UK GUIDANCE ON THE USE OF MOBILE PHOTOGRAPHIC DEVICES IN DERMATOLOGY

Acknowledgements

This document is a supplement to *Quality Standards for Teledermatology: Using 'Store and Forward' Images* (available here http://bit.ly/2gSEJVo), which was published in 2013, itself as a supplement to *Quality Standards for Dermatology: Providing the Right Care for People with Skin Conditions*, published by Primary Care Commissioning in 2011 and available at http://bit.ly/VayyN2.

As with the earlier standards, this work has been developed with the support and commitment of the project working group, which comprises key stakeholders including the British Society of Teledermatology, the British Association of Dermatologists (BAD), Scottish dermatologists, the British Dermatological Nursing Group (BDNG), the Primary Care Dermatology Society (PCDS), patients and patient organisations (the Psoriasis Association and Nottingham Support Group for Carers of Children with Eczema), Medical Illustration (University Hospitals Bimingham NHS Foundation Trust) and a GP.

We are also extremely grateful to all those who offered expert advice and feedback in response to the consultation. In particular we would like to acknowledge the input and comments from the General Medical Council (GMC), the Information Commissioner's Office (ICO) and the Information Governance Alliance (IGA).

Financial support has come from the British Association of Dermatologists (BAD), the British Dermatological Nursing Group (BDNG) and the Primary Care Dermatology Society (PCDS).

Contents

Published July 2017

Foreword from Nick Levell, President of the British Association of Dermatologists

I am delighted to introduce this publication, which is the result of dedicated work by a range of stakeholder groups from both within and beyond the speciality of dermatology. Perhaps because dermatology is such a visual discipline, it has been at the forefront of work around the use of images in clinical care and is one of the first specialties to tackle the particular opportunities and challenges presented by the growing use of mobile photographic devices in medicine.

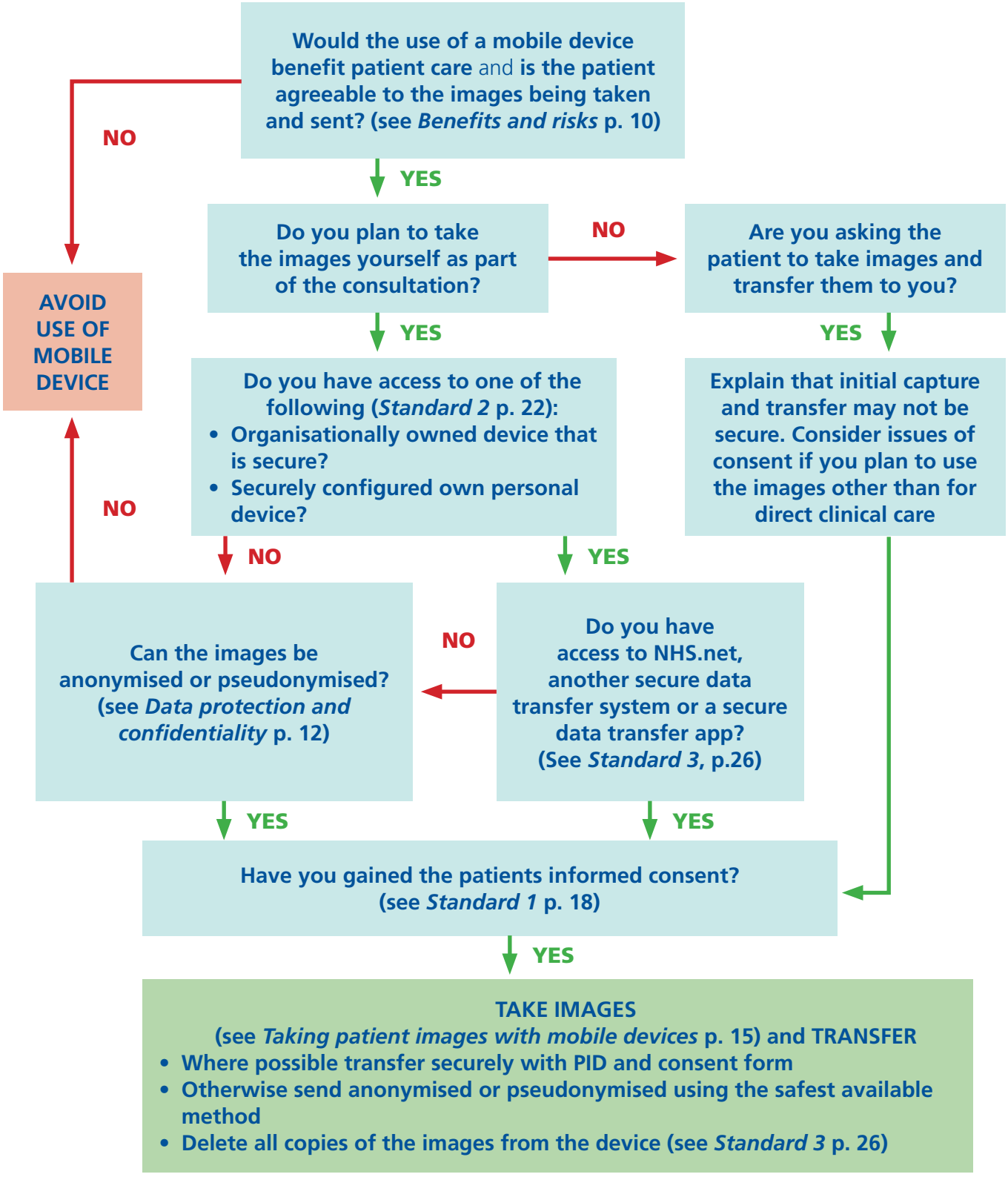
The importance and value of this guidance will, I think, continue to grow as a new generation, used to receiving instant answers to their questions via mobile devices, reaches adulthood. This generation sees mobile technology as second nature and will expect doctors to use it safely and skilfully in order to help their patients get the best medical care. For example, the growing trend towards multi-disciplinary team working, with virtual team meetings and sharing of clinical images is often supported by teledermatology, and teledermatology increasingly depends on clinicians' use of mobile photographic devices.

The safe and secure transfer of images supported by full clinical information allows patients to receive expert opinions from around the UK without risk to their personal data. It is also likely that the uses for clinical images will continue to grow as technology develops and mobile use by clinicians becomes ever more widespread. An obvious example might be in the reduction of 'never events' due to wrong site dermatology surgery.

Finally, I believe that much of this guidance will be of value within other clinical areas and in the wider health service – not just for other specialities but more broadly for organisations seeking to develop their own policies around the safest and most expedient use of mobile devices to capture and transmit clinical images.

Nick Levell, President of the British Association of Dermatologists

FIGURE 1: SUMMARY for healthcare professionals using mobile devices



Executive summary

This guidance supplements the standards outlined in *Quality Standards for Dermatology: Proving the Right Care for People with Skin Conditions* (PCC, 2011) and those added in *Quality Standards for Teledermatology: Using 'Store and Forward' Images* (PCC, 2013). It applies wherever mobile devices are being used to capture and transfer patient images and has been written to support the safe use of mobile devices by healthcare professionals for patient care. It explains the risks and benefits of using mobile devices, particularly in relation to information governance.

Ideally, clinical photographs should be taken by experienced medical photographers in medical illustration departments. However, mobile devices are increasingly being used to take clinical images, particularly in settings where medical illustration services are not readily available, such as community/primary care services. Also, patients are keen to take and share clinical pictures. These changes offer potential benefits to patient care but it is important that healthcare professionals have a clear understanding of their responsibilities when capturing and transferring such images.

This document has two sections. The first half provides guidance in three key areas and the second half sets out clear standards for healthcare professionals. An explanation of the key terms used can be found on pp.5–6.

GUIDANCE

1: The benefits and risks of using mobile devices

Benefits

- Where medical illustration services are not available or not practical to use, mobile device photography can be helpful by providing useful additional information for the patient record, thereby potentially improving patient care.

Risks

- Patient-identifiable clinical images could inadvertently be shared through social media or via the internet, for example, or copied to cloud-based backup services without the device owner's knowledge.
- Patient care might be compromised if images are of poor quality.

2: Data protection and confidentiality

- Images captured and stored on a mobile device are potentially insecure if there is inadequate password protection or excess connectivity. This has implications for images containing patient-identifiable data (PID).
- Where security cannot be guaranteed during data transfer, the General Medical Council (GMC) and Information Commissioner's Office (ICO) both suggest ways in which data can be made non-identifiable (through anonymisation or pseudonymisation).
- There are also dedicated apps available to handle clinical images securely on a mobile device.

3: Taking patient images with mobile devices

A clear understanding of the device's capabilities and features is important. This section includes a range of basic tips that can improve image quality when using a mobile device.

STANDARDS

1: Gaining the patient's informed consent

- Consent should always be sought before capturing a patient image.
- It is the healthcare professional's responsibility to give the patient clear information on the risks and benefits of using an image captured on a mobile device – without this there is no informed consent.
- Written consent is recommended, preferably using a standardised consent form that covers use in direct care and also allows for consent to use the image for teaching and wider dissemination, ie on the internet.

