Institute of Medical Illustrators

IMI National Guidelines

A Guide to Good Practice

Mobile Phone Photography Guidelines

These guidelines have been developed by the Institute of Medical Illustrators, in consultation with specialist advisors. They should be considered a guide to good practice, providing a baseline for auditable standards. If necessary, adaptations may be made to take into account your local conditions.

clinical photography, design and video in healthcare

Registered Office: 12 Coldbath Square, London. EC1R 5HL. Tel: 0207 837 2846. Web: www.imi.org.uk
Registered No: 933565. Registered Charity No: 313433

Contents

The aim of these guidelines is to provide advice for IMI members in order to:

- Provide a guide to good practice
- Support members by providing national guidance
- Protect members from disciplinary action as a result of an information security breach
- Enable members to respond to individual organisations' requirements based on advice and recommendations from the Institute of Medical Illustrators

The document has been checked for accuracy relating to the Data Protection Act 1998 by the Information Commissioners Office (ICO) case reference number ENQ0477035.

Definitions

Data controller	An organisation or body which uses personal data
DH	Department of Health
DPA	Data Protection Act 1998
DPC	Data Protection Commissioner (Republic Of Ireland)
EEA	European Economic Area
Encryption	Coding or scrambling of information into cipher text using cryptography technology and a decoding key is required to decode the information
HSE	Health Service Executive (Republic of Ireland)
ICO	Information Commissioner's Office
IMI	Institute of Medical Illustrators
MI	Medical Illustration
ROI	Republic of Ireland
Sensitive personal data	Data relating to religious or other beliefs, sexual orientation, **health**, race, ethnicity, political views, trades union membership, criminal record.
Smartphone	Mobile phone built on a mobile operating system with internet connectivity and advanced computing capability

The guidelines relate solely to the use of mobile phones for clinical photography purposes and do not in any way override local health and safety policies in terms of interference with medical devices.
The reference to mobile phones is intended to include all portable devices with integrated cameras, with or without internet connectivity.
It is recommended that these guidelines should be included in the appendix of local Clinical Photography, IT (IM&T), Information Governance and e-health policies.
Throughout the document we refer to NHS Trusts. However, in most cases the information is equally applicable to any healthcare provider in the UK or ROI.

Introduction

These guidelines have been produced to provide standardised national guidance for IMI members in the UK and ROI who have service management or image management responsibilities. It is recommended that they be used to facilitate corporate discussions and local policy development relating to the use of mobile phones for clinical photography

Background Information

Mobile phone cameras differ from conventional 'stand-alone' cameras as many have a combination of internet connectivity and the ability to send picture messages, therefore are subject to hacking and security breaches resulting in potential disclosure of highly sensitive patient images. This is of particular concern where devices are personally owned by individuals and do not belong to Trusts/Hospitals where encrypted devices may be employed and managed securely using specialist mobile device management software via local Information Governance and IT departments.

The Institute has received widespread reports of growing pressures on clinical photographers and service managers in NHS Trusts and other healthcare organisations to authorise, endorse or manage images taken on clinicians' personal mobile phones. In some instances they have been asked to provide training or create guidelines and protocols on the use of mobile phone images, which raised significant information governance concerns within the clinical photography profession. These concerns were discussed by IMI Council who agreed that national guidance should be developed for IMI members.

In the development of this document professional advice was sought from the Information Commissioner's Office to ensure accurate representation of Data Protection information and to enquire about the wider issue of the use of mobile phones for clinical photography within the NHS. In response to this enquiry, the ICO stated the following:

"*The seventh principle of the Data Protection Act 1998 (DPA) requires that an organisation keeps personal data secure. Ultimately, it is a data controller's responsibility to ensure that their procedures are compliant with the DPA. A data controller can take into account national standards or codes of conduct to assist in their compliance with the seventh principle*

"The DPA does not expressly prevent phones or similar devices being used in a clinical setting. In some cases it might be advantageous to doctors and patients – for example by allowing diagnoses to be made remotely.

However it would raise several new security risks, many of which could be avoided if phones were not used. The lack of encryption and ease of accessing and sharing the images is a significant risk. It is important to note that requiring doctors to use their personal devices is almost certainly not justified, as it would become very difficult for the Trusts to exercise proper control over how the data is used. If the Trusts provided staff with appropriately configured devices, they might be able to use them in compliance with the DPA.

