Mobile Messaging Platforms

1. Information governance considerations for staff on the use of instant messaging software in the NHS Scotland.

Posted on March 17, 2020 by elenaberatarbide

2. Information governance considerations for staff on the use of **instant messaging software in NHS Scotland.**

16 March 2020

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

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).

3. This document is a quick guide for helping you think through the information governance (IG) issues when using instant messaging in NHS Scotland and in particular 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.

4. 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?

	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

(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 the NHS in Scotland, appropriate tools would include Microsoft Office Teams application which is available in an app for mobile phones. 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. Please also note that some apps, such as Whatsapp are owned by other social networking companies such as Facebook.

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.

5. 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** 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

---

(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 and the GMC ethical guidance..

6. 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. 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

7. 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

1. Instant Messaging Software

Posted on March 17, 2020 by elenaberatarbide

Information Security and Governance Guidance

The **Guidance** on Instant Messaging contains generic information on the best use of Instant Messaging Applications.

At this time, as we face Covid-19, communication methods are key to help our essential services communicate and function. With this in mind, some of the practices that will be followed during this time are not the practices that would normally be followed.

Please see the **Covid- 19 ISM Information Governance guidance** for further information.

It is expected that communication methods will revert to pre-Covid-19 authorised applications at the applicable time in order that best practice Information Security and Information Governance requirements are followed and met.

Best practice is to use the tools and applications provided by your Board. However, it is recognised that, in emergency, other methods of communication may be required and the Guidance addresses those methods. It is **strongly** encouraged that Microsoft Office Teams be used as widely as possible at this time.

Each Board will have its own policies in relation to Information Security. While the Guidance attached seeks to provide generic advice, reference should always be made to local arrangements.

If you have any queries please contact your local information governance and security team.

1. Solicitors Tips for Employers on WhatsApp in the Workplace

2. Share:

-
-
-
-

Use of the mobile phone application WhatsApp has become more and more relevant, largely replacing texting as one of the most popular forms of communication.

But what role does WhatsApp play in the workplace? Undoubtedly, it may have some benefits. More specifically, it may allow employees to interact more freely by setting up work groups whilst sending links and images to one another with relative ease.

On the downside, however, many employers may be concerned about the potential risks posed by WhatsApp.

David Hession, an Associate Employment Law Solicitor, explains some tips for UK employers who are worried about their employees using the app.

3. WhatsApp at Work

Like text messaging, WhatsApp allows employees to message each other discreetly, often without employers being aware. This can cause problems where employees complain, or even raise grievances about bullying, harassment or degrading treatment on WhatsApp.

This raises all sorts of issues for employers. For instance, some of the problematic questions employers could be faced with are:

Do they commence disciplinary proceedings against employees who have conducted themselves inappropriately on WhatsApp?

Does the private nature of WhatsApp conversations mean that employers are powerless to act?

Is there anything an employer can do to prevent or restrict their employees from using WhatsApp inappropriately?

4. Can an Employer Prevent the Use of WhatsApp in the Workplace?

The likelihood is that thousands of WhatsApp or text messages are sent every day without employers being aware. It is often difficult for employers to police their employees during working time, let alone outside of working hours.

Any measures seeking to prevent employees from communicating with each other through WhatsApp are likely to be seen as overbearing, or even oppressive. This could have a damaging effect on workplace relations.

An employer's best option for dealing with the dangers of WhatsApp is to have a sensible policy in place. This is a useful way of setting out some guidelines.

Employers could even set out in the policy that any employees who engage in abusive or discriminatory conduct towards colleagues on WhatsApp could face disciplinary action. This could tie into any existing social media policy that an employer has in place.

5. Can Employers take Disciplinary Action for Inappropriate WhatsApp Conduct?

6. If an employee is approached about the inappropriate use of WhatsApp, then there are a couple of points they are likely to raise. Firstly, they may argue that any offending comments took place outside of working hours and are therefore outside the course of employment.
7. Secondly, WhatsApp differs from other forms of social media such as Facebook or Twitter in that comments cannot be seen publicly. Instead, they can only be viewed by individuals who are part of a particular WhatsApp group.
8. Of course, each individual case will differ. Employers are likely to have a strong case for taking disciplinary action where employees specifically set up work related WhatsApp groups designed to abuse or belittle other employees. Employers may wish to take robust action in these circumstances, such as issuing a final warning or even dismissing the employee.

9. What Practical Steps can be Taken to Prevent WhatsApp Misconduct?

Having a sensible and balanced policy in relation to WhatsApp and group text messaging is one way that employers can try to manage this issue. A policy could include examples of what is considered acceptable behaviour. As mentioned above, this could tie in with existing social media policy.