2: Safe use of mobile devices to take patient images

Any device that is being used to capture clinical images that will not be either anonymised or pseudonymised should, as a minimum, have:

- a strong passcode (6+ characters)
- data encryption enabled
- any cloud-based backup systems disabled before use.

Some trusts may supply dedicated devices or operate a clear 'bring your own device' (BYOD) policy. This is the approach recommended by the ICO and this document should form part of such a policy and/or be used in the process of developing one.

In the absence of a clear BYOD policy the risks to personal data are greater and, in consequence, healthcare professionals may wish to consider installing a secure clinical image transfer app to keep PID images completely separate from their own use of social media or cloud-based storage.

Where patients use their own devices at the request of a healthcare professional, the security risks should be fully explained and consent sought in the usual manner.

3: Safe transfer and storage of images captured with mobile devices

If the healthcare professional is transferring data that is identifiable then it is important to ensure it arrives securely at the right destination for storage and use. It should not be vulnerable to interception or redirection but should be protected in line with the Data Protection Act (1998) (DPA). This can be achieved by sending encrypted data as follows:

- via email using NHS.net or *to* NHS.net similar secure NHS systems;

  or

- by downloading to a secure (preferably NHS) wifi network or by cable to a PC that acts as a conduit to a secure network server and not as a storage device;

  or

- by means of a secure clinical image transfer app.

When this level of security cannot be guaranteed, the use of anonymised or pseudonymised data may be a pragmatic solution.

It is important that images are *completely* deleted from the mobile device once transferred and that the storage system holding PID is encrypted/password protected, searchable, regularly backed up and held within England, Scotland or Wales, as appropriate.

Introduction

Photographs are very useful in conveying clinical information and showing how conditions change over time. Some hospitals have medical illustration services with expertise in all aspects of image acquisition and handling, and wherever possible these professional services should be used. However, in hospitals where they are not available, across the wide range of community-based services and in emergency situations, mobile devices have become an increasingly popular, flexible tool for supplementing the visual record. Local and national surveys have shown that over half of secondary care doctors have used their personal smartphone to take clinical photographs of patients[1, 2] and the practice appears to be widespread in primary care. In addition, patients are generally comfortable with the use of mobile devices by healthcare professionals[3] and are often keen to share photographs taken on their own mobile devices where they feel it will improve care.

This guidance outlines how healthcare professionals can use mobile devices and images that have been captured on them in a confidential and secure manner and in a way that balances clinical effectiveness, safety and ease of use. It is intended as a resource for healthcare professionals in primary and secondary care.

What is covered by this document

This document supplements an earlier publication *(Teledermatology: Using 'Store and Forward' Images)*.[4] It addresses the increasingly widespread use of mobile photographic devices in healthcare in order to ensure that healthcare professionals fully understand:

- the circumstances in which the use of mobile devices to capture and transfer images may be appropriate;
- the risks and benefits associated with the use of mobile devices in this way;
- how best to mitigate these risks and explain them to patients when seeking informed consent;
- the concept of anonymisation/pseudonymisation as a pragmatic solution where secure transfer of images cannot be guaranteed.

The aim overall is to offer realistic and practical guidance for instances where the use of mobile devices is appropriate and to set standards that ensure patient safety and data security are maintained.

Terminology

Key terms are given below with an explanation of their use in this document.

MOBILE DEVICE: a portable electronic device that can be used to take photographs/capture digital images, such as mobile phone, tablet, camera with internet connectivity.

IMAGE: the photograph taken on a mobile device.

DATA: the information being held on or transferred from a mobile device. Images are one form of data and the terms are broadly interchangeable for the purpose of this guidance.

SECURE: refers to the safe processing of individuals' personal data under the terms of the Data Protection Act (1998) (DPA),[5] which is the legal framework overseen by the Information Commissioner's Office (ICO) that regulates the processing of **patient-identifiable data** about living individuals in the UK. Secure data is protected from unwanted dissemination and from the eyes and actions of unauthorised users.

SECURE CLINICAL IMAGE TRANSFER APP: a specially designed application that can be used to make mobile devices secure for use with clinical images. They typically encrypt images prior to transfer, automatically send them to a secure NHS

storage system and delete them after transfer without allowing the images to be copied to a cloud-based storage system. These apps are increasingly being developed and used because they resolve the security issues around sending **patient-identifiable data**. They are being developed and marketed by referral management and other healthcare providers, including some medical illustration departments.

PATIENT-IDENTIFIABLE DATA (PID): anything that could link the image to an identified patient. This could include a name or hospital number, for example, if these appear on the image or in a separate image in the same set and transferred as a single package, eg a photo of the patient consent form sent alongside a clinical image. It also applies to images that show the face or any identifying marks on the body. PID is subject to data protection requirements and should be transferred only through secure, organisationally approved methods.[6] (To avoid using PID, in circumstances where secure transfer may not be available, you can **anonymise** or **pseudonymise** data.)

ANONYMISED DATA: (see also **pseudonymised data**): neither contains nor is attached to anything that would identify the subject of the image, ie name or hospital number, consent form containing this information, etc. Anonymised data, because it cannot be linked to a person, is exempt from data protection requirements and may be transferred in ways that would not be considered secure for **patient-identifiable data**. The problem with completely anonymised data is that it relies solely on the sender remembering the original source and subsequently linking the image and the response to the correct patient record. This risk of data being lost to the patient record can usually be overcome by using **pseudonymised data**.

PSEUDONYMISED DATA: (see also **anonymised data**): personal data is considered to be pseudonymised when processed in such a way that it can 'no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'.[6] This means that the data is processed in a way that is non-identifiable, the additional information is kept separate and the key or code to reveal the identity of the subject is known only to the two healthcare professionals involved in the transfer. Usually an artificial identifier is added to the data in place of name or hospital number in a system agreed between the sender and receiver of the image, so that it cannot be re-identified until the transfer is complete and the image is safely held at its secure destination. Effectively pseudonymised data can be transferred in the same way as anonymised data, using non-secure methods if necessary, but can be re-identified and captured on the patient record, with associated benefits for patient care. Pseudonymisation can be a pragmatic approach in circumstances where secure transfer methods are not accessible,[7] but it should always be borne in mind that the EU General Data Protection Regulation (GDPR) considers pseudonymised data to be personal data.

References

1 Alexander H. and Halpern S. 'The use of mobile devices by medical staff to image patients in a district general hospital setting', Br J Dermatol 2015, 173(suppl. S1): 181–183.

2 Alexander H. and Halpern S. 'A study evaluating the use of smartphones to photograph patients by UK dermatologists', Br J Dermatol 2016, 175(suppl. S1): 188–190.

3 Soriano LF, Jolliffe V, Sahota A. Smartphones in the dermatology department – acceptable to patients? Br J Dermatol. 2017 Mar 24. doi: 10.1111/bjd.15492. [Epub ahead of print] PubMed PMID: 28338227.

4 PCC (2013) *Quality Standards for Teledermatology: Using 'Store and Forward' Images*. (Available at http://bit.ly/2gSEJVo).

5 Data Protection Act (1998) London. HMSO. (Available at http://bit.ly/18Er0gh).

6 EU GDPR 2016/679, Article 4(5). (Available at http://www.privacy-regulation.eu/en/r32.htm).

7 Information Commissioner's Office (ICO) (2012) *Anonymisation: Managing Data Protection Risk Code of Practice*. (Available at http://bit.ly/1RPK2Wm).

Guidance

The guidance section explains the issues that are relevant for a healthcare professional using a mobile device to capture and transfer patient images. It is important to understand these issues in order to ensure clinical images are captured and handled in a way that is clinically appropriate, legal and useful.

Guidance

The benefits and risks of using mobile devices

The decision to use a mobile device to capture, store and transfer images for patient care should be an informed one, made with a full understanding of the potential risks and benefits and with the best interests of the patient in mind. Whatever the scenario or care setting it is the responsibility of the healthcare professional to assess the risks and benefits and to explain them clearly to the patient.

Benefits

Mobile devices are smaller and more portable than conventional cameras and are capable of providing high-resolution images to the standard required for teledermatology. Where professional medical illustration services are not available or are not practical the availability of a mobile device can contribute to timely access to services, optimisation of patient care and accuracy of the patient record.

The following examples show scenarios in which the use of a mobile device might be in the best interests of the patient:

- For patients' home monitoring of chronic diseases or to provide information to supplement a face-to-face consultation if, for example, a rash flares and fades or the presentation of a lesion changes.
- In a primary care/community setting to save an elderly person a trip to hospital or as part of hub-and-spoke dermatology services.
- For triage to supplement written referral or allow advice and guidance.
- To facilitate capture of specific images during a physical examination, eg clinical and dermoscopic images of pigmented lesions as required by the National Institute for Health and Care Excellence (NICE) guidelines for melanoma and for monitoring of atypical naevi.[1]
- To improve access to an urgent dermatology opinion.
- To facilitate discussion and advice about clinical cases between junior and senior colleagues, provide material for teaching/research and support the spread of expert knowledge across a clinical network.
- For collection of photographic evidence of a patient's condition in an acute and changing situation, eg evolving emergency dermatoses.
- To provide images of investigation results to supplement clinical information for discussion and to facilitate assessment.

