White Paper on the use of social media messaging services by medical professionals practising under UK law

December 2017

Mishcon de Reya

CONTENTS

This White Paper was produced to address the trending topic of the use of social media messaging within the UK healthcare sector, and has been written in collaboration with Siilo, a leading secure messenger in Europe and UK.

Mishcon de Reya

1. WHITE PAPER ON THE USE OF SOCIAL MEDIA MESSAGING SERVICES BY MEDICAL PROFESSIONALS PRACTISING UNDER UK LAW

Who is this White Paper for?

- Any medical professional and clinician employed in hospital, primary and social healthcare
- Information and Communication Technology professionals servicing the healthcare sector as well as information architects, clinical information officers and Caldicott guardians NHS authorities and trusts including the Secretary of State for Health
- Information Commissioner's Office
- Recipients of medical services in the UK i.e. patients.

White Paper goal and scope

This White Paper seeks to identify and analyse the British legal and regulatory framework provided to Medical Professionals, ICT Professionals and ICT Businesses regarding the use of Mobile Messaging Services to exchange Patient Data, including patient treatment or potential treatment plans, between Medical Professionals. When reading this White Paper it is important for all readers to bear in mind a Medical Professional's duty to share Patient Data with other Medical Professionals. Especially those who have a treatment relationship with the patient whereby this duty can be, and is often justifiably, as important as the Medical Professionals' duty to protect patient confidentiality.

In this White Paper we make a distinction between two types of Mobile Messaging Services: "Social Media Messaging Services" being those targeting laypersons and used by the general public for social purposes (including services such as WhatsApp, Facebook, Snapchat, and SMS); and "Medical Messaging Services" that are designed for and specifically target Medical Professionals communicating with one another on a secure platform.

Terminology

- "curb-side consultation": an informal and unofficial consultation obtained from a Medical Professional by either a layperson or a fellow Medical Professional. When such consultations take place between two Medical Professionals the discussion most commonly centres on the likely causes of a patient's illness, natural history of a disease, possible interventions, remedies or treatments. Unlike formal consultation it does not involve a detailed history, examination or patient assessment.
- "Data Controller": a natural or legal person, public authority, agency or other body which, alone or jointly with others, is responsible for and determines the purposes and means of the processing of personal data.
- "Data Processor": a natural or legal person, public authority, agency or other body which processes personal data on behalf of a Data Controller.
- "GDPR": The General Data Protection Regulation, which will be in effect in the UK as of 25 May 2018.
- "ICT Businesses": Information and Communication Technology professionals servicing the healthcare sector.
- "ICT Professionals": Information and Communication Technology professionals employed in the healthcare sector, including Caldicott Guardians, CMIOs etc.
- "Medical Messaging Services": Mobile Messaging Services dedicated to the professional standards and legal framework in which Medical Professionals operate medical messaging. Services provided as a dedicated data processor for Medical Professionals seeking to communicate with other Medical Professionals, such business operations should adopt revenue models that are aligned with data protection requirements regarding health information.
- "Medical Professionals": professionals employed within the UK healthcare system, i.e. clinicians and all associated healthcare professionals, primary and social care professionals, etc.
- "Mobile Messaging Services" or "Short Messaging Services": communication services on mobile devices for users to exchange messages with limited characters in length whether including text, photos, videos or other data, in a conversational format, one-to-one or in groups, over the Internet or SMS protocol, where a message can be sent without the requirement of the recipients device to be switched on in order for the message to be successfully transmitted. For the purposes of this White Paper, Mobile Messaging Services have been subdivided into Medical Messaging Services and Social Media Messaging Services.

- "Patient Data": any information, including personal data, about an individual patient which may be relevant about current or future health or illness.
- "personal data": any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
- "Social Media Messaging Services": commercial consumer centric Mobile Messaging Services offered to users to engage virtually with other users for social reasons, as well as advertising and commerce.

2. SUMMARY

In light of the increasing use of Social Media Messaging Services by Medical Professionals for work-related purposes, NHS Trusts have openly stated that the technology and security standards adopted by Social Media Messaging Services are inappropriate and insufficient with regards to the standards of care required of ICT Businesses operating within the health care sector. Mobile Messaging Services offering their services to Medical Professionals must adhere to the additional security and privacy standards required of Medical Professionals.

