Faculty of Forensic & Legal Medicine

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

Sep 2023 Review date Sep 2026 – check www.fflm.ac.uk for latest update

Royal College of Paediatrics and Child Health
Leading the way in Children's Health

A note regarding terminology:
In this document, the person examined, and of whom intimate images may be photo-documented, is a patient. The patient may also be a complainant, (or complainer, the term used in Scotland), if they have alleged an assault or abuse.

1. Background

1.1 Concern has been expressed about the possibility of inappropriate disclosure and use of intimate images obtained during the forensic medical examination (FME) 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 images whether obtained in a forensic medical examination or other clinical assessment. Doctors and other healthcare professionals, (HCPs), should be aware images taken during a medical examination, forensic or otherwise, may become evidence in court, and so this guidance is applicable. Also see paragraph 9.1.

1.2 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, including where doctors and HCPs have been ordered by a Court to pass images to police or officers of the Court, e.g., solicitors.

1.3 Furthermore, it provides reassurance to patients, and/or their parents/carers, that such intimate images are taken, stored and managed with care, respecting confidentiality as far as is possible. Such reassurance is likely to enable patients, and/or their parents/carers to give consent to intimate images being taken and so clearer evidence may be provided to the Court. Without such reassurance and safeguards, patients and/or parents/carers will be concerned about how such images may be used and so be less likely to consent to images being recorded.

2. Definition

2.1 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 **specialist medical video-camera**, or similar suitable and recommended technology. This is often a colposcope, however, a careful explanation is necessary if using this term, as women who have experienced its use in a gynaecological context, may think it would be used in the same way. See also paragraph 9.1 and 9.2

2.2 These images may be taken during the course of clinical practice or an investigation into alleged or suspected sexual or physical abuse.

3. Procedure

3.1 Before an intimate image is taken of a child, the following procedure shall apply, please see: *Service specification for the clinical evaluation of children and young people who may have been sexually abused, RCPCH & FFLM*, 2015; (please note this document is currently under review).

In the examination of an adult or a child, informed consent from the patient and/or person/authority who holds parental responsibility for the child will be obtained and recorded. See *GMC Decision Making and Consent*, 2020. For a non-competent adult, professional guidance, including that issued by the FFLM should be used: *Recommendations - Consent from patients who may have been seriously assaulted*, 2022.

3.2 A child is a young person who has not yet reached their 18th birthday; at age 16 years, it is presumed the young person can consent. A young person under the age of 16 years may have the capacity to consent alone. Obtaining consent, (whether from an adult or a child) will involve ensuring they understand to what they are giving their consent and their capacity to do so. See the links above and also the *GMC 0-18 years guidance*, 2018, and note differences within the countries within the UK.

3.3 In obtaining consent, the patient and/or person acting on their behalf must be advised the images will have both clinical (e.g., for diagnosis) and forensic (e.g., evidential) purposes; 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 (subject to paragraph 5, Disclosure below).

3.4 If the patient or person with legal authority to act on their behalf declines permission for intimate images to be obtained, this choice must be respected and a record of it made in the notes. A patient who is also a complainant of sexual assault, may have experienced it being recorded by the alleged assailant(s), e.g., by a camera 'phone and so a request to allow photo-documentation of intimate images may be unacceptable and may possibly re-traumatise the patient. A patient or parent/carer may choose to consent to images being recorded, only if there are 'positive' findings. In such circumstances, it is important this is discussed, but if consent to recording is declined, then this must be respected, and comprehensive written notes and line diagrams, only, will be available as a record of the examination.

3.5 It must be explained the intimate images will be used in peer review, and, as this is part of the audit and clinical governance process, specific consent from the patient or their parent/carer is not required. However, specific consent must be obtained if the images are to be used for medical education and training.

3.6 All the images will be coded and securely stored, with password protection according to local protocols, policies and procedures 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.

3.7 Whilst intimate images are retained as part of the medical record, they should not be stored within the paper notes/record, (if held in such a format), as this presents a risk to the protection of anonymity. If the patient record is in an electronic format, then intimate images should either be stored separately, or they should be within files which have restricted access.

3.8 In whatever way the intimate images are stored, there **must** be a clear audit trail to demonstrate who has had access to them, when and for what reason. Also see paragraph 6.4, regarding auditable records of working copies which are disclosed, e.g., to an expert and returned.