Risks

The risks fall broadly into two categories – those relating to quality of care (ie where poor image quality impedes accurate diagnosis or management) and risks to data protection and patient confidentiality (eg through patient-identifiable images being made widely available through photo-sharing or shared on inappropriate platforms). It is the responsibility of the healthcare professional to explain any risks to the patient and seek their informed consent as outlined in **Standard 1**.

Risks to patient care

1 A photograph, however good the quality, can never match the patient being seen in a clinical consultation.

2 Photographs taken on a standalone camera by someone trained in medical photography will be to a high and consistent standard with optimum resolution, which is typically not achieved with a mobile device. In addition, images taken by patients may not capture all the relevant parts or aspects of a skin condition.

3 As with any technology, digital devices are subject to accidents, damage and malfunctions, with the risk of data loss.

4 Images captured on mobile devices – particularly on patients' own devices – could be inadequately, inaccurately or unclearly annotated, which means they could fail to be linked with the appropriate patient record.

5 Where images are pseudonymised there is a risk that the patient data and image are not united when received, or are wrongly paired. This would result in no data – or the wrong data – being attached to the patient record. It could also mean that a clinical question is misinterpreted or goes unanswered.

Risks to data protection and patient confidentiality

1 Most mobile devices have internet connectivity and use cloud-based backup services. This means there is potential for patient images to be rapidly and widely circulated via the internet or to appear on image-sharing social media sites such as Facebook. For guidance on how to ensure the equipment used is secure, see **Standard 2**.

2 Mobile devices are more susceptible to loss or theft, especially if used both at work and at home. If the device is not adequately password-protected with the appropriate level of security patient images could be illegally or inappropriately accessed (see **Standards 2 and 3** for further guidance).

3 Mobile devices are not suitable for long-term storage of patient images, so any images used for clinical decision-making or patient monitoring must be transferred to secure central storage which is accessible as part of the patient's healthcare record and then deleted from the original device. (See **Standard 3** for guidance on secure transfer between colleagues or NHS institutions using mobile devices.)

4 Images transferred from a mobile device using a method of data transfer that does not meet NHS Digital standards of encryption are not necessarily secure. See **Standard 3**.

5 Anonymised or pseudonymised images could still be global positioning satellite (GPS)-located/tagged or could include other factors that risk revealing the patient's identity, eg date, diagnostic category etc.

6 Images may still be accessible after apparent deletion from a mobile device and/or after the mobile device has passed out of use. See **Standard 3** for guidance.

When patients capture and transfer their own images

This constitutes a non-secure transfer unless the phone has the capacity to encrypt files before sending. Likewise any images patients take and hold on their own phones may not be secure. It should be noted that, where the patient has chosen to capture and transfer the images, issues of device usage/transfer and data protection/information governance are not relevant until the image has been received by the healthcare professional (but see also **2.1.4.2**).

Once the image has been received by a healthcare professional, any onward data transfer and storage should meet NHS data protection and information governance requirements.

Issues of consent will differ and will relate to any onward transfer, storage and use of the images once they have been received.

References

1 NICE (2015) Melanoma: assessment and management [NG14] (http://bit.ly/2sdpnjW).

- In order to minimise any risk to quality of care, images must be of sufficient quality to be useful for safe and effective care and should be identifiable and available as part of a patient's health record.
- Patient privacy and confidentiality are potentially at risk when using mobile devices. For this reason, equipment used for image capture and methods of image transfer must be secure and patients must be advised of the risks of using non-secure methods of image transfer to receive or send images from their own devices.
- Where secure image capture and transfer cannot be assured, anonymisation/ pseudonymisation, should be considered.

Data protection and confidentiality issues

Without care the use of mobile devices to take, store and transfer images can lead to breaches of patient confidentiality and of the Data Protection Act (1998) (DPA).[1] Patients should feel assured that any personal information held by a healthcare professional will be held in confidence. This is the principle of patient confidentiality and the General Medical Council (GMC) has published guidance about how this is best achieved.[2] The use of mobile devices by healthcare professionals to take and send images needs to take account of the GMC guidance and the DPA wherever the image is linked to patient-identifiable data.

The DPA requirements

In order to comply with the law and with related guidance, all patient-identifiable data (PID) comes under the terms of the DPA and must be handled securely. The guidance on risks and benefits has indicated situations where the use of mobile device technology could potentially breach the DPA and **Standards 2 and 3** set out the best practice requirements for secure capture, storage and transfer of images containing PID.

It is inevitable that sometimes patient care dictates the need for image capture and transfer using a mobile device in circumstances where it is not possible to follow best practice. In order to avoid exposing PID to insecure storage or transfer, both the GMC and Information Commissioner's Office (ICO) have provided advice about using anonymised or pseudonymised data to avoid compromising patient confidentiality.

Anonymisation and pseudonymisation

The GMC and ICO make clear that in the absence of PID (where there is so-called 'anonymisation' or 'pseudonymisation'), issues of data protection become less relevant. Anonymised data is not linked to an individual and is therefore not subject to the DPA. Data protection law continues to apply to pseudonymised data, but the risks to patient confidentiality are much reduced.

ANONYMISED DATA neither contains nor is attached to anything that would identify the subject of the image and cannot therefore be linked to a person.

PSEUDONYMISED DATA is personal data processed in a way that renders it non-identifiable without the addition of separately and securely held information that can be securely transferred between the healthcare professionals sending and receiving the data.

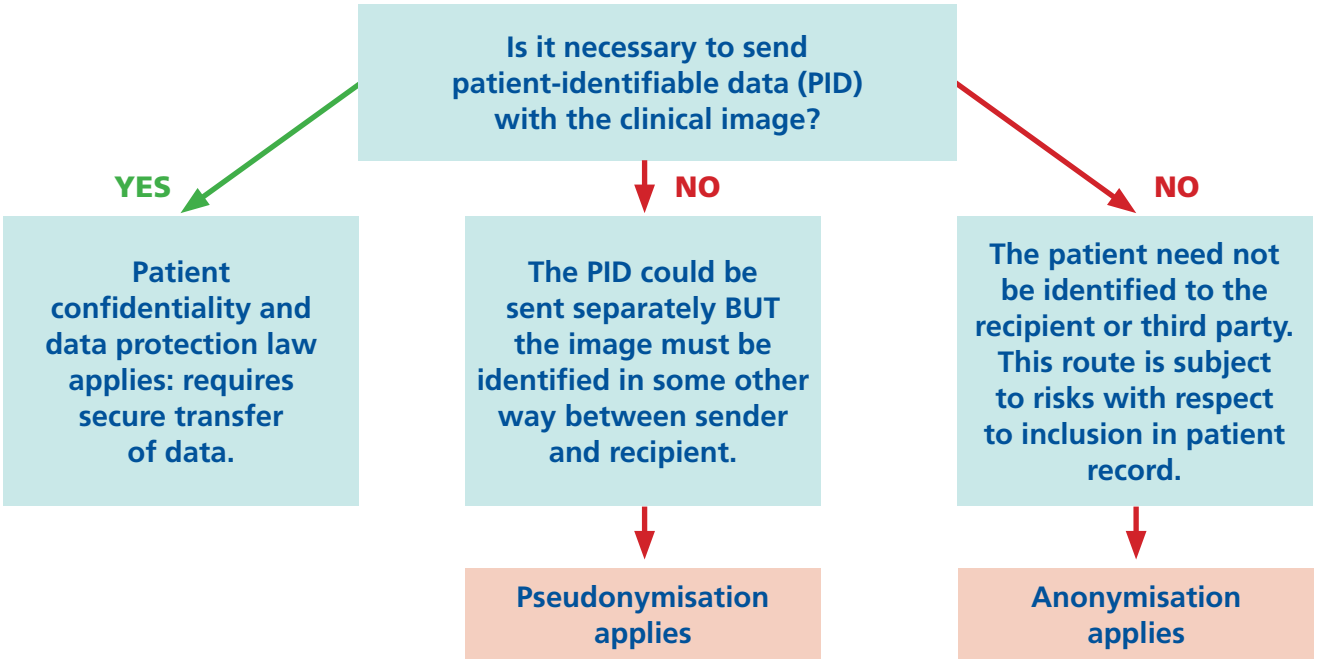
The 2017 GMC guidance around confidentiality states as the first of its eight principles:

> Use the minimum necessary personal information. Use anonymised information if it is practicable to do so and if it will serve the purpose.[2]

The ICO cites the reference to anonymisation in European data protection law (Recital 26 of the European Data Protection Directive 95/46/EC) which:

> makes it clear that the principles of data protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.[3]

FIGURE 2: Patient confidentiality and data protection



It should be noted that where pseudonymised images are sent and received it is the responsibility of the healthcare professionals who send and receive them to have a clearly agreed system that will ensure that the correct image links to the correct patient.

Image transfer and data protection/confidentiality: balancing the risks

If the healthcare professional wishing to transfer data is in a setting where secure transfer of clinical data cannot be assured, then there is a need to balance the risk of anonymising or pseudonymising the data with the risks of transferring PID non-securely. This is in the context of the best interests of the patient, their care and the role that the images might have in improving that care.

