Mobile Phone and Mobile Apps for Clinical Photography
A Guide to Good Practice
The IMI National Guidelines have been prepared as baseline guides on specific aspects of medical illustration activity and provide auditable standards for the future.

The Guidelines can either be implemented in full, or may be amended according to individual requirements.

Copies are available on the IMI website (www.imi.org.uk).

© Institute of Medical Illustrators 2019

All rights reserved. Unauthorised copying, distribution or commercial exploitation is prohibited and will constitute an infringement of copyright. Reproduction permission granted for personal and educational use, and for the development of Medical Illustration departmental guidance, subject to acknowledgement of the source material.

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 local policy.

Published by the Institute of Medical Illustrators, October 2019, Version 2.0.

Lead Author – Anthony Edwards
# Contents

Acknowledgements ................................................................. 4
Objective .................................................................................. 5
Introduction ............................................................................ 6
Use of Mobile Phones in the Clinical Setting ................................ 6
Ownership of Devices .............................................................. 6
Data Protection ........................................................................ 8
Personal Data ........................................................................... 8
Consent .................................................................................... 8
Security and Data Storage ....................................................... 10
Freedom of Information .......................................................... 10
Data Processing ....................................................................... 11
Data Sharing ............................................................................ 11
Instant Messaging Apps .......................................................... 12
Processing Images from Mobile Phones .................................... 12
Quality Control ........................................................................ 13
Consent .................................................................................... 13
Data Security ............................................................................ 13
Penalties .................................................................................. 14
Mobile Phone Apps ................................................................. 14
Summary .................................................................................. 15
Glossary ................................................................................... 16
References ............................................................................... 17
Bibliography ............................................................................. 18
Lead Author and Working Group ............................................ 19
Acknowledgements

These guidelines have been prepared by the Mobile Phone Apps Working group on behalf of the Institute of Medical Illustrators (IMI). They are a revision of the Mobile Phone Photography Guidelines published by IMI in June 2014. The revision takes into consideration the changes in legal requirements following the introduction of General Data Protection Regulations (GDPR) in May 2018, and to acknowledge the increasing role that mobile Apps are playing in the delivery of healthcare services. It is recommended that these guidelines be included in appendices of local Clinical Photography, IT (IM&T) Information Governance and e-health policies. These guidelines do not override local health and safety policies in terms of interference with medical devices.

This document has been checked for accuracy relating to the Data Protection Act 2018 and General Data Protection Regulation by the Information Commissioners Office (ICO) case reference IC-12437-Z2H2 and the Data Protection Commissioner (DPC) Ref: DPC-17-2103-151943-b9a5d.
Objective

These guidelines provide advice for all IMI members on best practice in the use of mobile phones in clinical settings, the use of mobile phone Apps for clinical photography, and the legal requirements pertaining to data protection when capturing patient information. They also act as a reference for other healthcare workers involved in the production and circulation of patient data. Throughout this document there will be references to mobile phones; this is intended to include all portable devices with integrated cameras, with or without internet connectivity, that are capable of recording patient data. Whilst there is a particular emphasis on the use of mobile phones for clinical photography, these guidelines are relevant to all patient data captured on mobile devices including but not limited to, still images, video, audio and text.

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

• Provide a guide to best practice and legal requirements;
• Support members by providing national guidance;
• Provide advice for members in cases of information security breach;
• Enable members to respond to individual organisations’ requirements based on advice and recommendations from the Institute of Medical Illustrators.
Introduction

Technology is developing at an unprecedented rate and many of the advances offer huge potential for improvements within healthcare. Smartphones are now commonplace and they have penetrated the clinical setting in the same way that they have daily life. Improved hardware, lenses and sensors, and an increasing variety of mobile phone Apps, offer the opportunity to change the way patient care is delivered. However, there is a need to balance innovation with regulation.

There are benefits and risks to the use of mobile phones for clinical photography. Mobile phones are already in the hands of most clinical staff, they are easy to use and provide an instant result that can be shared very quickly and easily with colleagues.

The risks of using mobile phones in a clinical setting include poor security (both physical and digital), the ease with which images can be shared, and quality limitations. Clinical photography is a highly skilled profession and while good quality images have the power to enhance patient care, poor quality images may negatively impact on patient care by missed diagnosis or delayed treatment.

