Smartphone and mobile phone security for the clinician

Smartphones are near ubiquitous and widely used by doctors in discussing patients. In all communication doctors should take steps to protect confidentiality, yet there is a paucity of available information on how clinicians can bolster cyber security and minimize risk when using their mobile phone.

Effective communication within and across teams is essential for good care. Doctors are encouraged to contact their colleagues and seniors when needed and to likewise respond promptly in turn. Possibly because of the ubiquity of mobile phones (already carried by 98% of the workforce 6 years ago, the current uptake of mobile phones is likely near universal; Haroon et al, 2010) and the difficulties engendered by the bleep system (65% of bleeps interrupt patient care, 25% are unimportant or unnecessary and 33% result in no change to care) (Katz and Schroeder, 1988; Blum and Lieu, 1992) mobile phones are increasingly used to discuss patients and coordinate care.

In 2015, a survey of 206 doctors in a NHS district general hospital found that 92% used their personal mobile phone for hospital-related work and 77% explicitly used their mobile phone to discuss patient matters (Martin et al, 2015). A more recent impromptu survey of seventy doctors across three NHS teaching hospitals (H Barber, unpublished observations, 2016) showed that 73% used instant messaging applications to discuss patients even though 68% thought this was the least secure method of doing so. The increase in smartphone use has important considerations both for cyber security and patient confidentiality. A basic technical understanding of mobile communication is essential if clinicians are to know how to minimize the risk of breaching confidentiality or falling foul of Good Medical Practice.

Good Medical Practice

The General Medical Council has not published specific guidelines on the use of mobile phones in discussing patients. However, their existing guidance on confidentiality does have implications for how doctors should approach this issue. General Medical Council (2013) guidelines stipulate you 'must make sure that any personal information about patients that you hold or control is effectively protected at all times against improper disclosure', that 'you should not share identifiable information about patients where you can be overheard, for example… in an internet chat forum' nor should you 'share passwords' to systems that you use. Therefore an essential part of good practice is for any discussion of patients using mobile phones or smartphones to be secure and 'protected' from whoever would threaten to disclose that discussion.

Threats to security

Besides complying with Good Medical Practice, doctors have additional motivation to ensure their communications are secure. It is not difficult to imagine a scenario where a doctor would become a prime target for hacking, such as in treating a patient who is a household name or simply dealing with a case that has itself has received exceptional media attention. Phone hacking entered the public consciousness with the case of Milly Dowler (Prodger, 2011) and its victims have included not just celebrities, but also those associated with them, such as the case of Dr Hasnat Khan and his relationship with Diana, Princess of Wales (Press Association, 2012).

Phone calls and text messaging

Traditional calling and texting is insecure. Mobile phone calls are unencrypted, except for the radio link between the handset and the network, and landline calls are almost entirely unencrypted. Furthermore, with the advent of 4G, voice calls now frequently travel over the internet; this means that any security previously afforded by a closed phone network amounts to nil (Murdoch, 2016). Text messaging is also one of the least secure methods of communication. Text messages are sent via radio waves to a computer server, which then processes the messages and sends them on to the recipient. It is possible to read the messages at any stage along the way (including at the computer server, as network employees have previously been dismissed for doing; Prigg, 2004).

Instant messaging applications

Instant messaging applications allow real-time text transmission, over the internet; notable examples include: WhatsApp, Facebook Chat and iMessage, among others. When a mobile phone can access the internet and run instant messaging applications, it can be considered a smartphone (as it has an advanced operating system with features formerly confined to the personal computer). The

Dr Harry Barber is Foundation Year One Doctor in the Acute Medical Unit, University College London Hospitals NHS Foundation Trust, London NW1 2BU
(harry.barber@doctors.org.uk)

> The assumption by many is that instant messaging applications pose an inherently greater risk to patient confidentiality than traditional methods of communication. The converse is true.

assumption by many (H Barber, unpublished observations, 2016) is that instant messaging applications pose an inherently greater risk to patient confidentiality than traditional methods of communication. The converse is true. Instant messaging applications are now among the most secure methods of communication. They also offer features that provide valuable meta-communication such as showing whether a message has been received and whether it has been read. Furthermore, they allow group communication. Together these features allow one to communicate immediately with the consultant surgeon (who is in between cases in theatre), the registrar (who is managing a sick patient on another floor), and junior colleagues (pursuing other tasks elsewhere), where each individual knows whether a message has been received and/or read. Indeed, of those doctors who admitted to using instant messaging applications to discuss patients, 73% found 'group chat' a useful feature and 66% found 'knowing when a message has been read' a useful feature.