As a general rule, the higher the risk attached to the method of transfer, the lower risk the images should be. For example, a high-risk method of transfer indicates use of an anonymised/pseudonymised image, whereas an image that cannot be anonymised (ie a full-face image or one showing a tattoo) should be transferred only via a secure (low-risk) method. Various scenarios are suggested and graded in terms of risk in Figure 3.

The GMC has also produced guidance on making and using visual and audio recordings of patients[4] and healthcare professionals should be aware of this.

References

1 Data Protection Act (1998) London. HMSO (available at http://bit.ly/18Er0gh).

2 GMC (2017) *Confidentiality: Good Practice in Handling Patient Information* (pdf, available at http://bit.ly/1cxf5Dd).

3 ICO (2012) *Anonymisation: Managing Data Protection Risk Code of Practice* (pdf, available at http://bit.ly/1RPK2Wm).

4 GMC (2011) Making and using visual and audio recordings of patients (http://bit.ly/1kYn7r1).

FIGURE 3: Mobile device risk levels by image type and method of transfer

Risk level	Image type
LOW	• Close-up image showing no identifying features • No patient-identifiable data (PID) sent (ie anonymisation of data) or an artificial identifier accompanies the data and/or PID is sent separately by secure means (ie pseudonymisation of data)
MEDIUM	• Medium-distance body shot showing no face or other identifying features (eg tattoos) • No PID sent (ie anonymisation of data) or an artificial identifier accompanies data and/or PID is sent separately by secure means (ie pseudonymisation of data)
HIGH	• Full-face image of patient, with or without PID • Images that include identifiable tattoos, genitalia, breasts • Copies of written information and/or scans/X-ray images containing patient data

Risk level	Method of transfer
LOW	• Use of specialist secure clinical image transfer app to encrypt the data, link to a secure image management system and ensure no trace of the image remains on the device • Use of secure device with password-protected encrypytion software and connectivity with cloud-based storage and social media disconnected, sent via an NHS.net secure email address and image fully deleted after transfer
MEDIUM	• Sending an anonymised (no PID) image for advice only • Sending a pseudonymised image (with artificial identifier accompanying the image and/or PID sent separately by secure means)
HIGH	• Sending an unencrypted image with PID from one NHS.uk email address to an NHS.uk email address in a different organisation, or to an NHS.net address
VERY HIGH	• Sending any image with PID using a non-NHS email address • Sending any image with PID via a messaging app (even one that purports to be secure)

- PID falls under the Data Protection Act (DPA) (1998) and must be treated accordingly.
- Anonymised data and securely pseudonymised data do not require the same levels of secure transfer as they are not linked to an individual.
- Pseudonymised data, once re-identified and linked to the correct patient record, then becomes PID and is subject to the usual protection, as does anonymised data if it is subsequently identified and attached to the patient record.
- Secure image transfer apps, provided suitably tested, can remove the need to anonymise or pseudonymise data.

Taking patient images with mobile devices

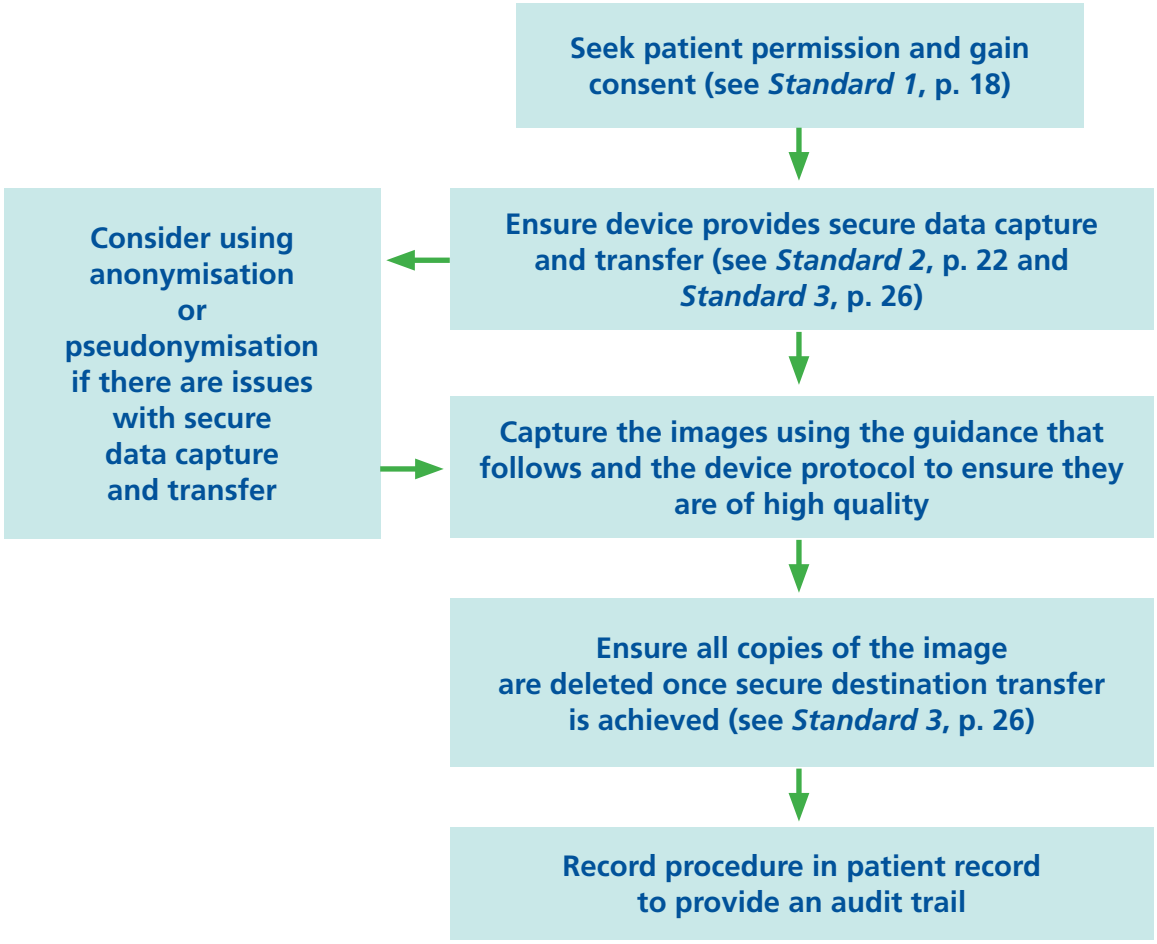
Where images are taken in the interests of clinical care they form part of the patient record and are potentially legal documents. Poor-quality images cannot support accurate decision-making and may hinder diagnosis and patient care. It is therefore of paramount importance that wherever it is deemed in the patient's best interests to use mobile devices for image capture, every effort is made to achieve optimal quality. All mobile devices are different and image quality varies. The following basic tips can increase the chance of sharp, clear images that are fit for purpose.

Tips and information on using mobile devices for clinical photography

- **DEVICE AGE AND SPECIFICATION** – will determine whether the images captured are of sufficient quality for diagnostic purposes.
- **FLASH** – usually produces a sharper image with higher contrast and better colour consistency, but keep your distance – flash used too near the subject will bleach out the image.
- **FRAMING** – take a selection of images – a distance image that includes a known anatomical landmark as well as close-ups.
- **FOCUS** – allow time for the camera to engage its auto-focus facility.
- **SCALE** – magnification/distances are not set on a mobile device camera, unlike a digital SLR camera, so it is important to include a scale measure, such as a ruler, in the shot so that views can be repeated and more accurately compared. Scales which contain a colour control patch to indicate variations in skin tones could be a useful addition.
- **PROCESSING FEATURES** – some mobile devices incorporate on-board image processing, such as 'high dynamic resolution' (HDR) and automatic post-capture adjustments. Take time to understand your device and review the settings prior to use for clinical photography.
- **DERMOSCOPIC ATTACHMENTS** – these are available for some mobile devices and are useful for photographing skin lesions. If comparing dermoscopic images remember that ideally you should compare images taken on the same device. Where attachments are available, use of polarised and non-polarised dermoscopy is recommended.
- **SELECTION** – retain all images that are clinically and legally relevant and make patients aware that suboptimal images will be deleted.
- **TIME-DELAYED SHUTTER ACTIVATION** – can sometimes help avoid camera shake.

Issues of device ownership and connectivity are crucial for secure storage and transfer of images. It is important to understand these before using a mobile phone to capture clinical images. For full information see **Standard 2**.

FIGURE 4: The process of using mobile photographic devices in dermatology – summary for healthcare professionals



Standards

The standards that follow give recommendations each underpinned by a clear rationale. They set out the responsibilities of the healthcare professional with regard to patient clinical images captured on a mobile device. They cover the process from seeking initial patient consent to deleting the images from the device once they have been securely transferred.

Standard 1: Gaining the patient's informed consent

This standard considers informed consent with reference to images that are captured, transferred, viewed and stored using mobile devices. It assumes an understanding of the general principle of informed consent and related issues of competence as outlined in the relevant literature and of their application to teledermatology using non-mobile devices.[1, 2]

Consent in brief[3]

- Consent should always be sought before capturing a patient image.
- Written consent is best and use of a standardised consent form is recommended.
- Written consent is particularly important regarding use of patient-identifiable images for education and teaching beyond the patient's direct care and for any images used in widely disseminated media, ie the internet.
- All consent should be informed and it is the healthcare professional's responsibility to give the patient clear and balanced information and to document that this has been done.
- Patients may withdraw their consent at any time.