3.9 Images of faces should **never** be included when recording intimate images, in order to protect anonymity. If the patient has an injury to their face, which requires photo-documentation, this is undertaken separately, see *PICS Working Group Guidelines on photography*, 2019. Patients, and/or their parents/carers, should be advised when images are being actively recorded, and asked to alert the clinician, if they wish to move. Similarly, care must be taken when the clinician may ask the patient to change position. If necessary, the recording may be stopped and restarted to avoid capturing the face of the patient. If, in error, the patient's (or another's) face is captured in the recording, then this must be noted in the patient's notes/records, including the time point in the recording at which it occurs, so viewing of that part of the images can be avoided, including if shown at a peer review meeting. See also paragraph 9.1 and 9.2.

3.10 Intimate images **must** be supported by line diagrams and a written description in the patient's record. **A comment on the quality or limitation of the recording should also be included, i.e., whether the images accurately reflect the clinical findings.**

4. Statements and Reports for Court

4.1 The doctor or HCP must state in the statement or court report if the examination has been photo-documented and whether there are intimate images as part of the patient record.

4.2 The doctor or HCP who undertook the examination will describe the findings and explain/interpret them in writing, stating what evidence is contained within the photo-documentation. If the doctor or HCP is not able to interpret the findings, this must be made clear in the report/statement, e.g., they were a trainee, under the supervision of an experienced clinician. In this situation, the supervising clinician would usually provide the interpretation.

4.3 As noted in the clinical record (see 3.10), the quality of the images must be described and whether they truly represent the clinical findings must also be commented upon in the statement or report.

4.4 Intimate images must not be attached to the statement or report.

4.5 If the images have been subject to peer review, then this will be noted in the report or statement. If peer review takes place later, after a report or statement has been written, an addendum to it may be necessary. See the FFLM guidance on this: *Peer review in Sexual Offences including Child Sexual Abuse Cases*, 2021.

5. Disclosure

5.1 Doctors and HCPs conducting forensic medical examinations are 'third parties' for the purposes of the Criminal Procedure and Investigations Act (CPIA) 1996.

5.2 Organisations should have a protocol or guidance to manage disclosure requests. If there is any doubt about the request and/or the consent, advice should be sought, for example, within the organisation, from the Lead Clinician, the Caldicott Guardian, the Data Protection Officer and/or the legal department. The doctor or HCP may seek advice from their medical indemnity or medical defence organisation, (MDO). If requested to disclose intimate images, the doctor or HCP should consider making representations regarding by whom the intimate images should be seen, to ensure it is an appropriately trained medical expert, citing this document. However, the clinician must disclose the intimate images if they are ordered to do so, by a Judge, via an order in writing, or there is a public interest in doing so.

5.3 A doctor or HCP can and should decline to allow inspection of the intimate image by a non-medical professional, see 5.2 above, citing this document, in which case 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 Act 1980. See The Home Office Guidance: *Criminal investigation guidance for witness summons*, 2022.

5.4 Doctors and other HCPs must be aware if the intimate images or copies of such images (as opposed to a report which refers to them) were to be 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 or HCPs should not hand over intimate images or copies of images to the police or prosecutor without appropriate informed consent or a court order.** See paragraphs 3.1 – 3.4 above and *Peer review in Sexual Offences including Child Sexual Abuse Cases*, 2021

As well as criminal cases, requests and orders to disclose images may arise in Civil/Family proceedings. Doctors and HCPs may wish to consider making representations, including to the Court, of the importance of the interpretation of the findings by the doctor or HCP. This may include a respectful request to consider delaying or limiting distribution and suggesting the doctor or HCP assists with any clarification needed, first, in response to a request or court order. (Also see paragraph 7.4).

5.5 If the intimate images are inspected or held by the prosecution, and it is the decision of the prosecutor whether the relevant test for disclosure is satisfied, the doctor or HCP must be notified of the decision. Consideration will need to be given as to how the patient or the person with parental responsibility is informed of the disclosure.

6. Examination/review by prosecution or defence experts

6.1 In England and Wales, **the various 'Procedure Rules', have expectations of those involved in the Court process**:

- *Rules & Practice Directions - Civil Procedure Rules*
- *Criminal Procedure Rules and Practice Directions 2020*
- *Family Procedure Rules*

These include the **'Overriding Objective'**, where cases must be dealt with 'justly'; this includes **'expeditiously'**. **This puts a duty on Sexual Assault Referral Centres (SARCs), clinics or hospitals to respond appropriately and in a timely way, when intimate images are to be reviewed by an expert.**

6.2 The defence or prosecution may apply for their medical expert to inspect the intimate images. It is best practice for the expert to view the images with the clinician who undertook the examination and recorded the intimate images, at a suitable venue. This will usually be the SARC, clinic or hospital where the examination took place, and the images are securely stored.