Use of Mobile Phones in a Clinical Setting

This section focuses on the use of mobile phones, primarily by healthcare practitioners, in a clinical setting and the legal and governance issues that need to be considered whenever a decision is made to use a mobile device to make a record of a patient’s condition.

Ownership of Devices

Ownership of mobile phones is an important factor when considering clinical photography and falls into two categories, those owned by the employing organisation and those that are personally-owned, known as bring your own devices (BYOD). The advantage of organisation-owned devices is that they can be optimized for clinical use to include:

- Stronger access controls – e.g. two factor authentication;
- Industry-standard data encryption;
- Managed back-up of data – not backed up to personal cloud;
- Managed licensing of accepted Apps for clinical photography and image management;
- Ability to wipe data remotely should the device be lost or stolen.
At first glance BYOD may appear to be a cost-neutral solution but the difficulty of managing and securing data across a variety of device types and operating systems may negate the savings. Patient data held on BYOD remains the property and responsibility of the organisation and systems need to be in place to allow access to data when needed. There is a significant risk of personal devices being accessible by family or other third parties, meaning it is vital that patient data is never stored in a standard photo gallery or accessible without secondary authentication.

**Research**

A recent study\(^1\) of UK orthopaedic clinicians found that 100% (n=100) of the sample owned a smartphone.

- 91% had patient photos and videos on their phone.
- 83% used online (cloud) back-up of their device.
- 79% admitted photographing an anaesthetised patient without prior consent.\(^1\)

A 2017 study\(^2\) in University Hospital Limerick (ROI) found that 100% (n=40) of responders had active ‘group chats’ on WhatsApp to communicate with members of their team.

- 97% admitted to routinely sending sensitive patient data via WhatsApp.
- 30% of respondents had lost their phone in the last year.\(^2\)

A 2018 study\(^3\) at two paediatric teaching hospitals in Dublin (ROI) reported 98% (n=265) smartphone ownership among hospital doctors.

- 97% use smartphones to communicate with their team (73% using WhatsApp).
- 57% had clinical images on their phone.
- 42% obtained consent for patient images.\(^3\)
Data Protection

It is worth remembering that any image that records a patient’s condition is a health record and the same standards of confidentiality, security and accessibility must be applied to them as to other health records. The convenience of using mobile phones should never outweigh the responsibility to protect patient data. The GDPR guidelines came into effect in May 2018 and allow individuals greater control over how their personal data is collected and processed.

Personal Data

Personal data is at the centre of the GDPR guidelines and is defined as data relating to a living individual who is or can be identified either from the data, or from the data in conjunction with other information that is in, or is likely to come into, the possession of the data controller. Health records are considered to be in a special category of personal data that covers the data subject’s physical or mental health or condition or sexual life. As special category data is considered to be more sensitive there is more protection afforded in relation to processing this type of data.

A photograph of an individual is not automatically considered to be personal data. However, if a photograph is taken for the purposes of recording, learning or deciding something about an individual then it will constitute personal data. What if the subject is not identifiable? What constitutes being identifiable is not always straightforward. While the face is the most obvious identifying feature for the majority of individuals it is not the only marker – a tattoo, a birthmark or a distinctive lesion may all give clues to an individual’s identity. Images that include elements of how a patient is dressed, traditional cultural clothing, a uniform or a distinctive medical condition can all have an impact on identification. With this in mind it is worth considering the potential in all clinical images for identification.

Consent

There are two aspects of consent that must be considered in relation to making a clinical recording of a patient. The first is consent to treatment; asking the patient’s permission to make a recording of them. NHS guidance on consent to treatment stipulates that consent should be given to the healthcare professional directly responsible for the patient’s current treatment. In relation to clinical photography this refers to the person taking the photograph (see IMI National Guidelines on Confidentiality & Consent).

The second aspect is concerned with consent for how that recording or data will be processed. Clinical photography has historical connections with research and teaching and as a result many organisations have consent policies and practices that typically allow for different levels of consent that a patient may permit; health record (or direct
medical care), for educational use and when required, consent to publish images. GDPR has specific standards for consent and how data is collected and processed. The regulation states that:

**Consent must be clear and concise** – patient must be made aware of what the intended use is and the implications for such use. If an image is to be published patients should be aware that this can mean that it will be in the public domain.