The use of an appropriate and secure Medical Messaging Service tailored for use within the healthcare sector to better assist Medical Professionals when assessing and treating patients and providing curb-side consultations is nothing more than a new application of a well-established non-contentious custom and practice. Ultimately, Patient Data can be shared between Medical Professionals, including by way of a Mobile Messaging Service, provided the principles stipulated in the GMC's confidentiality standards ('Confidentiality: Good practice in handling patient Information' – January 2017 – in effect from 25 April 2017) are followed and one of the permitted purposes for the disclosure and sharing of information taking priority over patient confidentiality applies.

Codes of practice and guidance on confidentiality obligations of Medical Professionals to their patients clearly stipulate that the duty to share information can be as important as the duty to protect patient confidentiality, especially in connection with the provision of safe, complete and effective patient care.

Before communicating over a Medical Messaging Service, the Medical Professional must determine whether the receiving Medical Professional has a professional treatment relationship with the patient or not. This will ultimately determine whether patient consent is required for such disclosure and secondly whether the anonymisation of such Patient Data would be an inappropriate and potentially negligent act on the part of the Medical Professional for not clearly identifying the patient that is being discussed when communicating within the medical team of the patient.

The Information Governance Alliance stipulates that the communications, being information that would classify as a health record (in accordance with the Data Protection Act 1998), does not in itself mean that the Mobile Messaging Service is required to store the information, but rather that the information must be captured and documented by the Medical Professional on the relevant medical health record for the patient in question possibly by way of transcription or periodic storage.

In a 2013 statement, the Department of Health stated that there was no prohibition on health organisations processing data offshore, provided the relevant risk assessments have been applied and implemented and are Data Protection Act compliant. Ultimately, Patient Data must not be transferred or stored outside the EEA unless the relevant data protection standards for such a transfer are met.

For Trusts, simply forbidding the use of Social Media Services, which are still used by Medical Professionals in respect of Patient Data will not be enough – they need to take more active steps, and providing a compliant alternative will help show that they have taken appropriate steps to protect the Patient Data for which they are responsible.

3. BACKGROUND

The healthcare sector and Medical Professionals handle, on a daily, even hourly basis, extremely sensitive personal data which patients not only expect, but have a right to expect, will be looked after and handled with the utmost care, confidentiality and security.

The Information Commissioner has taken active steps to investigate the breaches in respect of the handling of sensitive personal data within the healthcare sector, including breaches as a result of activities undertaken by Medical Professionals.

The handling and processing of personal data in the medical and healthcare sector is under careful monitoring and scrutiny and any and all technology providers working in the sector must be aware of the legal and ethical/moral standards required by Medical Professionals seeking to correctly and efficiently service patients. Any and all such technology providers must therefore ensure and provide appropriate assurances to Medical Professionals and medical organisations that the technology utilised and provided by them is appropriate and secure, and that the technology systems and services are used in accordance with local law and regulations governing the actions and omissions of Medical Professionals.

In addition to Medical Professionals' and ICT Businesses' strict adherence to legal and regulatory standards, it is important that all persons handling or accessing Patient Data comply with best practice standards with regards to the technology systems implemented in connection with such Patient Data processing and handling activities. The overarching data process' standards and restrictions must place patient safety and security at the forefront of any and all data protection, data professional and information security policies and transmissions.

4. INTRODUCTION: THE RISE OF SOCIAL MEDIA MESSAGING APPS WITHIN THE HEALTHCARE SECTOR

The Information Commissioner's Office and various NHS Trusts have recognised and publically commented on an increase in the use of Social Media Messaging Services between Medical Professionals where such communications centre on work matters or patient wellbeing, treatment plans and assessments.

Research among 287 doctors and 564 nurses working at the five hospitals in the Imperial College healthcare NHS trust in London found that 64.7% of the doctors were using SMS messages to send patient related clinical information, 46% had used picture messaging, while 33% had used app-based messaging[1] to send patient related information to their colleagues and 71.6% of doctors in the study wanted a secure way of sending such information.

Medical Professionals develop professional collaborative networks, partially on their own initiative, both physical and virtual in nature. Patient needs are the starting point for these networks, based on the idea that the various players in that network can offer the patient added value, service and knowledge source at different moments in time and from different locations. Medical Professionals have been exchanging sensitive Patient Data with one another via Social Media Messaging Services with the intention of efficiently sharing decisions and possible treatment plans with other Medical Professionals, whether to merely inform or seek approval for decisions, curb-side consultation, a second opinion, or for education, knowledge sharing or training purposes.