However, not all instant messaging applications are secure. There is a great deal of heterogeneity in both their functionality and their security. It is thus important that the clinician understands what makes an instant messaging application secure in order to understand how patient information can best be kept safe.

The security of an instant messaging application is determined by a number of different features, including encryption. Encryption is the process of encoding messages such that only authorized parties can read them. The strength or extent of this encryption is perhaps the main criteria that determines the security of an instant messaging application. The strength of encryption of different instant messaging applications (among other features) can be evaluated by the Electronic Frontier Foundation scorecard (Electronic Frontier Foundation, 2015) to give an indication of the overall security of an instant messaging application. This scorecard uses seven criteria to determine which instant messaging applications are most secure and therefore which doctors might use:

1. Is your communication encrypted in transit?
2. Is your communication encrypted with a key the provider does not have access to?
3. Can you independently verify your correspondent's identity?
4. Are past communications secure if your keys are stolen?
5. Is the code open to independent review?
6. Is the crypto design well-documented?
7. Has there been an independent security audit?

These are now discussed in more detail.

Is your communication encrypted in transit?

Is your message encrypted along all the links in the communication path, while travelling from one clinician to the other? If the encryption is removed at any point, for example at the network provider for mobile phone conversations or messages, then there is a weak link.

Is your communication encrypted with a key the provider does not have access to?

This criterion differentiates 'link encryption' (which can meet the first criterion) from 'end-to-end encryption'. In link encryption the keys can be stored at any point along the path, such as at the server of a network provider; therefore someone at that point could use the key to decrypt (or 'unlock') your messages. However, if these keys are only kept with the end users then only the communication partners have access to the unencrypted content. Therefore if this criterion is met, the communication can be secure even if the network provider's computers are compromised.

Can you independently verify your correspondent's identity?

One (Alice) might send a letter to a friend (Bob) only for an unscrupulous downstairs neighbour (Steve) to open and read it before resealing it and putting it back in the hall and neither Alice nor Bob would be any wiser (*Figure 1*). However, if the letter is sent by recorded delivery then Bob must verify his identity (for example with a signature) before the letter can be opened. When instant messaging applications have a built-in method for knowing who you are communicating with, it can prevent these 'man in the middle' attacks (where two people think their communications are end-to-end encrypted, yet there is an eavesdropper removing the encryption, reading the unencrypted content then re-encrypting it before passing it on). This criterion is only met if any such attack can be detected, even if the network provider's computers are compromised.

Are past communications secure if your keys are stolen?

Like the network provider, the devices used by the communication partners themselves are also subject to

Figure 1. Intended path of communication *vs* actual path of communication.

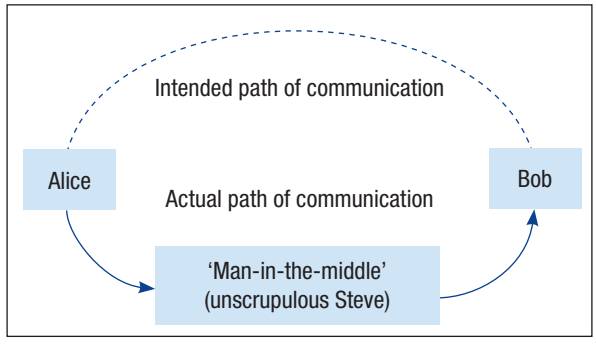

Table 1. A summary of the Electronic Frontier Foundation scorecard results for five commonly used instant messaging applications

