is to be applied then the Trust IT and IG departments must be contacted for specialist advice and guidance at the earliest opportunity.

6.10. Images originating from Trust devices must not be used for training or Publication without the principles of section 1.3 being applied. All

arrangements with other providers to receive images must be made with this point in mind.

6.11. Images may be required to be disclosed under the Data Protection legislation or Access to Health Records Act 1990.

6.12. Where images are being managed by a data processor, they must be removed from Trust devices once the receiving organisation has confirmed receipt of any images and stored appropriately.

7. Photographs taken within the Trust.

7.1. The Trust position is that images taken of the patient or incident must only take place where there is a significant value add to the ongoing care of the patient, and where the details being captured are unable to be documented in words. The Trust mandate is to provide direct care not gather evidence for any other purposes.

7.2. The Trust recognises that section 7.1 is not always appropriate or relevant and there may be exceptions to this rule. Where the responding clinician believes that the image is relevant to the situation or incident attended, and there are no other suitable means for capturing this data, an image may be captured but with due regard to the image content and its relevance.

7.3. The clinician must take into account the wishes of the patient, others on scene (related to the case) and the purposes of processing this image(s). It is the ultimate responsibility of the person taking the image to be able to justify the legal basis for doing so.

7.4. Images Taken of Patients at the Scene Under no circumstances, should clinical photographs be taken on mobile phones (regardless of Trust or private ownership).

7.5. If an image is deemed relevant to the ongoing care of the patient, and the details cannot be clearly recorded in text, this image must be included in the patients clinical record (ePCR or PCR).

7.6. Where an image can be included this must be directly taken through the Trust approved ePCR software so that it is not stored on the device Image storage locations.

7.7. This is the most appropriate way for inclusion into the patient care record and is a Trust approved process.

7.8. Devices used to take images can be seized by the Police as evidence.

7.9. For the purpose of section 8.1.1 the Trust position that images that would be deemed relevant would be in line with the following examples:

7.10. This list is not exhaustive and used for illustration purposes only:

7.11. An image that shows exceptional circumstances relating to the patients care, social circumstances or living arrangements that directly demonstrates an important factor in the ongoing care of this patient.

7.12. An image of a document or care plan that can be directly related to the ongoing care of the patient such as plans not for resuscitation and Respect plans.

7.13. Where the photo contains a identifiable marks, scars, tatoos, face of the patient these must only be included in exceptional circumstances not as a standard practice.

7.14. Under no circumstances should photos of a deceased patient be taken. This aligns with EOLC Procedures

7.15. Staff intending to take photographs that are (or could be) capable of being linked to a patient, must seek where appropriate, explicit informed consent for the images to be taken. The patient's decision must be recorded on the PCR or ePCR.

7.16. The uploading of photos (mainly of babies) to social media is not acceptable.

7.17. The Trust will retain clinical images. These will form part of the patients clinical care record and must never be retained by individuals.

7.18. Images must only be taken and shared as part of direct care, and in accordance with data protection legislaton and Caldicott principles.

7.19. Currently the Trust does not have any approved process for attaching images into a paper completed record once it is transferred into an electronic version. Due to this images are only to be taken where they can be included through an approved process such as ePCR or ultra sound scan etc.

7.20. Further details relating to the UK GDPR and Data Protection Act can be found on the Information Commissioner's Office website, which can be accessed via the following link: http://www.ico.gov.uk

7.21. The Human Rights Act, UK GDPR and Data Protection Act are all concerned with a patient's right to dignity and privacy. See Section 1.2

7.22. The use of photographic material for any non-therapeutic purposes without the patient's express consent is a breach of this legislation.

7.23. Further information on the Human Rights Act can be found from the following link: http://www.dca.gov.uk/hract/hramenu.htm

7.24. When seeking agreement to take clinical photographs, clinicians must consider patient's capacity with reference to the Mental Capacity Act (2005).

8. Clinical Research

8.1. Images must not be used for training, publication or research unless they have been taken for this explicit reason and with explicit informed consent documented. Any plan to incorporate images into research must have this specifically identified in the Data Protection Impact Assessment (DPIA) with the associated governance completed.

8.2. Whilst the principles of patient consent continue to apply, the recording and management of such images in respect of patients photographed for use within the Trust, or for passing to approved agencies, will be the responsibility of the Medical Director under the auspices of their role as Caldicott Guardian.

