Information governance considerations for staff on the use of **instant messaging software** in acute clinical settings

Information governance considerations for staff on the use of instant messaging software in acute clinical settings

Version number: 1.0

Published: 9 November 2018

NHS England Publications Gateway Reference: 08496

Prepared by: Kiran Mistry, Data Sharing and Privacy Unit, NHS England

If you have any queries about this guidance on instant messaging, please contact NHS England's Data Sharing and Privacy Team by email england.dsp@nhs.net

This information can be made available in alternative formats, such as easy read or large print, and may be available in alternative languages, upon request. Please contact 0300 311 22 33 or by email england.contactus@nhs.net.

Instant messaging is a useful tool in supporting the delivery of direct care, particularly in an acute context. There are, however, some important data protection considerations surrounding the use of these systems, including:

- The transfer of sensitive data across unregulated servers outside the European Economic Area (EEA)
- Compliance with data protection requirements regarding 'fair processing', individuals' rights, and records management
- Data protection security risks, including bringing your own device (BYOD) to work.

A proportionate approach is therefore needed: staff need to balance the benefits and risks of instant messaging depending on the purpose for which they wish to use it (e.g. using it in an emergency versus as a general communication tool).

This document is a quick guide for helping you think through the information governance (IG) issues when using instant messaging in an acute clinical setting.

Instant messaging can have clinical utility but remember that the law places obligations on organisations to protect patient confidentiality. If you are a clinician, you may also have to defend yourself against regulatory investigation if you have not taken sufficient steps to safeguard confidentiality.

Choice of App

The security features of an app can help ensure that your message stays private between you and the intended recipient or recipients. The following features are particularly important if your message contains a patient's identity or information that could potentially be used to identify a patient.

- **Encryption** – does the app meet the NHS end-to-end encryption standard of "AES 256"?
- **End-user verification** – can the app verify that the people using the app are indeed who they say they are?
- **Passcode protection** – can a secondary PIN be used to protect the app, and can it be time-out enabled?
- **Remote-wipe** – can the messages be removed if the device is lost, stolen or redeployed to another staff member?
- **Message retention**[1] – does the app allow automatic deletion of messages after a set period of time?

[1] It is important to handle all medical records in line with all relevant legislation, codes of practice and guidance, such as the General Medical Council (GMC) Code of Confidentiality.

Only use a standalone instant messaging application if your organisation does not provide a suitable alternative. In such a case, the following table may help you choose an instant messaging app. Note that we have not tested the features of these apps: we are simply reflecting what was stated on their websites at the time of publication.

	End-to-End encryption (AES 256)?	Passcode protection?	Remote wipe?	Message retention – automatic deletion?
WhatsApp	Yes	Not on app	No, but account can be deactivated	Secret conversation
Viber	Yes	Yes, on hidden chats	No	Yes
Telegram	Yes (letter-sealing feature)	Yes	Yes	Yes
Signal	Yes	Yes, on Android	Not Known	Yes

Be sure to follow your organisation's policies in relation to mobile devices and instant messaging. Remember too that losing your device will now have professional as well as personal ramifications.[2]

Records Management

- **Minimise the amount of patient identifiable data you communicate via instant messaging**
- **Instant messaging does not change your responsibility to maintain a comprehensive medical record.** Don't use the instant messaging conversation as the formal medical record. Instead, keep separate clinical records and delete the original messaging notes.[3] Any advice you receive on instant messaging should be transcribed and attributed in the medical record
- Remember that instant messaging conversations may be subject to freedom of information requests or subject access requests

[2] Refer to your organisation's Bring Your Own Device (BYOD) policy and to the Information Commissioner's guidance on BYOD https://ico.org.uk/media/for-organisations/documents/1563/ico_bring_your_own_device_byod_guidance.pdf

[3] Any clinical decisions communicated via instant messaging should be transferred to the medical notes as soon as possible. For further information please see the GMC guidance on record management http://www.gmc-uk.org/guidance/good_medical_practice/record_work.asp and http://www.gmc-uk.org/guidance/ethical_guidance/13427.asp

Device Settings

The National Cyber Security Centre (NCSC) publishes helpful advice on how best to secure your device, including advice that is specific to different operating systems.[4] In particular:

- **Don't allow anyone else to use your device**
- Set your device to require a passcode immediately, and for it to lock out after a short period of not being used
- Disable message notifications on your device's lock-screen
- Enable the remote-wipe feature in case your device is lost or stolen

App Usage

- **Ensure you are communicating with the correct person or group, especially if you have many similar names stored in your personal device's address book**
- If you are an instant messaging group administrator, take great care when selecting the membership of the group, and review the membership regularly
- Switch on additional security settings such as two-step verification
- Review any links to other apps that may be included with the instant messaging software and consider whether they are best switched off
- Separate your social groups on instant messaging from any groups that share clinical or operational information
- Unlink the app from your photo library

[4] https://www.ncsc.gov.uk/guidance/end-user-device-security