Royal College of Paediatrics and Child Health
Association of Chief Police Officers
Faculty of Forensic and Legal Medicine
Guidelines

Guidance for best practice for the management of intimate images that may become evidence in court

Background

1. Concern has been expressed about the possibility of inappropriate disclosure and use of intimate images obtained during the forensic medical examination of complainants of sexual violence or abuse. This guidance is intended to create an agreed practice and disclosure framework in order to reassure practitioners and complainants. This guidance applies to all intimate forensic medical examinations. Clinicians should be aware that images taken during a medical examination, forensic or otherwise, may become evidence in court.

2. The guidance applies to the management of intimate images within clinical practice and all jurisdictions including criminal, family and civil justice systems. The object of the guidance is to ensure respect for the privacy of the subjects of the intimate images and to eliminate the risk of the improper distribution of the images.

Definition

3. An 'intimate image', for the purposes of this guidance, is a photographic, digital or video/DVD image of the genitalia, anus and/or breast obtained using a colposcope or similar suitable and recommended technology. These images may be taken during the course of clinical practice or an investigation into alleged or suspected sexual or physical abuse.

Procedure

4. Before an intimate image has been taken of a child or adult, the following procedure shall apply[1]:

   a) Informed consent of the complainant and/or person/authority who holds parental responsibility for the child will be obtained and recorded. For a non-competent adult the current guidance[2] issued by the FFLM will be followed. Young people under 18 with capacity may consent alone.

   b) In obtaining consent, the complainant and/or person acting on their behalf must be advised that the images are diagnostic for clinical needs and forensic tools and, consequently, they might be shown to other medical experts including experts instructed on behalf of a defendant. Exceptionally, they may be shown to a court (but subject to paragraph 10 below)

   c) If the complainant or person acting on their behalf refuses permission for intimate images to be obtained this must be respected and recorded in the notes.

   d) It should be explained that they will be used in peer review. Specific consent should be obtained for the images to be used for medical education and training.

   e) All the images will be coded and securely stored, or securely stored with password protection according to local protocols, policies and procedures[2] in order to protect anonymity. Secure fall-back arrangements should be in place in case they are needed in the absence of the original coder, including cross-referencing in the notes. Images of faces must **never** be included in order to protect anonymity.

   f) Intimate images are retained as part of the medical record.

[1] Guidance on Paediatric Forensic Examinations in Relation to Possible Child Sexual Abuse RCPCH and FFLM (available at http://www.rcpch.ac.uk and http://fflm.ac.uk).
[2] Consent from patients who may have been seriously assaulted (available at http://fflm.ac.uk)

Statement/Court report

5. The doctor must state in the statement or court report if the examination has been photo-documented and intimate images produced.
6. The findings will be described and interpreted in writing, stating what evidence is contained within the photo documentation. Line drawings should be undertaken in contemporaneous notes.
7. The quality of the images must be referred to and whether they truly represent the clinical findings.
8. Images must **not** be attached to the statement or report.

Disclosure

9. Doctors conducting forensic examinations are 'third parties' for the purposes of the Criminal Procedure and Investigations Act (CPIA) 1996.
10. Doctors do not have an obligation to disclose intimate images to non-medical professionals and should not unless they have appropriate[3] informed consent, or they are ordered to by a Judge, or there is a public interest[4].
11. A doctor can and should refuse to allow inspection of the intimate image by a non-medical professional, the prosecution or defence may seek a witness summons under either section 2 of the Criminal Procedure (Attendance of Witnesses) Act 1965 or section 97 of the Magistrates' Court 1980.
12. Doctors must be aware that if the intimate images or copies of such images (as opposed to a report which refers to these images) are handed to the police or prosecution, then the decision to disclose them further falls to the prosecutor as the images are no longer third party material. **Therefore, doctors should not hand over intimate images or copies of images to the police or prosecutor without appropriate[2] informed consent or a court order.**
13. If the intimate images are inspected or held by the prosecution, and it is the decision of the prosecutor that the relevant test for disclosure is satisfied, the examiner or doctor must be notified of the decision. Consideration will need to be given as to how the complainant is informed of the disclosure.