Of course in an emergency situation where there is no alternative, the ICO is unlikely to decide that a breach has occurred."

(ICO Jan 2013, case reference ENQ0477035)

The primary purpose of these guidelines is to help ensure that medical illustration staff and departments comply with legislation and avoid any breaches of the Data Protection Act 1998 (DPA) (or, in the Republic of Ireland, the Data Protection Act 1988, Data Protection Amendment Act 2003) as a result of processing images created on non-secure devices.

Practice

Clinical photography of patients is considered to constitute personal data and is therefore governed by the UK and ROI data protection acts. Other guidance is more specific to photography. The DH guidelines document 'Using mobile phones in NHS Hospitals – January 2009' considers all aspects of mobile phone use and the following section relates specifically to the use of mobile phones for photography:

"3.8 The Information Commissioner's Office states that all public and private organisations are legally obliged to protect any personal information they hold. In relation to this, any individual who takes a photograph of another individual using the camera on their mobile phone, subject to exceptions such as for limited household purposes, will be processing personal data and must comply with the Data Protection Act 1998 (DPA) in relation to the circumstances in which the photograph is taken and the use of that photograph".

This means that except where patients may photograph themselves or a family member (limited household purposes) any photograph taken of a patient on a mobile phone is subject to the strict guidelines of the DPA as clinical photographs can be classified as sensitive personal data as defined by the DPA 1998:

"Sensitive personal data: a health record that consists of information about the physical or mental health or condition of an individual, made by or on behalf of a health professional in connection with the care of that individual" (DPA 1998)

In the ROI specific guidance on mobile phone use in hospitals includes the HSE Mobile Phone Device Policy *version 2*, and the HSE encryption policy 2003. The HSE Mobile Phone Device Policy states:

"4.13 Confidentiality & Privacy

Mobile phone devices equipped with cameras must not be used inappropriately within the HSE. In this regard users must not:

a) Take photographs or video recordings using a HSE mobile phone device or any other device in areas where an employee, patient or client has a reasonable expectation of privacy.

b) Distribute photographs, videos or recordings of any type using HSE mobile phone devices around the HSE, unless the content and use have been approved in advance by the user's line manager."

The seventh principle of the UK's DPA (the fourth principle of the DPA in ROI) requires that an organisation keeps personal data secure. Ultimately, it is the individual organisation's responsibility as the data controller to ensure that their procedures are compliant with the DPA:

The NHS Chief Executive has directed that "there should be no transfers of unencrypted person identifiable data held in electronic format across the NHS. This is the default position to ensure that patient and staff personal data are protected. Any data stored on a PC or other removable device in a non-secure area or on a portable device such as a laptop, PDA or mobile phone should also be encrypted". (DH 2008 – Digital Information Policy)

This strengthens the argument that personal mobile phones are unsuitable for clinical photography from a security perspective as the devices themselves are usually unencrypted and are at risk of disclosing personal information if lost or stolen.

The ease of sharing images is also a significant concern. Even if the device itself is encrypted, there is the risk of images being emailed or sent via text message to individuals on unencrypted devices and saved or forwarded to an insecure storage area.

In all instances, whether personal mobile phones are encrypted or not, the additional concern of 'offline' storage should be considered:

"Personal data must not be transferred outside the EEA unless adequate provisions are in place for its protection" (DPA 2008 - Principle 8).

The ROI (Data Protection Amendment) Act 2003 – section 12) concurs with this, stating:

"The transfer of personal data to a country or territory outside the European Economic Area may not take place unless that country or territory ensures an adequate level of protection for the privacy and the fundamental rights and freedoms of data subjects in relation to the processing of personal data having regard to all the circumstances surrounding the transfer".

Most personally owned mobile phones have an integral cloud based storage facility which is simply an online storage facility using remote servers which are accessed via the internet. It must be made clear that a third party (MI department) cannot guarantee the integrity or security of any images that have been stored on a cloud based server that is external to the local organisation. Many commercially available cloud based storage facilities are based in the United States of America and therefore fall outside of the EEA. Effectively this means that personal information is not governed according to UK, ROI or EEA laws which could cause information security infringements and breaches the DPA.