**Consent must have positive opt-in** – a clinician should never pre-tick boxes on a consent form before asking a patient to sign. Boxes should be left blank until the patient has been asked for permission giving them greater opportunity to refuse.

**Consent to processing should not be a precondition of service** – many patients will feel an obligation to agree to their images being used by the person treating them. Clinicians should make patients aware that saying no will not impact on the quality of the care they receive.

**Keep evidence of consent** – One of the current challenges with the use of mobile phones to record clinical images is that there is often no record of consent kept with the images (mobile Apps will usually have this function and will be discussed later). In the case of unconscious / anesthetised patients this is particularly important to prove that permission was sought and granted. Generic surgical consent forms that bundle photography / video consent together with consent for the procedure will not satisfy GDPR requirements.

**Make it easy to withdraw consent** – Although there is a legal basis that gives patients the right to withdraw permission for use of their images, it should be explained that in the event that an image has already been published it can't be 'unpublished'.

---

**Example**

In a typical clinical situation a junior doctor is sent to a dressing change to view the progress of a wound. In order to make it easier to report back to their consultant, they ask the patient if they would mind them taking a quick photograph of the wound. While the doctor may feel like they gained consent this only covers permission to treatment – there is no implied permission for use or any record made of the patient's consent. The doctor may go on to share the image with other members of the team electronically without gaining the necessary permission to do so. As the data controller, they are responsible for breaching GDPR rules.
Security and Data Storage

All organisations (Data Controllers) have an obligation to process and store personal data securely. This includes physical and technical measures, as well as organisational policies and appropriate protection against accidental loss, destruction or damage. As a health record all patient photography must adhere to local policies in relation to storage of clinical images regardless of who takes a photograph and for what purposes. Mobile phones present several risks from a data security perspective:

- Poor physical security; being portable, they can be easily lost or stolen.
- Low level passwords that are vulnerable to attack.
- They allow for easy distribution of images online and via Apps.
- Images taken directly on a phone are usually available within the phone’s gallery (Apps can prevent this and will be discussed later) and very often mixed with non-clinical images.
- They may be set up to automatically back up data to cloud storage. If cloud servers are located outside the European Economic Area (EEA), there are restrictions to how personal data can be transferred.

Freedom of Information / Subject Access Request (SAR)

Under Data Protection law, individuals have the right to access their personal data as well as the right to data portability. In order to facilitate a timely response to Freedom of Information (FOI) or Subject Access Requests (SAR), processes need to be in place that will allow clinical images to be retrieved and securely distributed. In most cases Data Controllers have one month to comply with SARs. Images held on personal mobile phones often have no audit trail, may be moved or deleted and therefore be unavailable or inaccessible at organisational level, and may prove difficult or impossible to track down and retrieve within this timeframe.

Example

A patient presents in the Emergency Department following a workplace accident. The attending doctor photographs the injury prior to treatment. Several months later the patient makes a Subject Access Request for the clinical images in connection with a personal injury claim being made against their employer. The images were never saved to the patient health record and the doctor has since moved on from the hospital. After going to great lengths to track the doctor down it is discovered that the phone had been lost and the images are no longer available. As data controllers both the doctor and organisation are in breach of data protection rules following the loss of personal data.
Data Processing

According to GDPR there is a distinction made between the collection of personal data and the processing of personal data; these roles are described as being that of data controller or data processor. The difference is an important one as legislation treats breaches by data controllers differently to data processors. Generally speaking an organisation, such as a hospital, will be considered to be the data controller but employees working within the hospital are also considered to be data controllers. It is also possible to be both controller and processor. It is important to consider how GDPR defines both roles:

A Data Controller determines the purposes and means of processing personal data. This includes:

- Deciding what personal data to collect.
- If that data can be modified.
- How the data is used.
- Whether to share the data.
- Whether to keep the data.

A Data Processor processes personal data on behalf of the controller.

- The processor is responsible for the security of the data they are processing and for informing the data controller of any data breach.
- A processor can be considered a data controller if they process data beyond the guidelines issued by the controller.

If an employee makes a decision to capture a patient image on their own device, if they share the image with others and if they delete or lose the image without having saved it to a hospital system, they will they be accountable as the data controller.

Data Sharing

Data sharing can be permissible under GDPR provided the new processing activity is in keeping with the original purpose for which the data was collected. Patient data may need to be shared between doctors on the clinical team or with another organisation for a second opinion or referral, but there remains an obligation on both parties, sender and receiver, to ensure that the data is secure at all times.