It would be naive to suggest that employers can actually stop or possibly even limit this type of conduct. However, with a policy in place, employers can often act with a firmer hand when it comes to taking disciplinary action. Employers may also consider sending warning notices to employees where any inappropriate behaviour comes to light.

10. Guidance for healthcare workers

This is a quick guide to help staff in health and care organisations think through the IG considerations when using mobile messaging.

It is fine to use mobile messaging to communicate with colleagues and patients/service users as needed. It is also fine to use commercial, off-the-shelf applications such as WhatsApp and Telegram where there is no practical alternative and the benefits outweigh the risk.

Mobile messaging can be useful in health and care settings, particularly in emergency situations, but you should take sufficient steps to safeguard confidentiality. Below are a series of tips that will help you to use mobile messaging safely and keep information confidential.

11. Tips for using mobile messaging safely

- Minimise the amount of personal/confidential patient information you communicate via mobile messaging.
- The mobile messaging conversation does not replace the formal health and care record. Instead, keep separate health and care records, transfer any clinical decisions communicated via mobile messaging as soon as possible and delete the original messaging notes.
- Remember that mobile messaging conversations may be subject to freedom of information (FOI) requests or subject access requests (SARs).
- Do not allow anyone else to use your device.
- Switch on additional security settings such as two-step verification.
- 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. You should be aware that if this happens, then everything is deleted from your phone, including contacts and photos.
- 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 a mobile messaging group administrator, take great care when selecting the membership of the group, and review the membership regularly.
- Separate your social groups on mobile messaging from any groups that share clinical or operational information.
- Review any links to other apps that may be included with the mobile messaging software and consider whether they are best switched off.
- Unlink the app from your photo library.
- Be sure to follow your organisation's policies in relation to mobile devices and mobile messaging.
- Remember that if you're using your own device losing it will now have professional as well as personal ramifications.

12. Guidance for IG professionals

Mobile messaging apps can offer benefits to staff in health and care organisations. IG professionals should develop clear policies to support staff in knowing whether and in what circumstances they can use these tools. It should be possible to manage any risks associated with using mobile messaging apps to ensure that the benefits to care can be delivered. A Data Protection Impact Assessment (DPIA) can support you to do this. A DPIA must be carried out before implementing the use of an app including due diligence on the provider, trackers and permissions embossed in the app.

There are some important data protection considerations surrounding the use of mobile messaging systems, including:

- the transfer of special category data across unregulated servers outside the UK - if servers are held abroad, you will need to comply with the rules and regulations of the country where the server is held
- compliance with data protection requirements regarding transparency, individuals' rights, and records management
- data protection security risks, including bringing your own device (BYOD) to work

Gloucestershire County Council Internet and Digital Communications Policy 1. Policy Statement Gloucestershire County Council (the Council) accepts that the internet and digital communications are essential to enabling the Council to meet its aims and objectives. It is a requirement that your use of the Council's internet and digital communications facilities is legal and appropriate for delivering the Council's responsibilities and does not create unnecessary risk. The Council will ensure that users have access to its internet and digital communications facilities. It is a requirement that all users read and accept this policy. The Council's internet and digital communication facilities are made available to users for Council business purposes. Limited personal use is permitted, provided that such use is strictly in accordance with this policy which can be found at Information Management and Security Policies 2. Risk Management The Council recognises that there are risks associated with use of the internet and digital communications tools. This policy aims to ensure appropriate access to, and use of, the Council's internet and digital communications facilities, which will help to mitigate the following risks: • Harm to individuals • Damage to the Council's reputation • Potential legal action and/or fines against the Council or individual(s) • Inappropriate use of council resources • Viruses and other malicious software • Service disruption 3. Scope This policy applies to anyone who uses the Council's internet and digital communications facilities. Digital communication facilities include, but are not limited to, email, instant messaging apps, video conferencing/calling, webinars, text messaging and telephony. All internet and digital communications users are expected to comply with this policy at all times when using the Council's internet and digital communication facilities,

