Cymorth Llywodraethu Gwybodaeth ar gyfer Gofal Sylfaenol
Information Governance Support for Primary Care
IGDC • DHCW

IG Guidance for Primary Care Providers

Capturing and Obtaining Clinical Images

Introduction

Information Governance is a framework which supports how organisations and individuals manage the way information is handled. It applies to personal and sensitive personal data of employees, patients, and service users. It is about setting a high standard for the management of all information and giving organisations the tools to achieve that standard.

The use of personal or confidential patient information should always be limited to the minimum required to meet the specific purpose of processing. Approved processes, systems and applications should be used where it is appropriate to do so.

This guidance is aimed at Primary Care Health Professionals when capturing and obtaining clinical images to support patient care. It is important for these professionals to understand their information governance responsibilities when capturing, obtaining, and transferring such images, ensuring this is conducted in a safe, secure, and confidential manner.

It is important to set out the processes for the management of clinical images and ensure that these processes are secure and maintain the confidentiality of patients.

Without using caution, taking, storing, and transferring images can lead to breaches of patient confidentiality and of data protection legislation. It is the healthcare professional's responsibility to give the patient clear information on both the risks and benefits of using an image captured on digital cameras, including mobile devices.

Benefits

Clinical images (photographs and video recordings) for clinical use can be a valuable tool in assessing and evidencing a patient's condition. Clinical images can provide additional information for the patient record, therefore potentially improving patient care. They can supplement referrals for advice or treatment and can be particularly useful to record changes overtime for certain medical conditions.

Risks

As with any technology, digital cameras and mobile devices are subject to damage, accidents, and malfunctions, with the risk of data loss. Due to their size and value, they may be more susceptible to loss or theft. If the device is not adequately password protected with the appropriate level of security, clinical images could be illegally or inappropriately accessed.

Clinical images captured and stored on a digital camera or mobile device are potentially insecure if they are not appropriately managed. Images could be unintentionally shared. For example, backed up to cloud-based services without the device owner's knowledge, meaning the security may not be guaranteed during data transfer of the image. Images may also still be accessible after apparent deletion from either device.

Obtaining images

Staff are expected to use their professional judgement in the management and obtainment of clinical images. Primary Care Service providers should ensure that the collection, management, and transfer of images for patient care is appropriate and secure. The decision 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.

Care should be taken to only request images where necessary, ensuring that the risks are fully explained, and the patient's consent sought in the usual manner for both clinical treatment and the processing of patient information.

Healthcare professionals must explain the specific need or reason for obtaining the clinical image. They should explain to the patient:

- Why the clinical image is required.
- How it will help in providing clinical care.
- Who can access the image.
- How and where it will be stored securely and how long for.
- How it will be used.

Note: Information on the processing of patient information may be presented in the form of a privacy notice. Further guidance on transparency and informing individuals on how their information is processed can be found on the ICO website.

The GMC has produced guidance on Making and using visual and audio recordings of patients which may be useful for all Primary Care Service providers.

Clinical images are confidential. These should be maintained within the patient's clinical record and treated with the same care as all other medical records.

Images provided by patients

Organisations are embracing several new ways of working, including remote/online consultation. In some cases, it may be appropriate for health professionals to request a patient send an image of an ailment e.g., an image of a rash. The health professional should highlight considerations of transfer and uses of the image provided, explaining to the patient that it will be captured and stored as part of the clinical record.

When patients capture and transfer their own images it may constitute as a non-secure transfer unless the device has the capacity to encrypt files before sending. Health professionals should ensure that the patient is aware that sending images is not 100% secure and the organisation will retain no responsibility for any misdirected images sent by the patient.

When the images are transferred to the health professional, the usual professional standards around consent, data protection and use/storage of the clinical images apply.

The Medical Defence Union (MDU) has produced guidance on Receiving and storing patient images from online consultations.

Images taken by a Healthcare Professional

Clinical images should only be taken where clinically necessary and with the consent of the patient. The healthcare professional should ensure:

- The purpose of taking the photographs and how they will be used has been carefully explained to the patient.
- Patient consent has been gained and is documented or other legal powers apply for the processing of clinical images (see the sections below on Confidentiality and Legal Basis for Processing Information and Capacity and Consent).
- Images are used for no purpose other than the patients care or treatment unless explicit consent has been obtained or other legal powers apply (see the section below on Confidentiality and Legal Basis for Processing Information).
- When taking images, the patient's identity is wherever possible, protected by ensuring that the face and any other obvious identifying features are obscured, for example, birth marks and tattoos.

Equipment

It is recommended wherever possible that clinical images are taken using an appropriate and approved organisational owned 'device' (e.g., digital camera or mobile device), to ensure the security of the images.

The equipment should be appropriately managed and secured to ensure that the images are kept safe, secure, and encrypted.

Ideally, the management of these devices would include central controls in 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.

Before using a device to capture clinical images health professionals should ensure that:

- It is configured with a strong passcode (6+ characters) or bi-metric access controls.

