Smartphone Photography in Healthcare

Reading time:
Jayson Nagpiing
Date created: 25/11/2020

Tags: Article | Medical Practitioner | Risk Education | Professionalism & Ethics

Under Australian law taking a photo for patient records is regarded as equivalent to recording any other information for the purpose of providing healthcare. Whether digital, photographic or written, how you handle and store records must be met with the same level of care, such as storing records for seven years or until the patient reaches 25 years of age.

MIPS is aware that many practitioners are routinely using their smartphones to record and share photos with colleagues to assist in diagnosis and treatment. Whilst some practitioners are ensuring protocol is followed by diligently filing photos, many photos and messages are being transmitted insecurely, unattached to a patient record and stored inappropriately in a cloud storage system outside of Australia open to third party access.

In a study of mobile device use among Australian healthcare practitioners it was discovered that WhatsApp was the most common file-sharing application.* Its use is widespread in Australian hospitals from students through to consultants. The study found:

- An average 12 messages shared per day with patient info
- That practitioners view:
  - apps positively for quickly communicating patient information
  - have concerns about the privacy implications arising from sharing patient information in this way.
- 67% consider patient data moderately safe on these apps
- 50% were concerned use was inconsistent with current legislation and policy
- Apps were more likely to be used if they were fast, easy to use, had an easy login process, and were already in widespread use

Junior doctors are particularly exposed as they will take photos out of interest and for future reference, often without any thought of consequence. MIPS recommends practitioners who intend to use their phones to record and share patient information take the following into consideration:

Legal ramifications

- Every photo **must** be attached to the patient’s medical record **as soon as is reasonably practicable** (that includes photos that may be deleted off the smart device).
- If the patient is not able to give consent for a photo then consent must be sought from senior next of kin, guardian or person with medical power of attorney.
- Any email/message to/from a practitioner in relation to an photograph sent electronically which provides details of the subject of

the photograph (ie lesion, necrotised site, etc) which seeks, expresses an opinion or gives a direction regarding patient care based on the photograph and accompanying email must be attached to the patient's medical record as soon as is reasonably practicable.

- To avoid confusing a photograph of a patient with any number of other patients, a patient should be clearly identified by name, UR number etc.
- A photo of a patient should never be used in a publication without the express consent of the patient.

Changing your behaviour

- Set up a process to identify and record/store any patient health records (eg secure personal cloud backup, copy or transcribe messages into patient record system, delete information after it has been copied and stored appropriately).
- Care needs to be taken when forwarding an email/message or photo on any device; if the email/message or photo is widely circulated the risk of a breach increases exponentially. Ideally, an email and photo should only be circulated to the person from whom advice is sought, not to multiple people
- Remember mobile devices become redundant quickly and disposed of appropriately. With this comes risk so arrangements need to be made to permanently delete all stored data from the device if it is to be disposed of or given to another user.

Suitable technology

- Gmail, Outlook web mail and any other email is not secure.
- Practitioners must satisfy themselves that proper secure systems and processes are in place to ensure that emails/messages and photos are able to be transferred onto a hospital patient record or their practice medical record for the patient.
- Security must be effective on a mobile device, such devices can be hacked, scanned etc and if lost there is real risk of a data breach which is reportable.
- Choose an app that can securely transmit information, ie end to end encryption (eg WhatsApp, Medex)
- Do not use apps where the terms and conditions provide ownership, use or access to your photos or messages as this would constitute a privacy breach.

Other

- It is inadvisable to store any photographs of genitalia on a mobile device.
- Practitioners need to check with hospitals where they are accredited regarding any policies / procedures that those hospitals have in place about the use of mobile devices and photography.
- If an adverse event / complaint happens and a practitioner is involved then they should be prepared to give evidence about what was on their device and what happened to the email or photo if it is not otherwise attached to a patient record.This may include having Court orders made to surrender the device.

Facebook Messenger vs WhatsApp

WhatsApp	Facebook Messenger
• Uses end to end encryption by default	• Encryption turned on by option of 'secret conversations'
• Does not store data in the cloud	• Cloud storage and backup
• If you delete or fail to backup conversations they are lost	• Facebook can access the data
• You can opt to automatically backup images received/sent	• Even if you delete it, it is not deleted from Facebook's server
• If managed appropriately, then suitable for use with patient information	• Not advisable for patient records

Facebook purchased WhatsApp in February 2014 for a 21.8 billion, 20 times the price Facebook paid for Instagram. WhatsApp user growth is very strong and while it is not monetised at the moment Facebook see potential for the App's use to become further widespread.

Other channels

Although Messenger and WhatsApp are the two most common forms of communication via smartphones there are many different channels that doctors and dentists are using for patient communications. Some specific tips and specifications for each channel:

SMS/MMS messages

There is a higher risk of information being seen by another person, other than the designated person. Standard text messages are not encrypted when they are sent or received. There is no system in place that prevents the message falling into the wrong person's hands if an incorrect number is given out or inputted.

Best Practice – to avoid texting altogether and have a discreet phone call. If you are engaging in discussions via this medium then you can take the following steps:

- Text messages between doctors should be transferred to the patient's clinical notes as soon as possible and then deleted from the phone.
- Content and spelling of your messages should be reviewed before sending.
- keep your phone secure and frequently deleting your message history.

Email (Outlook)

When you need to protect the privacy of an email message, encrypt it. Only the recipient who has the private key that matches the public key used to encrypt the message can decipher the message for reading. Further steps to take:

- Add senders to safe and blocked senders list.
- Only sign in from computers you trust.
- Create a strong password, do not share it and update it frequently.
- Use antivirus software.

Skype

All Skype-to-Skype voice, video, file transfers and instant messages areencrypted.

WeChat

WeChat is not encrypted. We do not recommend that you use this platform for confidential matters.

KakaoTalk

Kakao Talk has the option for secret messages that allow encryption. To use this service on Kakao Talk you must opt in. Standard messages are not encrypted.

Australian practitioners can also use MedX as an alternative to mainstream messaging services. MedX is free like mainstream services but is designed specifically for AHPRA registered doctors and includes end to end encryption and may provide better legal compliance than mainstream applications. MIPS is unaware what the current uptake among practitioners is for MedX but the system relies on practitioners registering with the service and installing the app.

As per all other healthcare, the AHPRA Code of Conduct applies and practitioners should be aware of the AHPRA Social Media Policy.

* JMIR Med Inform. 2018 Feb 9;6(1):e9. doi: 10.2196/medinform.9526. 'The Use of Communication Apps by Medical Staff in the Australian Health Care System: Survey Study on Prevalence and Use'.