whether accessed locally or remotely (e.g. via the Council's Remote Access Gateway; or via any Council owned device). Breach of this policy may be dealt with under the Council's Disciplinary and Dismissals Procedure and in serious cases, may be treated as gross misconduct leading to summary dismissal. 4. Responsibilities The Council's Director: Strategy & Challenge has overall responsibility for the effective operation of this policy. Responsibility for monitoring and reviewing the operation of this policy and making any recommendations for change to minimise risks to the Council's operations lies with the Head of ICT. If you do not understand the implications of this policy or how it may apply to you, you should seek advice from the ICT Service Desk. The Council's ICT Service will provide users with a logon id and password for their network account; this also controls access to the internet. Users are responsible for ensuring that any logon id and passwords are only known to and used by them. Users must not attempt to disable, defeat, or circumvent any Council security All managers have a specific responsibility to operate within the boundaries of this policy, ensure that all users understand the standards of behaviour expected of them, and to take action when behaviour falls below these requirements. 5. User Responsibility Use of the internet and digital communication facilities must be consistent with the Council's Code of Conduct for Employees. All users are responsible for using the Council's internet and digital communication facilities appropriately and in accordance with the statements in this policy. It is the user's responsibility to: • Ensure they read, understand and agree to this policy as part of their induction to the Council; • Use the Council's internet and digital communication facilities in accordance with the terms of this policy; • Use the internet and digital communications responsibly and in a way that will not harm the Council's reputation; • Recognise that the Council's internet and digital communication facilities are provided for business use and must be protected

from unreasonable and excessive personal use; • Report any misuse of the Council's internet or digital communication facilities. Follow the reporting a security incident link for more information. 6. Related policies • Code of Conduct for Employees. • ICT Equipment Policy • Information Protection and Handling Policy 3 Internet and Digital Communications Policy V2.4 December 2020 • Information/IT Access Policy • Data Protection Policy • Software Management Policy • Social Media Policy • Password Policy The above policies are available at Information Management and Security Policies 7. Things You Must Do When using the Council's internet and digital communications facilities you must: a. Security controls and use of your account details, you must: ⎪ Ensure that your logon id and password is only known to and used by you; ⎪ Keep your personal use of the internet and digital communication facilities to a minimum; ⎪ Assess the reliability of any information before using it (e.g. that it is from a reliable source, accurate, complete and current); ⎪ Comply with the legal protections to data, images, and video provided by copyright and licenses; ⎪ Inform the ICT Service Desk immediately of any unusual occurrence (e.g. an antivirus software warning, getting pop-ups without having your browser open, unable to open files or task manager) b. Access, you must ⎪ Contact the ICT Service Desk immediately if you receive a suspected virus or if you experience any unusual occurrences in respect of the Council's digital communication facilities (e.g. an antivirus software warning). c. Content, you must ⎪ Take care to ensure that your communications (messages) are sent only to those who should receive them. Re-read messages before sending, check for correct addressing and (particularly where they include personal or special category information), clarity, and ensure that the content will not embarrass or subject the Council to legal proceedings or a fine. ⎪ Take care to ensure that any calls you make or receive cannot be overheard. You should be fully aware of your environment at all times, and avoid making calls that refer to personal or special category information in public places, over loud-speaker or when using hands-free devices. You should also try to ensure that the recipient of your call takes these same considerations into account. ⎪ Use Egress to encrypt your communications (messages) when they include personal or special category information and are being sent outside the Council's secure network ⎪ Put in place arrangements to ensure that incoming messages are dealt with during periods of planned absence. 4 Internet and Digital Communications Policy V2.4 December 2020 ⎪ Retain messages which constitute an official record in accordance with the Council's Records retention and disposal schedule ⎪ Manage the contents of your accounts to retain them within the current maximum limit. ⎪ Put in place arrangements to ensure that the business content of your account is available to those who need it before you change role or leave the Council's employment. ⎪ Exercise caution when opening emails and messages from an unknown external source or where, for any reason, they appear suspicious. ⎪ Inform your line manager if you feel you have been harassed or bullied, or you are offended by material received from a colleague via digital communications. Information and advice on the Council's Whistleblowing policy and procedure can be on the employee information and support intranet pages. 8. Things You Must Not Do In using the Council's internet and digital communications facilities you must NOT: a. Security controls and use of your account details, do not: ⌋ Attempt to disable, defeat, or circumvent any Council security mechanism; ⌋ Send messages from another user's account or under an assumed name unless specifically authorised. ⌋ Respond to messages requesting personal information such as credit card details, user names or passwords, or