IMA	Encrypted in transit?	Encrypted so the provider can not read it?	Can you verify contacts' identities?	Are past communications secure if your keys are stolen?	Is the code open to independent review?	Is security design properly documented?	Has there been any recent code audit?
Blackberry Messenger	Yes	No	No	No	No	No	No
Facebook Chat	Yes	No	No	No	No	No	Yes
iMessage	Yes	Yes	No	Yes	No	Yes	Yes
Signal	Yes	Yes	Yes	Yes	Yes	Yes	Yes
WhatsApp	Yes	Yes	Yes	Yes	No	Yes	Yes

attack and the cryptographic keys they store may be stolen. One way to limit the consequences of having your keys stolen is to regularly change them. In the above example, unscrupulous Steve was reading the letter before Bob got to it and even if we were to start sending and storing those letters in locked boxes, he need only to steal Bob's key and he could open all the letters he has ever received. However, if each box requires a different key and past keys are destroyed, then 'today's key' only lets Steve open today's letter. Encrypting messages with ephemeral keys is known as forward secrecy. It ensures that even if a key is stolen, whatever you said in the past remains secure and only present messages are now vulnerable.

Is the code open to independent review, is the crypto design well-documented and has there been an independent security audit?

These final three criteria ask whether the design of the instant messaging application has been documented, whether it is generally open to review by someone else and whether it actually has been reviewed.

Using the seven criteria in the Electronic Frontier Foundation scorecard, the clinician can make an informed decision about which instant messaging application to use to best safeguard patient confidentiality; the scorecard results of common instant messaging applications are shown in *Table 1*. WhatsApp, the most popular instant messaging application worldwide, has this year 'switched on' end-to-end encryption for its one billion users and its security has accordingly been upgraded to 6 out of 7 on the Electronic Frontier Foundation scorecard (Metz, 2016).

Network, operating system, device

Sending and receiving messages involves many different components, of which calls, texts or instant messaging applications are but one (*Figure 2*). The network, software and device can all be responsible for a breach in security.

If the network provider is hacked, your data may be compromised. Examples of network provider hacks include both Vodafone, which was hacked in 2004 (some believe by the National Security Agency) (Bamford, 2015), and Belgacom, which was purportedly hacked in 2012 by Government Communications Headquarters, the UK

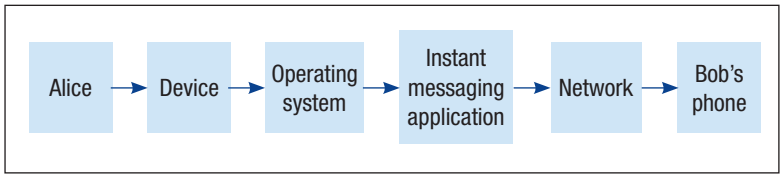

Figure 2. The components involved in the communication path.

government's spy agency (Gallagher, 2014). The best defence against such an attack lies not in your choice of network, but in ensuring the other components in the security chain (including the instant messaging application you are using) are solid.

If the operating system, the built-in phone software, is hacked, your data may be compromised. The two main providers of smartphone operating systems are Apple (which produces iOS) and Google (which produces Android). A threat intelligence report (Nokia Security Center Berlin, 2015) showed that 60% of malware (malicious software such as computer viruses) activity now occurs on mobile phones rather than desktop computers and that Android continues to be the main mobile platform targeted by malware. This is in part because the Android platform has over 80% of market share and thus is a bigger target (International Data Corporation, 2015). Thus, as it stands, you are less likely to be a victim of malware as an iOS user.

Finally, and perhaps most importantly, if the device itself is hacked your data may be compromised. One of the most common 'breaches' of security is simply losing one's phone. For this reason security experts often advocate one device for one use; the work phone gets lost at the hospital not the nightclub; conversely, the personal phone, if lost at the nightclub, contains no patient information. Clinicians should ensure their phone or phones are always password protected.