The use and advantages of Social Media Messaging Services by Medical Professionals has been researched and published in numerous publications on a global scale, many recognising the time saving benefits associated with the patient care work flow and secondly, better and more immediate opportunities for Medical Professional referrals to take place.

In light of the increasing use of Social Media Messaging Services by Medical Professionals for work related purposes, NHS Trusts have condemned Medical Professionals - not for communicating with other Medical Professionals, but rather for utilising Social Media Messaging Services that are not sufficiently secure, such security standards accounting for security information and also accounting for and appropriately protecting patient privacy and confidentiality in accordance with local laws, regulations and guidance relating to the handling of Patient Data. The use of inappropriate technology by Medical Professionals could result in inappropriate Patient Data handling and processing such as the inadvertent and unintentional storage of Patient Data on servers based outside of the EEA.

There is a general understanding that unless information is anonymised, Medical Professionals should not under any circumstances use existing consumer-focused Social Media Messaging Services. However, enforcing and controlling the manner in which Medical Professionals possibly share Patient Data over Social Media Messaging Services is a challenge for Trusts, their IT departments, clinical information officers, and Caldicott guardians largely because Social Media Messaging Services are used on personal devices of Medical Professionals for personal communications. The 'consumerisation of IT' is a growing trend which includes BYOD (Bring Your Own Device) policies and in order for employers, notably Medical Trusts, to authorise the use of technology providers and services on personal devices, employees must be informed of the business, legal, and security frameworks to which they and any technology providers they use or access for work related purposes must operate.

The sharing of Patient Data and information via Social Media Messaging Services, subject to the type of information being disclosed and transferred between Medical Professionals, may conflict with the requirements of a medical record under the Data Protection Act 1998 (and successor and related laws). Mobile Messaging Services in general must offer appropriate security strategies and assist Medical Professionals with their ongoing obligations of patient confidentiality and digital telecommunication security. Ultimately, the Medical Professionals will remain bound by the same rules that would apply to a Medical Professional when discussing, recording and transferring Patient Data and/or a patient medical record in person or by way of a telephone call, e-mail message or fax.

The NHS England's softening approach on the use of Social Media Messaging Services by Medical Professionals centres on the notion that any such communications must be of an anonymous nature unless and until the existing security and privacy

[1] Mobasheri MH, The ownership and clinical use of smartphones by doctors and nurses in the UK: a multicentre survey study. BMJ innovations 2015

landscape and concerns are addressed and security standards are sufficiently enhanced so as to be in line with the transmission and handling of medical records, of any format, in the professional healthcare environment. However, as has been stipulated elsewhere in this White Paper the anonymisation of Patient Data is not always appropriate or in the best interest of the patient, and therefore not an appropriate solution for Medical Professionals interested in Social Media Messaging Services and communication with their peers on work related matters.

To ensure Medical Professionals communicate with secure and appropriately tailored Mobile Messaging Services, it is important that the security standards to be adopted by such services targeting the medical and healthcare sector implement and comply with the highest information security and privacy standards. Below is a brief overview of the rules detailing patient confidentiality and technology standards and considerations to be had by Medical Professionals using Social Media Messaging Services.

5. THE LEGALITIES TO BE CONSIDERED BY MEDICAL PROFESSIONALS SHARING PATIENT DATA

Codes of practice and guidance on confidentiality obligations of Medical Professionals to their patients clearly stipulate that the duty to share information can be as important as the duty to protect patient confidentiality, especially in connection with the provision of safe, complete and effective patient care.

The General Medical Council has expressly stipulated that "the standards expected of doctors do not change because they are communicating through social media rather than face to face or through other traditional media. However, social media does raise new circumstances to which the established principles apply." It must therefore be noted and appreciated that in the first instance and as a general rule of thumb, the standards and main principles stipulated by the General Medical Council in respect of confidentiality ('Confidentiality: Good practice in handling patient information' – January 2017 – in effect from 25 April 2017) shall apply to all Medical Professionals, including those intending to communicate via Social Media Messaging Server and for that fact any Mobile Messaging Services, including Medical Messaging Services.