containing links to internet sites where such information is requested. ⌋ Transmit any message or file attachments you know or suspect to be infected with a virus. ⌋ Subscribe to mailing lists for personal purposes using your Council credentials, such as your email address, except for goods ordered from the Gloucestershire Portal GCC Staff Discounts. b. Personal, special category and sensitive information, do not: ⌋ Upload personal or sensitive information into non-contracted systems, unless otherwise authorised, for example when required to provide information by law; ⌋ Send personal or sensitive information by non-secure means, unless otherwise authorised, for example where the service user is aware of the risks and has requested communication by other means; ⌋ Forward personal, special category or sensitive information to an external location (including your personal home email address) or to another person who may not be authorised to see the information. c. Access, do not: ⌋ Access emails intended for others that are clearly marked 'personal' or addressee only (for example when providing cover for periods of absence). 5 Internet and Digital Communications Policy V2.4 December 2020 ⌋ Access systems containing personal, special category or commercial data over Public Wi-Fi; ⌋ Allow other authorised users/third parties with access to your desktop/IT access to information and systems they are not entitled to view e.g. when using webinars, Jabber or service desk facilities; ⌋ Allow third parties, contractors or suppliers, other than the current corporate ICT service provider, to remotely access/take over your PC or laptop via the internet (a supplier or contractor can instigate this by for example asking you to accept a connection or click on a link on their website) for advice contact ICT Service Desk. d. Content, do not: ⌋ Create, download, upload, display or knowingly access site

Data handling and SG IT Code of Conduct
All Scottish Government data should be handled in accordance with the Scottish Government data handling standard – http://saltire/Documents/IT%20Documents/Scottish_Government_data_handling_standard.pdf and the Scottish Government IT Code of Conduct - http://saltire/my-workplace/conduct-and-discipline/standards-of-conduct/Pages/it-code-of-conduct.aspx.

Transmission of personal data
If any personal data is likely to be transmitted via a proposed WhatsApp group on SG or personal devices, Cyber Security recommend that a GDPR data protection impact assessment is conducted and signed off by the relevant Information Asset Owner to identify any privacy risks before using WhatsApp during ministerial visits.

FOI
In terms of FOI there is no issue with WhatsApp. Work related messages sent/received on WhatsApp, regardless of whether it is a work or personal device, are subject to FOI(S)A. Any request made that would capture them would have to be considered in the same manner as if they were emails. Personal information to be considered and, dependant on the content, there may need to be consideration of applying an exemption – this would have to be considered by the FOI Unit on a case-by-case basis.

SG managed devices

Cyber Security colleagues recommend that official Scottish Government documents and communications should occur using Scottish Government managed devices. These devices feature up to date operating systems, are patched regularly to address vulnerabilities and have security products installed to address threats such as malware. They feature device encryption to protect data and measures to reduce the impact of loss / theft such as settings to lock themselves when not in use to limit physical access. Being corporately owned devices, the Scottish Government is also responsible for ensuring the secure sanitation of the device and any stored data at the end of device life.

Personally owned device – drawbacks

Personally owned devices are unlikely to offer the same degree assurance around security and confidentiality due to ownership issues and potentially lacking encryption, missing security updates and patches, having untrusted applications installed, being accessed by multiple people (who may not be subject to Civil Service T&Cs), having applications or settings that may backup / copy SG data on the device to an untrusted location (e.g. cloud device backup) or allow other possible data compromises (on and off device) to occur.

Security related considerations around the use of WhatsApp that should be considered by the Information Asset Owner (IAO) in deciding whether it is appropriate to use:

- While WhatsApp advertises that it uses encryption for transmission of messages (when sending them over the internet), be aware that the message content and files sent via WhatsApp may still be accessed by anyone with physical access to any of the receiving devices - therefore it is important that all devices in the group use device encryption, are set to lock automatically after a short period of inactivity and unlock with a suitable length passcode / biometrics and are capable of being wiped should they be lost.

- Cyber Security colleagues recommend that conversations are deleted from WhatsApp when no longer required.

- Cyber Security colleagues recommend members of the group are monitored to prevent messages being sent to unexpected people.

- As with many apps, the official WhatsApp app is regularly updated and some of these updates may be to address security vulnerabilities.

- Cyber Security colleagues also recommend a careful review of the WhatsApp T&Cs / End User Licence Agreement (EULA) to ensure that the parties understand how data gathered by WhatsApp may be used and shared. Also be conscious that WhatsApp T&Cs may be altered after the app is installed.

- WhatsApp has recently being investigated by the Information Commissioner Office for unlawful data sharing practices - https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/03/blog-a-win-for-the-data-protection-of-uk-consumers/.

- Sensitive information should not be sent via WhatsApp; instead SCOTS should be used.

Conclusion

Upon officials making themselves familiar with this document and the linked guidance, it is reasonable for officials to use WhatsApp occasionally as an internal communications tool to support business continuity – but only for information below OFFICIAL-SENSITIVE level.