1.1 Recommendations

1.1.1 The principle of consent

Any interaction between a patient and a healthcare professional is subject to informed consent being given by the patient.

Rationale

Rational, informed consent is a legal requirement.[4]

1.1.2 Written consent for taking images should be obtained whenever possible

Written consent using a standardised consent form (see **Appendix A**) enables the healthcare professional to undertake a routine approach to the capture and use of images on a mobile device. It ensures that the patient has the opportunity to consider the points necessary to provide informed consent. The consent form will define the level of consent with respect to the future use of the images. Healthcare professionals may wish to develop accessible information to provide to patients to support the consent process.

Exceptions to the use of written consent may include instances when verbal consent is given and the image is for medical records/expert diagnosis only or where it is not possible to gain consent in writing and it remains in the best interest of the patient to take the images. In cases where written consent is not possible due to lack of capacity, consent for future use would not extend beyond direct provision of care for the patient in question. Where verbal consent is given, the healthcare professional should document this.

The EU General Data Protection Regulation (GDPR), which comes into force in May 2018, states that 'Consent should be given by a clear affirmative act establishing a freely given, specific, informed and unambiguous indication of the data

subject's agreement to the processing of personal data relating to him or her, such as by a written statement, including by electronic means, or an oral statement'.[5]

The GMC advises that the patient's consent, which should usually be written, should be obtained before making a recording that will be used in widely accessible public media (television, radio, internet, print), whether or not the patient will be identifiable.[6]

1.1.2.1 Consent for transfer and use of non-patient-identifiable images

Although images of patients considered to be non-identifiable (because anonymised or pseudonymised) may be considered less vulnerable to breaches of privacy and confidentiality, consent to record, transfer and use such images must still be obtained.

Rationale

Whatever the context in which medical decisions are made, the clinician must work in partnership with the patient to ensure good care.[7] *People have the right to be involved in discussions and to make informed decisions about their treatment and care.*[1,8] *Documented signed consent is evidence that a discussion took place concerning taking and using of images. It is an opportunity for patient and clinician to pause and consider the broader implications of taking images and using a mobile device.*

1.1.3 Recording and storing patient consent

Wherever practicable the signed consent form or documentation of verbal consent should be held with the patient record or transferred to the electronic patient record (EPR) as appropriate.

Ideally, an image of the documented consent or electronic file with consent details will accompany the image set for a clinical episode, but where anonymised or pseudonymised images are used the consent form should, of course, be transferred separately.

Rationale

The mobile device may be used as a means of recording patient consent, documenting the level of consent given and the identity of the patient. However, this also means that the image set has no anonymity as a single package in transfer. This has implications for secure transit and storage, irrespective of the anonymity of the images themselves.

1.1.4 Information for patients about mobile devices

In order that patients can give informed consent, the healthcare professional should provide the relevant information in a way the patient can understand (including in special formats for those who need them, ie non-English speakers or patients with sight or hearing problems). The information should include:

- whose device it is and how it is protected, what will happen to the images on the device;
- what images will be taken;
- what information will be sent with the images;
- how the images are transferred;
- to whom they are sent and what the receiver will do with the images and any accompanying information;
- that the images will be stored as part of the clinical record in line with local records retention policies and who will have access to them;
- an explanation for the patient that withholding or withdrawing consent for images to be taken will not affect their rights as a patient but may influence management of their care.

Rationale

A mobile device has great utility for the patient and their management, but there are important considerations with respect to the handling of their personal data, its storage and subsequent uses.

How you might speak to a patient about capturing an image on a mobile device

When first asking for their consent:

"Can we take some photos of your mole/rash so we can observe it over time? If we don't take a picture it may be more difficult to keep track of changes. Would you be happy for other people to see the pictures for teaching purposes or would you prefer them just to be held in your notes, solely for your care? If you let us use them for teaching, it's possible anyone could see the pictures."

When explaining about the device and transfer process:

"This is a hospital device, not my personal mobile phone. I will take photos of your mole/rash and send them to your medical record via secure NHS email. They will become part of your medical record and we can use them for comparison over time. They will not be held on the phone."

Or:

"This is my personal mobile phone and I can assure you that I will delete the photos of your mole/rash as soon as I have sent them to your medical record by secure NHS email. I am not saving them anywhere else."

1.1.5 Consent and storage of images when patients capture and transfer images from their own mobile devices

Where patients submit their own images, consent for the images to be reviewed and stored as part of the clinical record can be assumed, but the healthcare professional in receipt of the images should wherever possible clarify consent and in all cases it is vital that the patient is informed about how their data/image will be used and shared. The assumption will be that the images are for use in care of the patient alone and not for wider use in education or research. Such additional uses would require documented specified consent (see **1.1.2**).

If a clinician requests that the patient sends images, the routine documented consent process should be undertaken. Patients need to understand that once received by a healthcare professional the images will be stored securely but that there are the usual risks associated with sending any images via the internet.

All images sent from patients should be available as part of the clinical record.

Rationale

Mobile devices afford patients an opportunity to enrich the content of their clinical record and the information available guiding their care. Documented consent may not be possible when the process is initiated by the patient. If initiated as part of a normal consultation, then there is the opportunity to undertake the normal consenting procedure, including specifying level of consent and explaining the shortcomings of use of personal mobile devices.

1.1.6 Consent for disclosure of images from the medical record

Images taken on mobile devices as part of the patient's care form part of the medical record and should be treated in the same way as written material in terms of security and decisions about disclosures. They are also subject to the GMC's guidance on confidentiality. The patient's consent will usually be required before disclosing images from which the patient can be identified.

Rationale

All data held on a patient's medical record is subject to the Data Protection Act (DPA) (1998).[9]

1.2 References

1 PCC (2011) *Quality Standards for Dermatology: Providing the Right Care for People with Skin Conditions*. (Available at http://bit.ly/VayyN2).

2 PCC (2013) *Quality Standards for Teledermatology: Using 'Store and Forward' Images*. (Available at http://bit.ly/2gSEJVo).

3 GMC (2017) *Confidentiality: Good Practice in Handling Patient Information* (pdf, available at http://bit.ly/1cxf5Dd).

4 Department of Health (2009) *Reference Guide to Consent for Examination or Treatment, Second Edition*. Gateway reference 11911. (Available at http://bit.ly/2sIJrhL).

5 EU GDPR 2016/679, Recital 32. (Available at http://www.privacy-regulation.eu/en/r32.htm).

6 GMC (nd) *0–18 Years Guidance for All Doctors* (http://bit.ly/1pIOFWH).

7 GMC (nd) *Consent: Patients and Doctors Making Decisions Together* (http://bit.ly/1vhqnlp).

8 GMC (2011) *Making and Using Visual and Audio Recordings of Patients.* London: General Medical Council. (http://bit.ly/1kYn7r1).

9 Data Protection Act (1998) London. HMSO (available at http://bit.ly/18Er0gh).

Standard 2: Safe use of mobile devices to take patient images

This standard explains the issues of device ownership, the connectivity required for secure data transfer and the encryption and storage/security requirements for any mobile device being used for clinical photography. The device owner is responsible for all data captured and/or stored using their mobile phone and should make sure they fully understand the device's features and how to use them, taking all steps to make the device secure, before they capture or receive patient images.

Healthcare professionals who use their own mobile devices to take clinical images may do so in a wholly or partly unregulated way (see scenario 3 below). This high-risk approach can be problematic in terms of device security. This standard aims to address this issue in a pragmatic way and the document as a whole could be used as the basis for developing an organisational policy in line with scenario 2.

Who owns the device being used? Three scenarios

1 The employing organisation (usually the local trust) issues healthcare professionals with NHS-approved devices that are centrally controlled.

2 Healthcare professionals regularly use their own devices within a clear 'bring your own device' (BYOD) policy from the employing organisation (which may involve use of a dedicated software package or app to partition personal and professional data) in line with ICO guidance.

3 Healthcare professionals use their own devices, whether on a regular or occasional basis, without oversight of the employing organisation and/or in the absence of a clear BYOD policy.

2.1 Recommendations

2.1.1 Device ownership and responsibilities

Ideally, every mobile device used for patient photography would be owned and managed by the employing authority (scenario 1). This management would include central control by the authority's IT department of every aspect of the devices' operation, including the applications that can be run on them, the level of encryption used, the security of the connections the devices can initiate and enforcement of a passcode. It would also enable devices to be tracked and support remote wiping of any device reported lost.

However, not all healthcare organisations have implemented these controls, and, particularly in primary care, scenarios 2 and 3 are more likely, as most healthcare professionals and patients will use a personal mobile device to take clinical images. This is known as 'bring your own device' (BYOD) and raises a number of issues that need to be addressed to ensure that images can be captured effectively and transferred securely to the appropriate healthcare IT systems. The ICO has published guidance on managing personal data within organisations where BYOD is used.[1] and the Information Governance Alliance (IGA) guidance focuses specifically on the healthcare sector and sets out some clear requirements for an effective BYOD policy.[2]

The present document should support and form part of any BYOD policy and could be used as the basis for developing one. Any such policy, particularly when combined with the use of an app or a dedicated software package, will resolve most of the issues covered under this standard.