6.3 A written request must be sent to the SARC/clinic/ hospital, specifying the name of the expert, their regulatory number and contact details, including a suitable, secure email address. When the expert attends, they should bring confirmation of their instructions and appropriate identification. A record must be made to show when the expert viewed the intimate images and with whom.

6.4 However, with the use of 'platforms', this may offer a secure electronic means of the examining clinician to review and discuss the images with the expert, avoiding travel. This is similar to what enabled peer review to continue after the start of the COVID-19 pandemic. The expert must agree to the use of a secure platform which meets the information governance requirements of the organisation where the examination was undertaken, or which holds the records. The expert may be required to make undertakings (see paragraph 6.5).

6.5 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 double-sealed package and returned promptly by an agreed secure delivery route, or destroyed according to an agreed protocol, (see also Appendix A). Secure delivery is not achieved by standard post. The master copy must remain securely stored. The password must be shared separately, via a secure route.

6.6 A medical expert who views, or any other 'custodian', who takes possession of an intimate image must sign an undertaking as set out in Appendix A, (below). This includes an undertaking not to show the intimate image to any person, save another medical expert, without the permission of the Judge. The medical expert will refer to the images in their report but must not attach any intimate image to it. **Undertakings must include not copying, sharing or showing the images to anyone else.**

6.7 The agreement regarding returning the working copy of images is determined by the examiner/clinician releasing the images or their organisation. In some facilities, it is essential it is returned, because it is not possible to generate further copies from the master record. When the working copy is returned to the clinician, there must be an auditable system to document when it was returned/received and by whom.

N.B 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; for example, this may be someone in the legal profession, e.g., a solicitor or paralegal, or a courier transporting the images. A medical expert who fails to comply with such an undertaking may compromise their probity and thus may put their professional registration at risk.

6.8 Electronic transfer of intimate images may only take place using secure systems when and where available and subject to agreed guidance being issued.

N.B. Doctors and HCPs and any other individual involved, must be satisfied the security is robust within their respective systems; e.g. with email; see *NHS Guidance for sending secure email*. Similarly, with developments in information technology, other electronic systems may be developed, including those which may permit secure sharing or time limited, unique password-protected access to a record, so that the examining doctor or HCP at the SARC/clinic/hospital and the expert may view and discuss the images, in real time, but the expert is at a different location. See Appendix B, (below).

6.9 An order of the Court may be made to disclose images, for example, to a medical expert who may work outside the UK. Whilst the principles described here still apply, there may be additional considerations in ensuring safe and secure disclosure and delivery to the medical expert and their undertaking to return or destroy the images, securely.

7. The use of images in evidence

7.1 Line drawings form part of the clinical record. Wherever possible line drawings should be used when giving evidence in Court, instead of using the original intimate image to avoid compounding the abuse of the child or adult.

7.2 It is **not appropriate** for lay people/non-clinicians to see these photographic intimate images. They will not be able to interpret them.

7.3 When a judge has ordered the disclosure of the intimate image in court, the doctor or HCP who recorded the images should be present to interpret the findings. If the doctor or HCP is unable to interpret the findings, this must have been made clear in their statement or report (see 4 above), so that the Court is able arrange for an expert to review the images.

All versions of the intimate images, in whatever form, shall be returned to the doctor or HCP who made the original images (or named individual at the SARC/clinic/ hospital where the images are retained). There **must be** an acknowledgement of their receipt, or destruction, depending on pre-agreed arrangements. If kept, the images shall be retained in accordance with legal requirements and relevant professional guidelines. It is essential the sharing of images and their subsequent return or destruction can be audited, to demonstrate compliance with best practice.