8.3. All procedures, protocols or pathway information involving images must reference this policy.

9. Underlying Principles

9.1. All images of patients regardless of format or recording medium form part of the patient record (either physical or electronic) and are therefore subject to the same security and confidentiality considerations as any other medical record, and must only be used in relation to the care of the patient.

9.2. Patients must always be informed of the intended use to be made of any photograph taken of them.

9.3. Where patients lack the capacity to give consent, the same mechanism must be applied within the guidance of the Mental Capacity Act 2005.

9.4. **Photographs taken within the Trust must be:**

- Stored securely internally or passed to a secure data processing facility.

- Removed permanently from the device used to take the image. The removal must be according to any prescribed procedure as part of specific approved pathways.

- Digital photographs can only be taken with equipment owned by the Trust or explicitly approved by the Medical Director or Consultant Paramedic. Specific guidance for photography of incident scenes which do not involve patients.

9.4.1. It is recognised that there is value in capturing images of the scene of incidents, such as road traffic collisions, in order to give the receiving clinicians an impression of the damage to vehicles or mechanism of injury.

9.4.2. These kinds of images are not considered to be clinical photographs as long as the identity of the patient is not compromised in any way. Staff must consider meta data captured, including GPS locations, when evaluating if patient identity may be compromised. Staff must still only use Trust approved devices to take these kinds of images and must delete/destroy images after the incident is complete.

9.4.3. No images arising from the Trust will be considered for training purposes at the present time. Where the image is needed for any purpose other than direct patient care requires explicit consent to be obtained at the time the image was captured or at a later date.

9.5. **Encryption**

9.5.1. The NHS is required to ensure that any identifiable information being transferred from an NHS organisation is encrypted. Any images which require transmission must be encrypted and sent via a N3 connection.

9.6. **Covert recording**

9.6.1. 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).

9.6.2. Such 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.

10. Responsibilities

10.1. The Medical Director has overall Executive responsibility, as Caldicott Guardian, for clinical photography.

10.2. The Head of Information Governance in conjunction with clinical stakeholders is responsible for this policy.

10.3. The Senior Operational Managers, Clinical Operations Managers and Clinical Team Leaders are responsible for the implementation and monitoring of this policy.

11. Competence

11.1. Any member of staff involved in clinical photography must have received training and education commensurate to the requirement of the equipment or system being used.

12. Monitoring

12.1. The Head of Information Governance is responsible for monitoring compliance with this policy. This policy will be reviewed by the Information Governance Working Group and the Clinical Governance Group.

12.2. The Medical Directorate Director will be responsible for ensuring adherence to the policy. Non-compliance or deviation from this policy that results in an adverse outcome for a patient will be dealt with in accordance with the Incident Reporting Policy (Datix) Procedure and actioned accordingly.

13. Audit and Review

13.1. The policy document will be reviewed every three years; or earlier if required due to change in local/ national guidance and/ or policy; or as a result of an incident that requires a change in practice.

12. Equality Impact Appraisal

12.1. The Trust has undertaken an equality impact appraisal to identify the impact the policy may have on disparate groups. There are no indications that this document will adversely affect any particular group, on the basis of age, gender, religion, race, ethnic origins, nationality, disability or sexual orientation.

14. References

- Data Protection Act 2018
- UK General Data Protection Regulation (UK GDPR)
- Common Law Duty of Confidentiality
- NHS Records Management Code of Practice 2021
- Human Rights Act 1998
- Mental Capacity Act 2005
- Computer Misuse Act 1990
- Freedom of Information Act 2000
- Confidentiality: NHS Code of Practice, DH, 2003
- Confidentiality: NHS Code of Practice - supplementary guidance: public interest disclosures, DH, Nov 2010
- Information Security Management: NHS Code of Practice, DH 2007
- Confidentiality, including Caldicott principles.
- HPC standards of proficiency for paramedic

15. APPENDIX ONE

Patient Photographic & Video Recording Policy

Use of cameras, video and audio recorders (including the use of smart phone and other mobile devices with recording functionality)

Do's and Don'ts

Do	Do not
Ensure you have the appropriate consent or authorisation; • Document and file recordings appropriately. • Use the correct device (Trust issued) • Ensure that this is added to the patient record	Record without consent or authorisation; • Record covertly. • Use a personal device • Share inappropriately

16. APPENDIX TWO

DEFINITIONS:

Recordings	Music, sounds, or images that have been stored on a 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
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 a 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
Data Protection Officer	The person with responsibility for regulating the use and security of personal information and adherence to Data Protection legislation