



EDITORIALS

Are you ready for General Data Protection Regulation?

Doctors urgently need guidance, training, and fully compliant channels for sharing sensitive data

Bernadette John *digital professionalism consultant*

DigitalProfessionalism.com, London, UK

Often described as the most important development in data privacy regulation for 20 years, the General Data Protection Regulation (GDPR) is intended to strengthen data security for individuals.¹ It will be implemented across Europe from 25 May 2018. With violations set to generate fines for organisations of up to 4% of annual turnover or €20m (£18m; \$25m), whichever is greater, the GDPR is not something that doctors or the NHS can afford to ignore.

Management of confidential data is fundamental to the work of clinicians, and so this new regulation introducing specific legal requirements around consent, transmission, and storage of data will affect doctors and anyone else processing personal data.

From May 2018, patients will be able to request access to, location of, amendment to, and erasure of their data.

Transparency and accountability are vital if compliance is to be achieved. Adherence to guidance from the UK's Information Commissioner's Office, NHS, and regulatory and professional bodies is of course essential. However, such guidance has been slow to materialise and has so far failed to provide clear recommendations, meaningful training, or signposting to GDPR compliant solutions for health professionals in the front line.

Busy doctors already use popular smartphone apps for clinical communications²⁻⁶—and everything from online calendars to Dropbox, Google Drive, and PDF creator apps. With data in so many locations it will be difficult for trusts to identify where information is stored when faced with a “subject access request” from a patient.

Another concern is that the most popular apps have the right to access all of the data on users' devices, including contact lists, calendars, email, SMS, instant messages, microphone, image gallery, camera, and location.⁷ All such data on a clinicians' device are potentially sensitive.

WhatsApp (owned by Facebook) is currently facing investigation by a pan-European data regulator—led by the UK Information Commissioners Office—regarding its failure to adequately address concerns about sharing user data across the wider group of Facebook companies.^{8,9} It is clearly not an appropriate channel for sensitive clinical communications. Doctors and other health professionals should stop using

WhatsApp immediately for any communications with clinical content.

Recent guidance on the use of instant messaging in clinical settings from NHS England states that clinicians may be required to defend themselves against regulatory investigation and sanctions if insufficient steps are taken to safeguard patient confidentiality.¹⁰ But the practicalities of working within the new GDPR are not usefully explored in any depth, and no GDPR compliant solutions are suggested, even though several exist. Indeed, the guidance observes, “instant messaging can have clinical utility,” and the advice to “review links to other apps that may be included with the Instant Messaging software and consider whether they are best switched off”¹⁰ is not possible in relation to links between WhatsApp and Facebook.

Also missing from this guidance is the most basic advice—that all devices used to access or discuss patient identifiable data using apps must have all clinical data erased permanently before discarding, selling, or trading-in. Concerns regarding the threats posed to patient data by the use of an app that does not conform to the required “Advanced Encryption Standard 256-bit (AES-256)”¹⁰ pale into insignificance next to the prospect of any future owner of a device accessing the previous owner's gallery of clinical images. Or the fact that recipients of images, shared via WhatsApp, are prompted to share them on their latest Facebook update.

Genuine anonymisation of clinical digital images taken using a smartphone or mobile device is more complex than simply cropping a photo and deleting or omitting the name or patient number. Digital photos have supplementary records embedded, including the date, time, and geographical coordinates of the image, and the make and model of the device used to take them.

Jobbing clinicians are not using popular apps for communication and collaboration because they no longer care about confidentiality. Many have simply not processed the genuine risks and implications and remain unaware of alternative GDPR compliant corporate solutions for clinical communications. These include Forward, Careflow Connect, Hospify, Med Crowd, MedicBleep, Siilo, and Cupris.¹¹ At the moment, clinicians are unclear about what they should do or why they must take great care around the selection of apps and other technical solutions they bring to work. Compliant channels for

communication and collaboration are an urgent priority if the NHS is to be ready for GDPR in May.

The NHS can't be expected to provide corporate solutions for everything, but to mitigate imminent risks the top priority must be to direct all healthcare workers to appropriate, "approved," GDPR compliant solutions for clinical communications, collaboration, and the processing of patient data through their digital devices. Practical, meaningful training is essential to ensure that clinicians can identify risks and make informed choices around the use of social and mobile technology. Regular, concise, technical updates or briefings are also essential in this quickly evolving technical landscape.

Clinicians must lobby NHS information governance leads now to ensure that working requirements for data sharing and collaboration are met in a way that protects patients, promotes safe care, and complies fully with the GDPR. And before May.

Competing interests: I have read and understood BMJ policy on declaration of interests and declare that DigitalProfessionalism.com provides advice, support, and training on issues around the use of digital channels for communication for clinicians, university clinical schools, and NHS trusts.

Provenance and peer review: Commissioned; not externally peer reviewed.

- 1 European Union. GDPR. The EU General Data Protection Regulation. <http://www.eugdpr.org/key-changes.html>.
- 2 Gould G, Nilforooshan R. WhatsApp Doc? *BMJ Innovations* 12 April 2016. <http://innovations.bmj.com/content/early/2016/04/12/bmjinnov-2016-000116.full.pdf+html>.
- 3 Kamel Boulos MN, Giustini DM, Wheeler S. Instagram and WhatsApp in health and healthcare: an overview. *Future Internet* 2016;8:37-50. 10.3390/fi8030037.
- 4 Martin G, Janardhanan P, Withers T, Gupta S. Mobile revolution: a requiem for bleeps? *Postgrad Med J* 2016;92:493-6. 10.1136/postgradmedj-2015-133722 26912500
- 5 Mobasheri MH, King D, Johnston M, et al. The ownership and clinical use of smartphones by doctors and nurses in the UK: a multicenter survey study. *BMJ Innovations* 2015;1:174-81 10.1136/bmjinnov-2015-000062.
- 6 O'Sullivan DM, O'Sullivan E, O'Connor M, et al. WhatsApp doc? *BMJ Innovations* 2017;3:238-910. 1136/bmjinnov-2017-000239.
- 7 John B. Ensuring secure communication in health care: a response to O'Sullivan et al on their paper "WhatsApp doc?" *BMJ Innovations* 2017. <http://innovations.bmj.com/content/early/2017/10/24/bmjinnov-2017-000239.responses>.
- 8 Gibbs S. WhatsApp faces EU taskforce over sharing user data with Facebook. *Guardian* 2017 Oct 26. <https://www.theguardian.com/technology/2017/oct/26/whatsapp-facebook-eu-data-article-29-working-party-taskforce-sharing-user>.
- 9 Gibbs S. France orders WhatsApp to stop sharing user data with Facebook without consent. *Guardian* 2017 Dec 19. <https://www.theguardian.com/technology/2017/dec/19/france-orders-whatsapp-stop-sharing-user-data-facebook-without-consent>
- 10 Mistry K. *The do's & don'ts for individuals on the use of instant messaging software in clinical settings*. Data Sharing and Privacy Unit. NHS England, 2018.
- 11 Thomas K. Wanted: a WhatsApp alternative for clinicians. *BMJ* 2018;360:k622. 10.1136/bmj.k622 29440047

Published by the BMJ Publishing Group Limited. For permission to use (where not already granted under a licence) please go to <http://group.bmj.com/group/rights-licensing/permissions>