[3] If the validity of the consent is in doubt the doctor should discuss the case with a Designated Doctor and/or his/her MDO.

[4] Consent: Patients and Doctors Making Decisions Together, GMC. 2008. 0 – 18 years: guidance for all doctors, GMC. 2007.

Examination/review by defence experts

14. The defence may apply for their medical expert to inspect the intimate images. Arrangements will be made to allow the medical expert to view the intimate images at an agreed venue, e.g. Sexual Assault Referral Centre (SARC) or hospital.
15. Exceptionally, if it is not possible for the medical expert to view the photo documentation at the agreed venue, then **an encrypted working copy** may be sent in a sealed package and returned promptly by an agreed secure delivery route. Secure delivery is not by standard post. The master copy must remain securely stored.
16. A medical expert who takes possession of an intimate image must sign an undertaking as set out in Appendix A. This includes an undertaking not to show the intimate image to any person, save another medical expert, without the permission of the Judge. The requirement to sign the undertaking also applies to individuals responsible for the safe delivery of the intimate image to and from a medical expert (see 15).
17. Electronic intimate images may only be transferred using secure systems when they become available and subject to agreed guidance being issued. See Appendix B.

The use of images in evidence

18. Line drawings form part of the clinical record. Wherever possible line drawings should be used when giving evidence instead of using the original intimate image to avoid compounding the abuse of the child or adult.
19. It is not appropriate for lay people/non-clinicians to see these images. They will not be able to interpret them.
20. When a judge has ordered the disclosure of the intimate image in court, the doctor who recorded the images should be present to interpret the findings.
21. All versions of the intimate images, in whatever form, shall be returned to the doctor who made the original images who must acknowledge their receipt, or destroyed, depending on pre-agreed arrangements. If kept, the images shall be retained in accordance with legal requirements and relevant professional guidelines.

Appendix A

Undertaking must be given and signed and dated by any named person who takes possession of an intimate image, including for the purpose of delivery:

I, _____ (named person) undertake that whilst the intimate image in the case of R v _____ is in my possession I shall:

- ensure that the images are handed personally to the addressee only or their appointed agent (delete as appropriate);
- not permit any other person (other than as detailed in the original consent) to see the intimate image without the permission of the court;
- not cause nor permit any copy to be made of the intimate image; this includes the defendant and his/her legal representative;
- ensure that the intimate image is always kept in a locked, secure container, save when in use and not left in an unattended vehicle or otherwise left unprotected;
- return the intimate image by a secure route to the medical examiner who recorded it, **or**
- destroy the intimate image (this should be prearranged)

Signature _____

Print name _____

Date _____

Appendix B

- The use of non-official devices such as personal digital cameras must be avoided as this would breach NHS Information Governance policies.
- The intimate image should be digitally endorsed with the date and time of capture.
- The intimate image must be transferred to a secure computer storage media as soon as practical and erased from the device digital memory when no longer required. In the case of digital camera flash memory cards it should not be possible to recover data erased from the dynamic memory.
- Where the data is transferred to a computer system for processing or storage, that computer system must be secured to prevent unauthorised use. The use of shared home or public computers for this purpose must be avoided. When data is no longer required it must be permanently removed from the computer's hard disc. The data destruction must be achieved by using a reliable data shredding tool that overwrites the data to an acceptable industrial strength standard. There are many products available commercially that destroy data in this way.
- Where the intimate image file is stored to external media such as DV tape, CD-ROM or DVD then that media must be stored in a secure location that is accessible by properly authorised individuals only.
- The use of memory sticks or other flash media to store or share images must be avoided as they are easily lost or stolen. Where used for data transfer, memory sticks or other flash media must be compliant and encrypted.
- Where intimate image data on external media are no longer required the media should be destroyed to the point that they are no longer possible to use. Where exceptionally the media are to be reused, the data must be securely destroyed as described for computer systems above and a test made that it is no longer possible to access them.
- Systems used to process or store such data will benefit through a system level security policy statement that describes the scope of and security arrangements applicable to that system including accountabilities.