Where personal devices are being used, the healthcare professional should minimise the risk of breaching the terms of the Data Protection Act

(1998) (DPA) by disabling photo-sharing and cloud-based storage backup and enabling encryption. If the images contain PID, secure transfer methods to get the images off the device should be guaranteed.[3] Where secure transfer cannot be guaranteed, anonymising or pseudonymising the images may be a pragmatic solution.

Rationale

All healthcare providers using mobile phone technology must ensure that they minimise risks to PID and confidentiality.

Anyone using their personal mobile phone to capture, store or transfer patient data (including images) is responsible for that data under the terms of the DPA.[4] Where that data is processed or held by an organisation, the data controller (usually the organisation itself) is responsible for ensuring processes are in place to maintain compliance with the DPA.[1]

2.1.2 Mobile device security

2.1.2.1 Physical device security

The physical security of mobile devices is very important as they are easily stolen or mislaid. It is therefore essential that any confidential information/ PID held on a mobile device is protected should it fall into the wrong hands. In order to achieve this, the device must be configured with a strong passcode (6+ characters) that needs to be entered before it will operate. It is also vital that any data stored on the device should be encrypted so it cannot be retrieved, as should any removable memory cards, where used.

2.1.2.2 Operating systems updates

The majority of operating systems updates contain not only bug fixes and additional functionality but also fixes to security vulnerabilities that have been identified in the device's operating system. It is therefore essential that the updates are applied as soon as they become available to ensure the security of the device.

2.1.2.3 Cloud-based backup services

Many mobile device manufacturers offer cloud-based backup services (eg iCloud, Google Drive, Dropbox etc.) where copies of the images held on a device are automatically transferred to cloud-based storage. Access to these images cannot be controlled and images may be copied over and stored without the user's knowledge. In order to stop patient-identifiable images from being uploaded any cloud-based backup service should be disabled.

Rationale

All healthcare providers using mobile phone technology must ensure they are compliant with relevant safety laws and regulation for secure use of digital technology.

2.1.3 Device connectivity

There are a number of ways in which data can be accessed on a device or intercepted during transfer via wifi networks. For this reason it is vital that devices holding PID are not connected to open networks, ie those that do not require a user name or password (such as those often available in coffee shops and bars). Any wifi network to which you connect your device must support WPA2/PSK authentication and encryption as a minimum. Local NHS wireless networks are normally configured securely, although care needs to be taken not to connect to a service provided for patients or other non-NHS staff.

Data transmitted over 3G/4G/UTM mobile networks should be secured via a virtual private network (VPN) or other encryption mechanism such as NHS.net mail.

2.1.3.1 Bluetooth

Devices used for the capture and\or storage of personal data should not use implementations of the Bluetooth standard previous to version 4. Bluetooth should be disabled when not in use. It should not be employed to transfer PID between devices and its use for any business functions should be subject to risk assessment and approval.

Rationale

All versions of Bluetooth have inherent potential security flaws both for pairing and for data transfer purposes. More recent versions are still vulnerable despite offering more secure implementation options.

Best practice mobile device security recommendations

Before using the device to capture clinical images ensure that:

- it is configured with a strong passcode (6+ characters);
- data encryption is enabled (may not be the default setting);
- cloud-based backup is disabled (until the image is fully deleted from the device);
- operating systems are fully updated
- any unsuitable default settings, such as including global positioning satellite (GPS) location information linked to photographs, are changed.

Healthcare professionals using their own mobile device (scenarios 2 and 3 on p. 22) may also want to consider:

- buying a device (or using an old one) purely for medical use, ie with no SIM or account to act solely as a wifi device with no further connectivity or backup storage (the employing organisation may provide suitable encryption under a BYOD policy);
- installing a secure clinical image transfer app to partition the images and download them without retention on the device itself.

2.1.4 Patient-owned devices

2.1.4.1 If a patient self-selects to take images

If a patient chooses to take images on their own mobile device for such purposes as mole monitoring, this is at their own discretion.

2.1.4.2 If patients are asked to take their own photographs to be shared with their medical record

If a healthcare professional asked the patient to take images and send them in for monitoring and storage, it is important that the risks are fully explained and the patient's consent should be sought in the usual manner highlighting considerations of transfer, storage and uses of the images (see **Standard 1**). Images of a sensitive personal nature (eg genitals) may be unsuitable for this form of remote monitoring and should be subject to a more detailed and documented discussion with respect to data protection in transfer and storage using their device.

Rationale

Self-monitoring is a normal part of self-care and should be encouraged. If these images are transferred to a healthcare professional/medical environment, the normal professional standards around consent, data protection and use/storage of the images apply.

2.1.5 Image quality

Every effort should be made to produce the best-quality image achievable at all times for diagnosing and monitoring clinical conditions. (For guidance on taking patient images using mobile devices see p. 15.) Image quality should be the first consideration where medico-legal or specific diagnostic details are a primary concern. Where the extent of a rash or a pattern is being assessed, image quality may be less relevant.

Settings, equipment and likely image quality

Highest quality

- Medical illustration in studio*
- Medical illustration, bedside*
- Clinician with digital single-lens reflex (SLR)*
- Clinician with other mobile device*
- Patient/carer with digital SLR
- Patient/carer with other mobile device

Lowest quality

* (consider use of dermoscopic attachment where high magnification and pigment analysis are helpful)

Users should be mindful that to accurately compare one image with another, taken over a given time period, requires standardised photography techniques and therefore photography should not be rushed – autofocus functions, viewpoint, backgrounds and area of view should all be considered.

Rationale

Clinical photography using a digital SLR camera will produce a better image than the camera phone due to the quality of the lenses in front of the light sensitive plane and the pixel formation.

Skin can be a difficult surface for an automated focusing system and it is important not to rush. Some camera phones will struggle to capture 1:1 close-ups, in which case the use of a small scale in the image frame can sometimes help the device focus on a defined edge.

Images legally form part of the patient's case notes and therefore all images taken should be retained. If particular images are extremely poor, wherever possible explain to the patient at the time that these require deletion and allow them to witness the process. The number of images retained and deleted due to poor photographic technique should be written in the patient's notes.

2.1.5.1 Discarded images

Not all images taken within a set are relevant or useful. It is acceptable to discard superfluous images, but it should be done in a safe manner and ideally in front of the patient. Bear in mind that most delete processes require a second step, eg 'empty trash'. For information on deleting images from the mobile device after transfer see **3.1.3**.

2.2 References

1 ICO (nd) *Data Protection Act 1998: Bring Your Own Device (BYOD)* (pdf, available at http://bit.ly/1Ny3xgN).

2 Information Governance Alliance (IGA) 'Bring Your Own Devices (BYOD) Information Governance Guidance', (pdf, available at http://bit.ly/2sdtxs0).

3 GMC (2017) *Confidentiality: Good Practice in Handling Patient Information* (pdf, available at http://bit.ly/1cxf5Dd).

4 Data Protection Act (1998) London. HMSO (available at http://bit.ly/18Er0gh).

Standard 3: Safe transfer and storage of images captured with mobile devices

This standard considers the responsibilities of healthcare professionals with regard to the transfer and storage (both temporary and archival) of images captured on mobile devices. It is based on the premise that data should be obtained, recorded, held, altered, retrieved, transferred, destroyed or disclosed in accordance with the Common Law Duty of Confidentiality,[1] the Caldicott Guidance, the Data Protection Act 1998[2] and other national and professional guidance.

3.1 Recommendations

(See also 7.1.3 of *Quality Standards for Teledermatology*)[3].

3.1.1 Data transfer

Transfer of patient images from a healthcare professional should be undertaken in a manner that ensures that the data arrives securely at the required point for storage and use. It should ensure that it is not sent to other places that are not intended or that do not meet the required standard and that the date the image was taken is clear. Data should not be vulnerable to interception or misappropriation during the transfer process.

Where healthcare professionals regularly use their own mobile devices to transfer clinical images their employing organisation should have a clear policy on how PID should be transferred and stored as part of the BYOD policy (scenario 2 on p. 22).

The healthcare professional should ensure that:

- all PID is encrypted prior to transfer wherever possible;
- PID is transferred between healthcare professionals by email using NHS.net or other secure NHS systems such as the e-referral service wherever these are available (if no secure NHS systems are available use another secure data transfer system with the appropriate level of encryption and with servers within England, Scotland or Wales, as appropriate (eg Egress) or a secure clinical image transfer app);
- Bluetooth and any similar connectivity is switched off when using the device to transfer patient data.

Image downloading methods must conform to the level of encryption and access security specified by NHS Digital. When downloading PID from a mobile device:

- it is reasonable to download using a wireless network provided the network conforms to the required level of encryption and access security specification – this will usually be the case in NHS institutions;
- it is acceptable to transfer data from a mobile device using a cable between device and a desktop PC as long as the PC acts only as a conduit to a secure network server and is not used as a storage device (or unless there is a suitable secure storage system on the PC and the process abides by the employing organisation's IT security policy).