The advice of IMI is that unless a mobile phone belongs to the organisation and is encrypted and configured to securely store and transfer data only via a Trust approved method then it should not be used for the purposes of clinical photography.
IMI does recognise however, that there may be instances where this has occurred and MI departments are required to manage or process the resulting images. This may be as a result of a clinician being in a remote location and in an emergency situation, or it may be a situation in which a patient has brought their own images of a transient medical condition. In these circumstances the following guidance should be considered:

- **Images produced by a clinician on a personal mobile phone:**
  If a MI department is asked to store images which have been captured by a clinician on an unsecure device, a disclaimer should be issued stating that the MI department cannot be held responsible for the image integrity, confidentiality, availability or security prior to upload. If such images are requested by legal agencies then it must be made explicit in an accompanying statement that a full audit trail of activity relating to the images cannot be provided and that the integrity, confidentiality and security of the images cannot be guaranteed by the MI department issuing them on behalf of the clinician who captured the images due to the lack of formal process or audit trail.
- **Images supplied by a patient from their personal mobile phone:**
  If managing images from unapproved devices on behalf of a patient who may provide their own 'clinical' images, it is advisable to issue a disclaimer to the patient stating the fact that image confidentiality and security cannot be guaranteed prior to storage and that audit trails cannot be proven to verify the integrity of the images if required to do so by external agencies.

  In both cases, written informed consent must be obtained from the patient for the intended use of the images prior to processing and release.

Organisations supporting the practice of personal device use should understand that there is no formal audit capability for image integrity if required in the eventuality of any dispute or challenge over patient treatment.

Summary

The decision to allow the use of Trust owned, encrypted mobile phone cameras is ultimately a judgement for each organisation, therefore individual Trust guidelines and variations in regional legislation must be observed. All NHS Trusts should have a clinical photography policy and reference to mobile phone photography must be included within that policy. Section 4.8 of The DH guidelines 'Using mobile phones in NHS Hospitals – January 2009' states that:

"NHS trusts should have a written policy regarding the use of mobile and camera phones, cameras and video recording devices. It should be easily accessible to staff, patients and visitors and have the patient at the forefront of any such policy. All staff should be aware of the policy, and its reasons. The policy should be reviewed periodically."

In addition, it is recommended that in recognition of the significant risk of breach of the DPA in regard to security of personal data, organisations do not permit the use of personal mobile phones for clinical photography and a full risk assessment should be carried out outlining the reasons, risks and benefits of doing so under exceptional circumstances to mitigate potential claims of liability or culpability. While IMI cannot itself make corporate decisions about the authorisation of the use of mobile phones, this document aims to provide guidance for local implementation to act as a safeguard for IMI members and individual organisations against formal complaints, or in extreme cases, legal action resulting from a breach of the DPA.

References / Bibliography

Department of Health (2008) *Digital Information Policy* https://www.igt.connectingforhealth.nhs.uk/WhatsNewDocuments/Encryption%20Guidance%2031.1.2008.doc *[accessed 18/05/2013].*

Data Protection Act (1998) London. HMSO http://www.legislation.gov.uk/ukpga/1998/29/contents

Department of Health (2009) *Using mobile phones in NHS Hospitals* PDF doc. http://webarchive.nationalarchives.gov.uk/20130107105354/http:/www.dh.gov.uk/prod_consum_dh/groups/dh_digitalassets/@dh/@en/documents/digitalasset/dh_092812.pdf [accessed 15/05/2013]

HSE *Frequently Asked Questions on Data Protection* http://www.hse.ie/eng/services/yourhealthservice/info/DP/Frequently_Asked_Questions/ *[accessed 05/06/2013 - ROI]*

HSE *Mobile Phone Device Policy (2010) version 2,* http://www.hse.ie/eng/services/Publications/pp/ict/Mobile_Phone_Device_Policy.pdf *[accessed 05/06/2013 - ROI]*

HSE *Encryption Policy (2013) version 3,* http://www.hse.ie/eng/services/Publications/pp/ict/Encryption_Policy.pdf *[accessed 05/06/2013 - ROI]*

HSE *Electronic Communications Policy (2013) version 3,* http://www.hse.ie/eng/services/Publications/pp/ict/Information_Security_Policy.pdf *[accessed 05/06/2013 - ROI]*

Information Commissioners Office. *Information Security.* http://ico.org.uk/for_organisations/data_protection/the_guide/principle_7 [accessed 18/05/2013]

ROI (DPA 1988, (Data Protection Amendment) Act 2003) Government of Ireland. Oireachtas

http://www.irishstatutebook.ie/2003/en/act/pub/0006/print.html