7.4 N.B. If intimate images are released into a non-medical setting, the staff working in such organisations, (e.g. police, lawyers, local authority), who interact with or who are part of the Justice systems within the UK, (e.g. criminal, civil, including family courts and possibly coronial services), must ensure there are robust and secure storage, access and viewing protocols, with audit arrangements to ensure there is no inappropriate access to intimate images. **Images must only be accessed and viewed for essential evidential purposes**. **(See paragraph 3.8, above: In whatever way the intimate images are stored, there must be a clear audit trail to demonstrate who has had access to them, when and for what reason.)**

Inappropriate access will have a negative effect on the patient, as well adversely affect the trust and confidence the public have in the Judicial system(s) and the organisations who interact with them. Moreover, individuals who access and/or view such images, but have no justification to do so, may face regulatory and/or employer disciplinary processes, as well as the possibly of prosecution. The individual's employing organisation may be reported e.g., to the Information Commissioner.

8. Requests from patients/carers to view or destroy images

8.1 A patient or their parent/carer may make a subject access request, (SAR); see: *Subject access code of practice* to view the medical record, of which the intimate image is part. Such a request will be processed in the usual way by the Trust/doctor's or HCP's employer, but as such records may also have an evidential purpose, it is appropriate to make reference to such access in the patient's notes and also in a statement or report. The 2018 Data Protection Act (DPA), which implements the General Data Protection Regulation (GDPR), allow exemptions to a SAR, where the right of access is likely to pose serious harm to the physical or mental health of an individual. Therefore, consideration must be given to whether such a SAR is potentially harmful to the patient. As a result, safeguarding and legal advice may also be required, e.g., where a parent or someone with parental responsibility, who may be the abuser, seeks access to such records.

8.2 If such a SAR is appropriate, the examining doctor or HCP should be available to explain the images and the findings; or if that is not possible, an appropriately trained doctor or HCP instead.

8.3 Similarly, a patient or parent/carer may request to have images destroyed. The doctor or HCP must obtain appropriate advice, including that outlined in paragraph 8.1, before any action is taken, explaining this is because of the potential evidential purpose of the record. However, clinicians and managers must also be aware of any order or direction which provides advice on or prohibits the destruction of records. In particular, in England and Wales, the following documents, both of which describe the records which must be retained and not destroyed:

Please note: the instruction from the then Chairman of the Independent Inquiry into Child Sexual Abuse (IICSA), 2015, and the moratorium contained therein, is no longer in place.

- IICSA published its final report in October 2022 and provides guidance in the following terms:

  With the publication of the Inquiry's Final Report on 20th October 2022, central government departments and their arms length bodies can now resume disposal of records that have been retained for IICSA, in line with their retention schedules.

  Although the Inquiry will not formally close until early 2023, there is no intention to make further requests for documents. In doing so, however, the Inquiry asks that departments consider the following when drawing up disposal plans:

  If any of the records you have retained for IICSA are likely to be of significant personal interest to victims and survivors, update retention schedules to reflect the recommendations in the Final Report.

  The obligation to retain records for other inquiries remains. The Inquiry's public correspondence routes will close in the coming weeks; as such, any enquiries about this letter should be directed to the Home Office: public.enquiries@homeoffice.gov.uk.

- The publication, *Corporate Records Retention Schedule*, 2022 from NHS England has yet to be amended to show the above advice.

  However, information about current requirements and responsibilities, with regard to records can be found via these links:

  - *Letter to NHS CEOs, IICSA*
  - *End of IICSA Moratorium Permanent Secretary, IICSA*

8.4 In relation to criminal investigations, it is appropriate to seek advice; for example the Crown Prosecution Service (CPS), in its *Guidance for Experts on Disclosure, Unused Material and Case Management*, 2019, states at 4.8.2:

'...You should, therefore, obtain advice from the investigator for the retention period that applies to this particular investigation and always before contemplating destruction of any material.'

8.5 NHS Digital has guidance on storage and retention of records: *Records and document management policy - NHS Digital* (October 2022) and *Records Management Code of Practice - NHS Transformation Directorate* (August 2023). It advises a **minimum** retention period of 30 years, or 10 years after death (if known).

8.6 See also *Forensic Records: Frequently Asked Questions for all healthcare professionals*, 2019.

9. Other issues

9.1 In the clinical assessment of children, images may be taken by medical illustration and these may be both of the face and body, and perhaps also intimate images. These may not be managed as described above, but be retained together, in the child's clinical record.

9.2 Unsolicited images may be sent to doctors by parents or other professionals. The approach to managing these images is addressed in the RCPCH and FFLM Best Practice Guide (2019) *Medical photography of possible physical abuse in children – RCPCH Child Protection Portal*.

