South Central Ambulance Service NHS
NHS Foundation Trust

CLINICAL SERVICES POLICY & PROCEDURE (CSPP No. 25)

Clinical Photography Policy in the Pre-Hospital Setting

January 2017

DOCUMENT INFORMATION	
Author: Mark Ainsworth-Smith Consultant in Pre-hospital Care Acknowledgment to. Dr Pamela Chrispin, Medical Director, East of England Ambulance Service **Reviewed: January 2017**	**Consultation & Approval:** Staff Consultation Process: (21 days) ends: Governance Committee: 12th March 2015 Board Ratification: N/A
This document replaces:	**Notification of Policy / Strategy Release:** All Recipients e-mail: Staff Notice Boards – Intranet:
Date of Issue:	March 2017
Next Review:	March 2019
Version:	1.1

CONTENTS **Page**

APPENDICES

CLINICAL PHOTOGRAPHY IN THE PRE-HOSPITAL SETTING POLICY AND PROCEDURES

1. Introduction

Clinical photography can contribute essential information to patient care. For individual patients an image may act as a valuable record of their condition and response to treatment. For healthcare professionals, clinical images are a key tool in training and education.

Images must only be used to benefit patients and there is a need to protect patient safety, dignity and confidentiality. Legislation covering the recording and management of identifiable information includes the Data Protection Act (1998), the Human Rights Act (1998), the recommendations of the Caldicott committee issued with HSC (99) 012 and the Information Governance Toolkit, which was implemented in the early part of 2004.

Images in this context include identifiable information such as photographs, audiotapes, video recordings, scanned or electronically captured records. Images of incident scenes and injuries are also included. Images used for publicity or other purposes should adhere to these general principles.

Use of social networking sites are covered by a separate policy but in general no patient-identifiable information should be placed in the public domain without explicit, valid consent from the patient.

2. Purpose

The purpose of this framework is to give guidance to staff or volunteers working for or on behalf of ambulance services to ensure they act in the best interests of the patient at all times, and are compliant with the law.

3. Principles

- Patients should, where possible, give specific consent for images or recordings to be taken, including the intended use and storage arrangements

- Recordings must only be made, transferred, stored and used when they will benefit patients, either directly or when the education of healthcare workers, other staff or the public will provide better care for future patients

- Images should normally be captured on Trust approved equipment only. In an emergency, other equipment may be used however particular care should be taken to ensure transfer, storage and use of such images is in strict accordance with Caldicott principles (Appendix A)

- The Trust does not condone the use of the use of non-Trust devices. There are many unresolved issues regarding staff using their own devices i.e. cloud storage, secure transmission, deletion / retention of information.

- Images should be processed and stored safely to prevent accidental loss, unauthorised viewing or damage in accordance with the Data Protection Act and Caldicott principles, on a secure NHS server or other secure server approved by the Trust

- Electronic transfer of images should be via a secure medium and ideally via a secure NHS portal

- Images should be destroyed once they are no longer of use and should never be stored in a way which does not fulfil NHS data protection and Caldicott criteria

Key elements of the legislation and guidance underline the requirement for patients to be fully informed of photographic (or indeed any) records being made of them, together with their intended use, particularly where this may extend beyond the patient record such as inclusion in personal logbooks or use for teaching or publication. The underlying legislation goes on to emphasise the requirement for patients to give their consent for photographic (and other) information on them to be recorded having been fully informed of the intended use. A document entitled "Good Practice in Consent Implementation Guide" was issued by the Department of Health (DH) in November 2001. The guidance within this document includes a specific section on "Clinical Photography and Conventional or Digital Video Recording".

The Confidentiality NHS Code of Practice was issued by the DH in November 2003 as a guide to NHS staff regarding confidentiality and patients' consent to the use of their health records. This document states explicitly that pictures, photographs, video, audio-tapes or other images of patients are deemed to be key identifiable information items. A copy of the code of practice can be found from the following link: http://www.dh.gov.uk/en/Publicationsandstatistics/Publications/PublicationsPolicyAndGuidance/DH_4069253

A key element of the Data Protection Act 1998 is the subject access provision, under which a patient or their designated representative (e.g. solicitor) can request copies of their health records, including photographs or other images. It is therefore essential that any image taken by clinicians is accessible in order that a copy can be produced for this purpose. Therefore, any agreements to pass on clinical images must include the agreement to provide copies on request, by means of a formal agreement for recipients to act as a data processor.