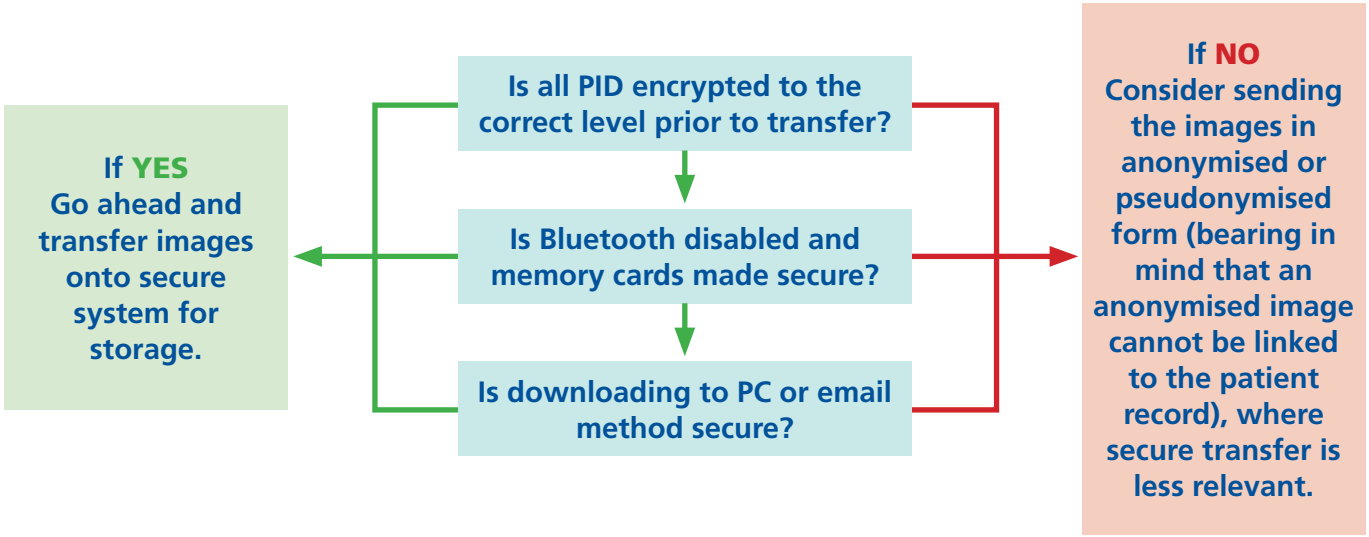
In circumstances where secure transfer cannot be guaranteed, sending pseudonymised or anonymised data may be a pragmatic solution.

Rationale

'There should be no transfers of unencrypted PID or personal data on staff 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.' (Director General for Information and Programme Integration, Department of Health)[4]

The principles of information governance and guidance on handling personal data, which includes digital images and information, are

FIGURE 5: Secure transfer of patient data



covered in full in Standard 8 of the Quality Standards for Dermatology.[5]

'Personal data must not be transferred outside the EEA unless adequate provisions are in place for its protection' (ICO, Guide to Data Protection, *Principle 8*)[6]

WhatsApp and similar instant messaging applications

WhatsApp and certain other instant messaging apps are said to offer secure end-to-end encryption of messages sent and received. Unfortunately, this is not a guaranteed secure method of transferring PID. Copies are often stored on the device or in a cloud-based memory system, sometimes without the user's knowledge and often outside Europe.

Unless all the automated connectivity, storage and archive facilities are disabled, it is not possible to make a device completely secure for transferring or viewing images without the use of a security-tested specialist application.

3.1.2 Data storage

When images are captured on a mobile device, they are temporarily stored on that device before being transferred. They should then be stored on a server for reference as part of the patient record.

3.1.2.1 Storage on a mobile device

Images taken and stored, even for a short time, on a mobile device are non-secure and all steps should be taken to protect the patient-identifiable images in order to remain compliant with the Data Protection Act (1998) (DPA).[2] See **Standard 2** for information on password protection and encryption, and note that cloud-based memory backups should not be used and automated archiving, if available, should be disabled, especially if non-secure cloud-based solutions are routinely used.

Once images have been securely transferred, all traces of the images must be completely deleted from the device and phone storage systems (see **3.1.3**).

3.1.2.2 Archival storage

Patient images must be stored in a secure environment that complies with the data protection law. Images should be uploaded promptly and securely stored to ensure availability for the designated purpose, which will usually be patient care. Where there is an electronic patient record (EPR), then the images obtained through the mobile device should be linked to the EPR and retrievable through it.

Images must be archived in a secure searchable storage system which records image data and the consent level for the designated use. Data should be backed up regularly on a central server and the server must be within England, Scotland or Wales, as appropriate.

FIGURE 6: Storage system compliance

Rationale

The principles of information governance and guidance on handling personal data, which includes digital images and information, are covered in full in Standard 8 of the Quality Standards for Dermatology.[5]

'Personal data must not be transferred outside the EEA unless adequate provisions are in place for its protection' protection' (ICO, Guide to Data Protection*, Principle 8).*[6]

3.1.3 Data deletion

Patient images should be deleted from the mobile device as soon as possible after being uploaded to archival storage facility. Ideally a PID deletion policy should be agreed as part of the BYOD policy within the framework of using the mobile device in the clinical setting. Some NHS institutions are able to remotely delete patient identifiable data from devices owned by the institution.

The purpose of transferring and deleting patient images in a timely fashion is to ensure that PID cannot be obtained by a third party through being left on a mobile device and that the images are made available to the clinical record as soon as possible.

Where a healthcare professional is using their own mobile device, it is their responsibility to ensure that the data is deleted from all possible backup sources.

Rationale

The principles of information governance and guidance on handling personal data, which includes digital images and information, are covered in full in Standard 8 of the Quality Standards for Dermatology.[5]

3.2 References

1 DH (nd) *The Common Law Duty of Confidentiality* (http://bit.ly/2tMdlzX).

2 Data Protection Act (1998) London. HMSO. (Available at http://bit.ly/18Er0gh).

3 PCC (2013) *Quality Standards for Teledermatology: Using 'Store and Forward' Images*. (Available at http://bit.ly/2gSEJVo).

4 Letter (30 January 2008) from Matthew Swindells, Gateway ref. 9424.

5 PCC (2011) *Quality Standards for Dermatology: Providing the Right Care for People with Skin Conditions*. (Available at http://bit.ly/VayyN2).

6 Information Commissioner's Office (nd) 'Principle 8' of *Guide to Data Protection* (http://bit.ly/1MRKU83).

Appendices

Appendix A

The example that follows is for use when a healthcare professional takes clinical photographs using a mobile device. This form is not intended for use when patients submit their own images. In such cases it is important to gain consent to store images in the clinical record and written consent is required if the images are to be used for teaching, publication or research.

Draft consent form for patient photography using a mobile device

Statement of healthcare professional taking photographs:

I have discussed with the patient the reasons for taking clinical photos using a mobile device, and how the images will be used, transmitted and stored and have explained to them the inherent risks and benefits. I understand the risks of data transfer from a mobile device and have taken appropriate steps to mitigate these risks.

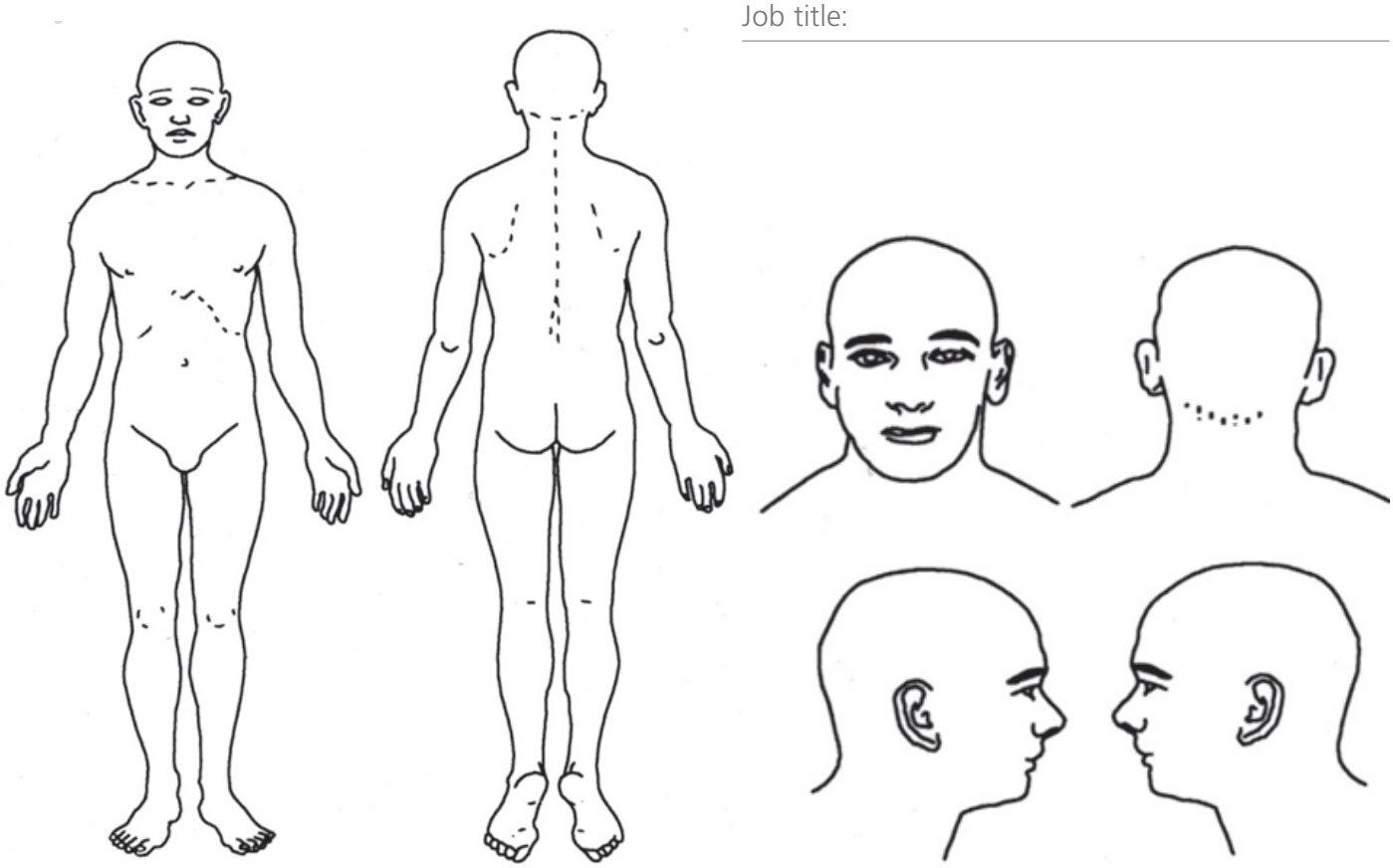
Healthcare professional's signature:

Date:

Name (PRINT):

Job title:

Areas requiring photography:



Statement of the patient

I have had the process of clinical photography using a mobile device explained to me and I have had the opportunity to ask questions about the procedure. I agree to clinical photography as described on this form. I understand that:

- the photographs may be temporarily stored on the mobile device until they are transferred to a healthcare organisation approved storage system.
- there may be a difference between the accuracy of clinical care using photographs as compared to face-to-face clinical assessment.
- I have the right to withhold or withdraw my consent for photography at any time without this affecting my right to future care or treatment. If, at a later date, I wish to retract my consent I will contact this Health Care Organisation.
- if I choose to take photographs myself as part of my medical record, the security of the image file held by the Health Care Organisation (HCO) can be guaranteed, but not earlier files prior to HCO receipt.
- this consent limits the use of these photographs to the purposes specified by me below and any additional uses will require my further consent.
- extra images not adequate for or needed in the record may be deleted.

☐ **Health records** – I consent to photographs being taken which will form part of my health record

☐ **Lecturing/teaching/publication** – I consent to the photographs being made available for teaching within this healthcare organisation, at meetings nationally and internationally and for publication in journals and/or the internet. I note that this means that the photographs may be seen by anyone and that it may not be possible for me to subsequently withdraw consent.

Patient's signature:

Date:

Name (PRINT):

A witness should sign below if the patient is unable to sign but has indicated their consent. A parent/guardian should sign on behalf of children.

Witness's signature:

Date:

Name (PRINT):

Appendix B

Technical information regarding data transfer, storage and deletion

See also 7.1.3 of *Quality Standards for Teledermatology*

Data transfer

- All PID should be encrypted prior to transfer using strong authentication (AES-256) that meet national standard.
- Wireless network downloading to a server is a suitable method of downloading as long as the network conforms to the required level of encryption and access security specified by NHS Digital. At a minimum level, the transfer should be conducted on an encrypted connection using a valid SSL Certificate from a trusted authority. The Certificate Signature Algorithm should be at least SHA-256 with RSA Encryption.
- Further security should include 'salting' all transactions and verifying checksums on all files to ensure the files sent to the server have not be modified before or during transmission.
- Also recommend is encryption of the data further on the handset device before transmission to add another layer of protection to the data – using at a minimum AES-256 cryptography.
- Bluetooth should never be used for file transfer of sensitive data. If Bluetooth cannot be switched off – then ensure a PIN is required to access your handset via Bluetooth (and it is different to the default PIN), and ensure it is not visible to other local devices.
- Data transfer between clinicians by email should use suitable levels of encryption eg NHS.net. Other NHS emails such as those assigned to an NHS trust are only secure within that organisation and not when connected to external organisations.
- Data can be sent using an electronic referral system. Such systems need to work with the appropriate level of encryption and have servers within England, Scotland or Wales, as appropriate, eg the NHS e-Referral Service.

Data storage

Mobile device storage (short-term)

- PID should only be held on storage isolated from external systems (ie not linked to other communication applications such as Facebook and cloud-based automatic backup facilities). The storage may be physically isolated through use of a dedicated isolation device or electronically isolated through use of defined software applications.
- Strong passwords – long, non-dictionary words that are not easily guessable and include numerals and symbols – are vital. Use of a different password for every account is best practice and recommended in the Information Governance Toolkit (https://www.igt.hscic.gov.uk/).

Archival storage

- PID must be stored in a secure environment which complies with the data protection law.
- PID to be uploaded for storage promptly according to local agreed guidance to ensure availability for designated purpose, eg patient care.
- Images must be stored in a manner that allows their retrieval connected with the designated use and a record of the consent, eg all patient care records should have clear patient identifier and be searchable according to this criterion. Teaching data can be stored according to content. Dual use patient identifiable data can be stored using both.

- Data should be backed up regularly on a central server.
- The server must be within England, Scotland or Wales, as appropriate.
- Where there is an electronic patient record (EPR), data obtained through a mobile device should be linked to the EPR and retrievable through it.

Data deletion

A PID deletion policy should be agreed to apply when using a mobile device in the clinical setting.

Options include:

- Use of an encrypted password-protected device electronically isolated from other systems. Such a device does not require immediate deletion. Deletion to be undertaken according to date of transfer to archiving. Can include remote deletion of PID through a wifi system within an institution
- Use of a device with more general connectivity which has a ring-fenced/sandboxed application which either blocks storage or blocks uploading to non-designated storage servers.

Appendix C

Working group members

Name	Role/title	Organisation/region
Julia Schofield	Project lead Consultant Dermatologist	United Lincolnshire Hospitals NHS Trust
Helen Alexander	Dermatology Specialist Registrar	Medway NHS Foundation Trust
David de Berker	Consultant Dermatologist	University Hospital Bristol and British Association of Dermatologists Health Informatics Committee
Carol Blow	General Practitioner with a special interest in Dermatology	Stonehaven Medical Practice, Aberdeen
Matt Bradley*	Mobile App/Secure Technical Architect	(supplier to) University Hospitals Birmingham NHS Foundation Trust
Carolyn Charman	Consultant Dermatologist	British Teledermatology Society
Shane Dark	Information Governance SME	Information Governance Alliance
Simon Dove*	Head of Service, Medical Illustration	Norwich and Norfolk University Hospitals NHS Foundation Trust
Saul Halpern	Consultant Dermatologist	British Teledermatology Society
Stephen Kownacki	Executive Chair	Primary Care Dermatology Society
Nick Levell	Consultant Dermatologist	British Association of Dermatologists
Colin Morton	Consultant Dermatologist	NHS Forth Valley
Elizabeth Ogden	Associate Specialist	Primary Care Dermatology Society
Carla Renton	Patient Group Representative	Psoriasis Association
Amanda Roberts	Patient Group Representative	Nottingham Support Group for Carers of Children with Eczema
Lynne Skrine	Dermatology Specialist Nurse	British Dermatology Nursing Group
Jane Tovey	Medical Illustration Services Manager	University Hospitals Birmingham NHS Foundation Trust

* Attended first meeting only

Appendix D

Stakeholder consultation

During the consultation period we contacted the organisations listed below and are grateful for the responses received. Where appropriate the finished document has been modified in line with their comments. We are particularly grateful to the ICO and GMC for their comments and input during the development of the document

Stakeholder contacted	Response received
British Association of Dermatologists (Health Informatics Committee)	Yes
British Association of Dermatologists (members, including trainees)	Yes
British Dermatological Nursing Group	Yes
General Medical Council (GMC)	Yes
Illustrated Network Scotland (MINS)	Yes
Information Commissioner's Office (ICO)	Yes
Information Governance Alliance	Yes
IT Department, University Hospitals Bristol NHS Foundation Trust	Yes
Medical Illustration Department, The NHS Foundation Trust / Dudley Group	Yes
Medical Illustration Department, Royal Devon and Exeter NHS Foundation Trust	Yes
Medical Illustration Department, Swansea Hospital	Yes
Primary Care Dermatology Society (PCDS)	Yes
Royal Liverpool and Broadgreen University Hospitals Trust	Yes

Appendix E

Glossary of abbreviations

BAD	British Association of Dermatologists
BDNG	British Dermatological Nursing Group
BYOD	'bring your own device'
DPA	Data Protection Act (1988)
EPR	electronic patient record
GDPR	EU General Data Protection Regulation
GMC	General Medical Council
GPS	global positioning satellite
ICO	Information Commissioner's Office
IGA	Information Governance Alliance
NICE	National Institute for Health and Care Excellence
PCDS	Primary Care Dermatology Society
PID	patient-identifiable data
SLR	single-lens reflex
VPN	virtual private network