9.3 In some circumstances, a historical image, e.g., a skin condition of the ano-genital area (perhaps a 'nappy rash'), is in a child's medical record and the consent given at that time, was for its use for medical (e.g., diagnostic and/or treatment) purposes, only. Such an image may later be considered to have a forensic or medico-legal significance, e.g., in the context of suspected/alleged child sexual abuse (CSA). Clinicians and organisations need to ensure they have appropriate procedures to deal with requests to disclose such records, should they arise.

9.4 The clinical, forensic, evidential and legal context in which clinicians, and other professional groups and organisations, deal with intimate images, means it is essential individuals and organisations ensure they remain up-to-date with the ethical, professional and legal responsibilities in taking, managing, storing, disclosing and sharing intimate images. They must also be aware of the risks when an unsolicited image may be sent, for example by a parent or carer which meets the definition of an intimate image, but legally, an 'indecent image'. Individuals and organisations should be aware of the relevant legislation in their jurisdiction, see box below.

England and Wales
Protection of Children Act 1978
Criminal Justice Act 1988

Northern Ireland
Protection of Children (Northern Ireland) Order 1978

Scotland
Civic Government (Scotland) Act 1982

Originally produced on behalf of the FFLM and RCPCH
by Dr Sheila Paul, Dr Helen Hammond and Dr Jacqueline Mok
Reviewed and updated by Dr Bernadette Butler, Sep 2023

Send any feedback and comments to forensic.medicine@fflm.ac.uk

APPENDIX A

N.B. please note paragraphs 3.8 and 7.4, above

Undertakings must be given, 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(s) of

(insert clinic/SARC unique ID number. N.B. Do **NOT** include patient's name)

_____

In the case of R v _____

Or specify (e.g., Family Court Proceedings)_____

_____

is in my possession, I will:

- ensure 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 their legal representative;
- ensure 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;
- if it is an electronic copy, ensure it is securely stored and the password to the computer and, if appropriate to the storage device, as well as that to the image itself, is kept secure and separately;
- return the intimate image by a secure route to the medical examiner who recorded/released it, (see paragraph 6.4 above), where its receipt will be recorded for audit and Information Governance (IG) purposes; or
- securely destroy the intimate image (this should be pre-arranged) to the appropriate and agreed standard, e.g., as required/stipulated by local/national IG requirements, as described in my instructions (and so will need clarification in the instruction to the expert).

New custodian/received by	Former custodian/handed over by
Name (print and include regulatory number, if appropriate)	Name (print and include regulatory number, if appropriate)
Signature	Signature
Role/Organisation (in this case) & contact details	Role/Organisation (in this case) & contact details
Date Time	Date Time

APPENDIX B

N.B. please note paragraphs 3.8 and 7.4, above

- NHS and other organisations, as well as their employees, including clinicians, and anyone else involved in the storage or transfer of such images must be aware of national and local Information Governance (IG) Policies and Data Protection law and be able to show they are up-to-date in training and compliant. SARCs/clinics/hospitals must ensure they have adequate and regularly reviewed policies on record management, which includes the requirements of managing intimate images. Systems used to process or store such data will benefit through a system level security policy statement which describes the scope of and security arrangements applicable to that system including accountabilities. Similarly, IT policies and protocols must ensure there is appropriate secure disposal in place for hard and software which is no longer required. This includes CDs or DVDs, which are damaged or where the recording is incomplete or does not proceed as usual.
- Non-official devices such as personal digital cameras or cameras in mobile 'phones must not be used; this would breach NHS and other Organisations' Information Governance (IG) policies.
- The intimate image should be digitally endorsed with the date and time of capture, name of clinician who recorded them, and patient unique identifying number.
- The intimate image must be transferred to a secure computer storage medium 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, the computer system must be secured to prevent unauthorised use. The system must be able to show who has accessed images and when. The use of shared home or public computers for this purpose is prohibited. 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 which overwrites the data to an acceptable industrial strength standard and/or complies with local/ national IG requirements. There are many products available commercially which destroy data in this way.
- Where the intimate image file is stored to external media such as DV tape, CD-ROM or DVD then the media must be stored in a secure location which is accessible by properly authorised individuals only; similarly, access must be recorded, so that who accessed the images, when and for what purpose can be audited.
- The use of memory sticks or other flash media to store or share images should be avoided, as they are easily lost or stolen. However, where used for data transfer, memory sticks or other flash media must be security and IG compliant and encrypted.