4. Taking Clinical Images

Clinical images should only be taken when they are necessary for treating or assessing a patient. Each image and image content which provides patient-identifiable information must be justifiable, and 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 parental responsibility for the patient. Patients must be informed about the intended use of any images taken for assessment or treatment. Staff need only give a verbal explanation and where consent is given this should be recorded in the PCR or ePR record.

Although it is best practice to inform the patient at the time of the image being taken, this may not be possible. In this case the patient should be informed at the earliest opportunity that an image has been taken. The image may not be used for any other purpose unless written permission is obtained from the patient, and no additional copies may be kept.

When seeking agreement to take clinical images, the patient's capacity to consent must be considered in line with the Mental Capacity Act (2005) and the Trust's Consent and Capacity Policy. If a patient dies before consent can be obtained, images where the patient is identifiable can only be released with the consent of the deceased's personal representative.

Some images containing patient-identifiable information may be intended for purposes other than direct clinical benefit (for instance for training purposes or publicity material). Under these circumstances specific consent must be taken with particular attention made to ensuring the patient understands the purpose behind the recording and the use to which it will be put. For non-identifiable imagery, the DH guidance states that "photographic and video recordings made for treating or assessing a patient and from which there is no possibility that the patient may be recognised may be used within the clinical setting for education or research purposes without express consent from the patient, as long as this policy is well publicised. However, express consent must be sought for any form of publication."

Equipment - Clinical images or recordings should be captured using equipment owned by or specifically approved by the Trust. ePR devices are recommended by the Trust as being the most secure equipment available to staff. If no authorised device is available then staff may use Trust owned mobile phones to take clinical or scene management images. These should be emailed via a secure server as soon as is practical. The PCR or ePR should be marked to show that an image or recording was taken and stored; the image should be deleted once emailed.

Scene photography - 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. These kinds of images are not considered to be clinical images as long as the identity of the patient is not compromised.

5. Transfer of Clinical Images

Captured images will need to be transferred to a secure storage facility. For electronic images this will usually be via direct download onto a secure server. Images should only be transmitted from the camera or other recording device where they provide ongoing benefit to the patient. Transmission should be via a secure method and preferably by NHS mail or other secure NHS route. All staff have a duty to ensure transmission of images minimises the risk of the image being disseminated inappropriately or in a way which compromises patient confidentiality, dignity or safety.

Images used for education and training purposes should ensure patient confidentiality where possible and should not be used in a way which allows free dissemination or patient identification, either directly or by triangulating with other available information (such as incident date, location, circumstances etc.).

Telemedicine – Remote advice is increasingly used to support clinical decision-making in a pre-hospital environment. Capture, transmission and storage of images should comply with the principles above, with particular attention paid to not breaching patient confidentiality during live transmission, especially in circumstances where conversations may be overheard or recording devices are present, including Press and TV crews.

6. Storage and Retention of Clinical Images

Unless explicit consent is gained for other forms of use, clinical images regardless of format or recording medium form part of the patient care record and therefore should be treated with the same levels of security and confidentiality as any other medical record, and must only be used in relation to the care of the patient. Access to images must be in accordance with data protection and Caldicott principles (Appendix A).

All images should be retained as per the relevant retention schedule in the Records Management Policy.

To ensure an effective audit trail, all images must be stored as soon as is practical with the relevant job number on Trust approved premises or computer systems, or with a Trust approved third party. Where possible digital images should be stored in their original format without manipulation to preserve their integrity.

All personal data associated with images taken by the Trust must be kept so that it conforms to the standard stipulated by the Data Protection Act 1998 (Appendix B).

7. Release of Images and Recordings

Any request for release of patient-identifiable information should normally be made in writing, and release approved only by the Caldicott Guardian or Information Governance Manager unless there are agreed processes in place, such as release of records to a Coroner. If there are any concerns about the process then the matter should be referred to the Caldicott Guardian prior to release. This is in line with the Data Protection and Confidentiality policies.

Copies of any images may be requested by the patient or on their behalf by a solicitor. Again release may only be approved by the Caldicott Guardian or Information Governance Manager.

There may be extreme circumstances (such as an incident in which a criminal act is captured on the image) in which there is an overwhelming public interest in breaching patient confidentiality. Under these circumstances specific permission should be sought from the Caldicott Guardian before transmitting or using such images for any purpose other than direct patient benefit.

8. Destruction

All images no longer required must be destroyed in a timely and secure manner in compliance with the Records Management Policy. These are not the property of individual staff.

9. Hazardous Area Response Team

As part of the national HART capability both video and still imagery is supplied to ensure advanced telemedicine can occur to those trapped within both a hazardous or confined space. The video element can be transmitted from the operator and reviewed on the Command Vehicle video screens or beamed via satellite to a secure viewing platform for Scene Commanders or Medical Advisors to review.