Conclusions and recommendations

No specific guidance yet exists to dictate how smartphones should be used to discuss patient information; in the absence of such guidance it is even more important that clinicians understand and mitigate the risks of such discussions. Instant messaging applications offer far greater security than any preceding mobile communication system.

KEY POINTS

- Smartphones are widely used to discuss patients yet guidelines for such discussion do not exist and understanding of mobile security is poor.
- Landline calls, mobile phone calls and text messages are largely unencrypted and insecure.
- Instant messaging applications can provide one of the most secure ways to communicate by mobile.
- The network, operating system and device itself are points of vulnerability in the communication path.
- Using a secure instant messaging application (such as Signal) in combination with a password-protected iPhone used exclusively for work helps protect against 'improper disclosure'.

However, clinicians must take heed of which instant messaging application they use, on which operating system and what steps they take to keep their device secure. Based on the available evidence it is recommended that clinicians use an instant messaging application such as Signal, Telegram Secret Chats or Silent Text on an iOS operating system, on an iPhone that is password-protected and used exclusively for work. The recommendation for regulatory bodies is that they provide sensible evidence-based rules to facilitate mobile communication, thus raising the profile of a little-talked-about but highly controversial topic from a whisper to a volume appropriate for discussion. **BJHM**

Conflict of interest: none.

Bamford J (2015) Did a rogue NSA Operation cause the death of a Greek Telecom employee? www.theintercept.com/2015/09/28/death-athens-rogue-nsa-operation (accessed 31 May 2016)

Blum N, Lieu T (1992) Interrupted care: The effects of paging on paediatric resident activities. *Am J Dis Child* **146**: 806–8 (doi: 10.1001/archpedi.1992.02160190038016)

Electronic Frontier Foundation (2015) Secure messaging scorecard. www.eff.org/node/82654 (accessed 15 April 2016)

Gallagher R (2014) The Inside Story of how British Spies Hacked Belgium's largest Telco. theintercept.com/2014/12/13/belgacom-hack-gchq-inside-story (accessed 31 May 2016)

General Medical Council (2013) Confidentiality guidance: Protecting information. www.gmc-uk.org/guidance/ethical_guidance/confidentiality_12_16_protecting_information.asp (accessed 31 May 2016)

Haroon M, Yasin F, Eckel R et al (2010) Perceptions and attitudes of hospital staff towards paging system and the use of mobile phones. *Int J Technol Assess Health Care* **26**: 377–81 (doi: 10.1017/S0266462310001054)

International Data Corporation (2016) Smartphone OS Market Share, 2015 Q2. www.idc.com/prodserv/smartphone-os-market-share.jsp (accessed 22 June 2016)

Katz M, Schroeder S (1988) The sounds of the hospital: paging patterns in three teaching hospitals. *N Engl J Med* **319**: 1585–9 (doi: 10.1056/NEJM198812153192406)

Martin G, Janardhanan P, Withers T, Gupta S (2015) Mobile revolution: a requiem for bleeps? *Postgrad Med J* (doi: 10.1136/postgradmedj-2015-133722)

Metz C (2016) Forget Apple vs. The FBI: WhatsApp just switched on encryption for a billion people. www.wired.com/2016/04/forget-apple-vs-fbi-whatsapp-just-switched-encryption-billion-people/ (accessed 22 June 2016)

Murdoch S (2016) Insecure by design: protocols for encrypted phone calls. *Computer* **49**(3): 25–33 (doi: 10.1109/MC.2016.70)

Nokia Security Center Berlin (2015) Nokia Threat Intelligence Report – H2 2015. http://resources.alcatel-lucent.com/asset/193174 (accessed 31May 2016)

Press Association (2012) Diana's former lover may have had phone hacked. www.theguardian.com/media/2012/may/13/diana-lover-phone-hacking-hasnat-khan (accessed 31 May 2016)

Prigg M (2004) Texts are not secure. www.standard.co.uk/news/texts-are-not-secure-7236241.html (accessed 31 May 2016)

Prodger M (2011) News of the World 'hacked Milly Dowler phone'. www.bbc.co.uk/news/uk-14017661 (accessed 31 May 2016)