Sensitive data is required to be protected with additional secure measures. These extra measures include the use of encryption, anonymisation and pseudonymisation to reduce the possibility of identification in the event of unintentional data leaks. Photographs present a unique challenge to data security as images themselves can’t be pseudonymised and anonymisation can’t be guaranteed.
Instant Messaging Apps

Instant messaging Apps are designed to appeal to the general population and allow easy dissemination of multi-media content to many people simultaneously. Messages generally don’t incur any cost to users and as a result they have become the dominant communication tools used today. Within hospitals, studies have shown that these Apps are being used to communicate and to share patient data but they are not compliant with data protection legislation. WhatsApp, for example, uses end-to-end encryption on messages but saves the content on both sending and receiving devices, images are saved to phone gallery by default and while this feature can be turned off, it requires the user to actively make a decision to do so. Backups can also be enabled that will save all data to cloud services potentially sending data outside the EEA. There is no secondary authentication required to launch the App once the device is unlocked, meaning the content is available to anyone who has access to the device. From an organisational point of view, generic messaging Apps raise a number of questions:

• Does the App provide strong data protection?
• Is content hosted within the EEA?
• Are messages mixed with personal messages?
• Can the organisation block access to certain messages?
• Can the organisation control data shared in messages?
• Can the organisation recover data sent in messages?

There is also the broader issue of whether the software can be trusted to act in the manner claimed – numerous recent leaks have shown that data is a valuable commodity and is being collected at every opportunity by software providers and often without the explicit consent required.

Processing Clinical Images from Mobile Phones

As clinical image management specialists, medical illustration services should, and will be expected to, manage patient images that have been captured on mobile phones. These may be opportune images captured by other healthcare professionals, routine image captures as part of a telemedicine service, or images that patients have captured themselves and would like saved within their health record.
Quality Control

When processing images taken by non-clinical photography staff there is an opportunity to exercise some quality control over the images that are being taken. While it is not expected that these images will be of the same standard as those taken by a clinical photographer, it should be pointed out if they are not fit for purpose, e.g. out of focus or silhouetted. In such circumstances a note should be made to indicate that the images were not deemed suitable as a clinical health record. It may also be possible to arrange for quality clinical images to be made by a clinical photographer. If that is not possible, it still provides an opportunity to remind the image taker that a high-quality clinical photography service is available at the hospital.

With telemedicine images there is added significance to the quality of the images involved – if a patient is being referred to, or triaged by, a hospital consultant there is an expectation that the images provided are of sufficient quality in order for them to perform this function. If consistently poor quality images are being provided from the same source, then it is recommended that training be provided by a qualified and registered clinical photographer in order to improve the chances of the images meeting the required standard.

It is also recommended that the source of the images be clearly marked whenever non-medical illustration staff take a photograph, to avoid any suggestion that the department is responsible for the poor quality of particular images.

Consent

Local consent policy should be followed at all times regardless of who has taken a photograph. Clinicians should be reminded of the legal requirements with regard to proper informed consent and the options available to document consent. When a patient has provided an image of themselves, the person receiving the image should obtain consent in line with local policy.

Data Security

Once an image has been transferred to a medical illustration service to be stored in a health record or image management system, it should be deleted from the device it was created on. Patients providing their own images are unlikely to want to delete them from their devices so it is worthwhile providing a statement that the medical illustration service cannot guarantee the security of images that exist on devices external to the image management system i.e. if a patient or clinician loses their phone and an image finds its way into the public domain, the medical illustration service has no responsibility over those images.
Penalties

As Data Controllers, hospitals are extremely exposed to the risks of employees using their own mobile phones to take images. This practice will inevitably lead to data breaches and instances of non-compliance with GDPR have the potential for significant fines. There are several criteria used when calculating the fines involved, but multiple episodes of the sharing of sensitive data through non-secure platforms is likely to be considered in the upper level of infringement and will attract a significant fine.

Mobile Phone Apps

Mobile phones have developed into multi-platform computing devices and through the development of Apps they now have an ever-increasing range of functions. The speed at which Apps are evolving makes it very difficult to predict which ones will still be relevant in the months and years ahead, but properly designed and configured Apps will allow for safe use of mobile devices in the clinical setting.