Video
The video from both body cameras and from the vehicle camera is all recorded on the back-office solution computers; when back at the HART base the video is downloaded onto a secure server where it will then be automatically backed up to the SCAS secondary secure server. .

Still images
These may be taken of both the scene and the patients; although the Command Vehicle has the ability to download and print the photos it maybe that the camera does not return from the hazardous area in time for this to be completed prior to the patient being conveyed to hospital.

Still images are not formally backed up by the Command Vehicle automatically and as such any images taken by the still camera would be forwarded for storing in line with this Policy.

Remit of HART video and still photography

The remit of the HART Command Vehicle's video and still photographic capability is to ensure detailed telemedicine and scene management can be completed in a safe and appropriate environment.

The video may well be viewed during the rescue operation by multi agency colleagues and as such it must be accepted that as part of the scene management process patient identifiable images may be captured without their immediate consent.

10. Breaches of Policy

Loss of patient-identifiable information must be notified immediately to the Caldicott Guardian and Information Governance Manager. It should be investigated and reported in line with the Incident Management Policy and if necessary be reported and managed as a Serious Incident. The HSCIC "Information Governance and Cyber Security Serious Incidents Requiring Investigation" matrix must be utilise to determine whetehr an incident is reportable to the Information Commissioner's Office and the department of Health.

Anyone found to be acting contrary to this policy will be investigated by the Trust and / or partner organisation and, if necessary, disciplinary proceedings will be undertaken.

This policy should be monitored and managed to ensure compliance.

References / Associated Documents

- Data Protection Act 1998
- Human Rights Act 1998
- Mental Capacity Act 2005
- Good Practice in Consent Implementation Guide - Department of Health, November 2001
- Confidentiality NHS Code of Practice – Department of Health, November 2003

Appendix A

Caldicott Principles

1. **Justify the purpose**
   Every proposed use or transfer of patient-identifiable information within or from an organisation should be clearly defined and scrutinised, with continuing uses regularly reviewed by an appropriate guardian

2. **Don't use patient-identifiable information unless it is absolutely necessary**
   Patient-identifiable items should not be used unless there is no alternative

3. **Use the minimum necessary patient-identifiable information**
   Where use of patient-identifiable information is considered to be essential, each individual item of information should be justified with the aim of reducing identifiability

4. **Access to patient-identifiable information should be on a strict need-to-know basis**
   Only those individuals who need access to patient-identifiable information should have access to it, and they should only have access to those items that they need to see

5. **Everyone should be aware of their responsibilities**
   Action should be taken to ensure that those handling patient-identifiable information, clinical and non-clinical staff, are aware of their responsibilities and obligations to respect patient confidentiality

6. **Understand and comply with the law**
   Every use of patient-identifiable information must be lawful. Someone in each organisation should be responsible for ensuring that the organisation complies with legal requirements.

7. **The duty to share information can be as important as the duty to protect patient confidentiality**
   Health and Social Care professionals should have the confidence to share information in the best interests of their patients within the framework set out by these principles. They should be supported by the policies of their employers, regulators and professional bodies.

Appendix B

Data Protection Act Principles

1. **Processed fairly and lawfully**
   Inform data subjects why you are collecting their information, what you are going to do with it, and who you may share it with. Information recorded as part of the process of providing care should not be used for purposes that are unrelated to that care.

2. **Processed for a specified purpose**
   Only use personal information for the purpose for which it was obtained, and only share information outside the organisation, team, department, or service if you are certain it is appropriate and necessary to do so.

3. **Adequate, relevant and not excessive**
   Only collect and keep the information you need. You cannot hold information unless you know how it will be used and its use is justified.

4. **Accurate and kept up-to-date**
   Make sure you check with data subjects that the information held is accurate and up-to-date.

   Check existing records thoroughly before creating new records and avoid creating duplicate records.

5. **Not kept for longer than necessary**
   Follow retention guidelines set out by the Records Management NHS Code of Practice. Dispose of information correctly and securely.

6. **Processed in accordance with the rights of data subjects**
   Individuals have several rights under the Act, including:
   - the right of access to personal data held about them
   - the right to prevent processing likely to cause damage or distress
   - the right to have inaccurate data about them corrected, blocked or erased.

7. **Protected by appropriate security**
   Organisations that process personal information must have security measures in place to ensure that the information is protected from accidental or deliberate loss, damage or destruction.

8. **Not transferred outside the EEA without adequate protection**
   If sending personal information outside the European Economic Area (EEA), make sure consent is obtained where required and ensure the information is adequately protected.