- Data encryption is enabled (may not be the default setting) so that information cannot be retrieved inappropriately, the same should apply to any removable memory cards, where used.
- Cloud-based backup is disabled (until the image is fully deleted from the device) to prevent automatic transfers being uploaded.
- Operating systems are fully updated.
- Any unsuitable default settings, such as including global positioning satellite (GPS) location information linked to photographs, are changed.

Use of own equipment

It is not advisable for health professionals to use their own personal devices for the management and capture of patient information. However, it is recognised that healthcare professionals do use their own devices on an occasional basis where no alternative device is available, this will often be conducted without oversight of the employing organisation and/or in the absence of a clear Bring Your Own Device (BYOD) policy.

The ICO recommend this approach is captured in an appropriate policy, therefore the Primary Care Service provider is encouraged to develop and implement a BYOD Policy. See the National Cyber Security Centre (NCSC) website for further guidance.

During times where there are no other practical alternative healthcare professionals should ensure:

- The device is appropriately maintained, and appropriate software updates and patching have been applied.
- The device is not jailbroken or any other tampering that alters the product's security.
- The device is appropriately protected with anti-virus products.
- The device is kept secure with strong passwords or Bi-metric access controls.
- No personal/confidential data is stored or recorded on personal devices.
- The device is configured to ensure that it does not automatically save images to personal backups i.e., iCloud.

- Home internet connections are secure (e.g., use a virtual private network (VPN)) and avoid using public WIFI.
- Images are securely transferred to the organisation's network as soon as possible and deleted from the camera/device once the transfer is complete.
- Additional encryption is used when transferring images to ensure the safety and security of the image in transit.

Healthcare professionals using their own device may also want to consider:

- Buying a device purely for medical use, for example, 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.

Primary Care Service providers and healthcare professionals are reminded that inappropriate management of clinical images could be considered a breach of confidentiality and must comply with the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act (DPA).

Confidentiality and legal basis for processing information

Clinical images are confidential medical records and should be treated with the same level of care and security as all other medical records. Photographs and recordings which are made during the care and treatment of patients must not be used for any other purpose.

The healthcare professional must be able to identify at least one lawful basis when sharing patient information, including the sharing of clinical images and an additional condition when sharing special categories of information. They must be able to demonstrate that they have considered this prior to sharing the information to satisfy the Accountability principle of the UK GDPR and Part 3 of the DPA. For example:

- Processing personal identifiable information for the purpose of health provision Article 6 (1)(e) of the UK GDPR – the sharing is necessary for you to perform a task in the

public interest or for your official functions, and the task or function has a clear basis in law.

- For processing special categories of information Article 9(2)(h) of the UK GDPR for special categories - processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3.

Further information on the lawful basis for processing can be found on the ICO website.

Capacity and consent

Where the patient is a child who lacks capacity to make a decision about a photograph of them being shared with the healthcare professional, the professional will need the permission of someone with parental responsibility.

If an adult lacks capacity, the healthcare professional must obtain consent from someone with authority to act on their behalf for healthcare decisions and/or proceed with the examination and clinical photography on the basis that it is in the patient's best interests to do so.

Safe transfer and storage of clinical images

If the healthcare professional is transferring an identifiable image, then it is important to ensure it arrives securely at the correct destination for storage and use. It should not be vulnerable to interception or redirection but should be protected in line with the DPA and the UK GDPR. For example, transferring to another healthcare professional within NHS Wales, the NHS Wales email system should be used or where healthcare professionals have access to 'MoveIT' this is considered.

A risk-based approach should always be considered for the security of transfer against providing patient care.

The transfer or sharing of clinical images should be given the same considerations when sharing any patient information. The healthcare professional must always meet the requirements set out in data protection legislation.

The healthcare professional should ensure that:

- All personal identifiable information is encrypted prior to transfer wherever possible.
- Personal identifiable information is transferred between healthcare professionals by email using the @Wales.nhs.uk domain.
- Bluetooth and any similar connectivity are switched off when using a device to transfer personal identifiable information.

When images are captured on a device, they are only stored temporarily on that device before being transferred. Once images have been securely transferred, all traces of images must be completely deleted from the device and its backup storage systems.

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

Clinical images must be stored in a secure environment that complies with data protection legislation. Images should be uploaded promptly and securely stored to ensure availability for the designated purpose, which will usually be patient care.

Anonymisation

Where a secure transfer of images cannot be guaranteed then anonymisation should be considered. This means that nothing is contained in the information nor attached to anything that would identify the subject of the image. The sender must also bear in mind that

completely anonymised information relies on the sender solely remembering the original source and subsequently linking the image and the response to the correct patient record. This may be overcome by pseudonymising the information.

Pseudonymisation

Personal information is considered 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 information are not attributed to an identified or identifiable natural person'. This means that the information 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 patient is known only to the two healthcare professionals involved in the transfer. Usually, an artificial identifier is added to the information 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, but it should always be borne in mind that the UK GDPR considers pseudonymised data to be personal data.