From a clinical photography perspective there are dedicated clinical imaging Apps which include WABA Medical Pics (WMP), a Secure Clinical Image Transfer (S.C.I.T) and Clinical Uploader, all designed to capture patient images and facilitate uploading of the images to image management systems. GDPR introduced a new concept of data protection by design – the idea behind this measure is to put an emphasis on protecting personal data as a core feature when designing a new product or process, as opposed to it being something that is accommodated at a later stage. The clinical imaging Apps listed above deliver on this, providing a solution to use mobile technology securely while remaining compliant with all relevant legislation. As technology continues to evolve and new products emerge, we need to ensure Apps for clinical photography meet the following standards:

- The ability to connect to a hospital image management system;
- A separate login when accessing the App on a mobile device;
- A timeout feature that prevents the App from being left open indefinitely;
- Operate in a way that facilitates subject access request;
- A function to record patient consent.
Summary

Mobile phones have the potential to change the manner in which healthcare is delivered, but they do present a number of challenges from an information governance perspective.

While it is understood that in exceptional circumstances a personal phone may be needed to capture a patient image in situations, where a service is designed around the use of a mobile phone for clinical photography e.g. telemedicine, then appropriately secure and configured devices are essential.

Detailed policies are needed to ensure compliance with data protection regulations.

IMI recommends that the use of mobile phones be managed proactively and with the following guidelines:

• Mobile phones should only be used in exceptional circumstances to capture clinical images.

• Where mobile phones are deemed to be a regular requirement, e.g. telemedicine, properly configured devices are recommended.

• Patient data should never be stored on mobile devices.

• App back-ups should be configured to a secure hospital server.
## Glossary

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>BYOD</td>
<td>Bring your own device, e.g. a privately owned mobile phone</td>
</tr>
<tr>
<td>Consent</td>
<td>Permission from data subject for how personal data may be processed</td>
</tr>
<tr>
<td>Data controller</td>
<td>A person, company or body which determines the need to collect and how to process personal data</td>
</tr>
<tr>
<td>Data Processor</td>
<td>A person, company or body that processes personal data for a controller</td>
</tr>
<tr>
<td>DH</td>
<td>Department of Health</td>
</tr>
<tr>
<td>DPA</td>
<td>Data Protection Act 2018</td>
</tr>
<tr>
<td>DPC</td>
<td>Data Protection Commissioner (Republic Of Ireland)</td>
</tr>
<tr>
<td>EEA</td>
<td>European Economic Area</td>
</tr>
<tr>
<td>Encryption</td>
<td>Coding or scrambling of information into cipher text using cryptography technology and a decoding key is required to decode the information</td>
</tr>
<tr>
<td>FOI</td>
<td>Freedom of Information</td>
</tr>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
</tr>
<tr>
<td>HSE</td>
<td>Health Service Executive (Republic of Ireland)</td>
</tr>
<tr>
<td>ICO</td>
<td>Information Commissioner’s Office</td>
</tr>
<tr>
<td>IMI</td>
<td>Institute of Medical Illustrators</td>
</tr>
<tr>
<td>PID</td>
<td>Patient Identifiable Data</td>
</tr>
<tr>
<td>ROI</td>
<td>Republic of Ireland</td>
</tr>
<tr>
<td>SAR</td>
<td>Subject Access Request</td>
</tr>
<tr>
<td>Sensitive Data</td>
<td>Data relating to religious or other beliefs, sexual orientation, health, race, ethnicity, political views, trades union membership, criminal record</td>
</tr>
<tr>
<td>Smartphone</td>
<td>Mobile phone built on a mobile operating system with internet connectivity and advanced computing capability</td>
</tr>
</tbody>
</table>
References


6 Medialogix. *Clinical Uploader App*. Available from: [www.medialogix.co.uk](http://www.medialogix.co.uk) [Accessed October 2019].
Bibliography


Lead Author

Anthony Edwards
Senior Clinical Photographer
St James’s Hospital
P.O. Box 580
James’s Street
Dublin 8

Working Group

Jane Tovey
Medical Illustration Services Manager
University Hospitals Birmingham NHS Foundation Trust
Birmingham B15 2GW

Lisa Fisher
Formerly Head of Medical Illustration
South Tees Hospitals NHS Trust