(i) Any personal information held by or in the Medical Professional's control should be effectively and appropriately protected against improper access, disclosure and loss at all times;
(ii) The Medical Professional should develop and maintain an understanding of information governance that is appropriate to his/her responsibilities;
(iii) The Medical Professional should know what Patient Data handling he/she can and should be undertaking and help within the perimeters of the law;
(iv) The Medical Professional should share relevant information only for direct care except where the patient has expressly objected;
(v) Where appropriate, the Medical Professional should ask for and obtain explicit written consent to disclose patient personal data for purposes other than care or local clinical audits unless the disclosure is required by law or is in the public interest;
(vi) The Medical Professional should inform patients of any and all Patient Data disclosure he/she intends to make that they would not otherwise expect, keeping a record of the discussion to disclose, not to disclose and the information disclosed; and
(vii) The Medical Professional should respect and always provide assistance and help to parties wishing to exercise their legal rights to be informed of how their information is used and how to access copies of such information.

The overarching principles detailed above should always be considered and borne in mind by Medical Professionals seeking to maintain an appropriate balance between confidentiality and disclosure of Patient Data, both in the interest of the patient.

A Medical Professional may disclose and share Patient Data over and above the rule on confidentiality where the following circumstances are established:

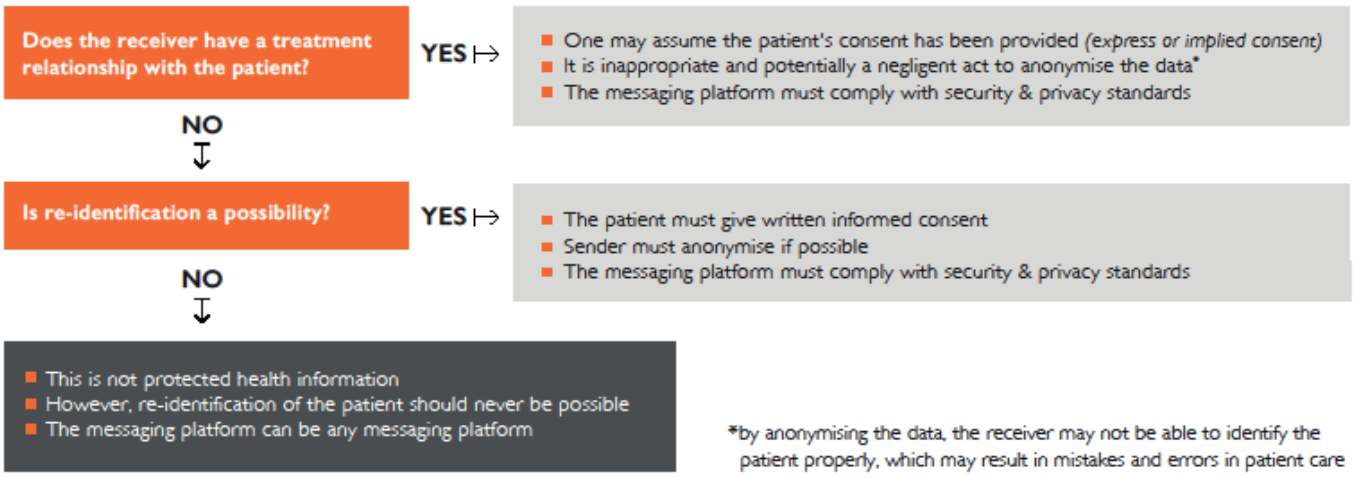
(1) Consent can be implied so as to ensure patient's care is maintained (such as Patient Data disclosure to persons involved in the treatment of the patient) or for a local clinical audit;
(2) Patient consent has been expressly granted;
(3) Disclosure and Patient Data sharing is of overall benefit to patients otherwise lacking capacity consent; or
(4) Disclosure is in the public interest.

The onus of ensuring any disclosure of Patient Data will not breach a patient's right to confidentiality vests with the Medical Professional disclosing such information, as it is this individual who has control over the confidential Patient Data to be transferred or data access to be granted to another Medical Professional. The receiving Medical Professional will gain control over the confidential information following the sharing and disclosure of the Patient Data, albeit potentially as a Data Processor acting under the instruction of the disclosing Medical Professional. Clearly identifying the Data Controller during the data transfer and sharing process is important in that it further clarifies the responsibilities on the relevant Medical Professionals.

Ultimately, Patient Data can be shared between Medical Professionals, including by way of a Mobile Messaging Service, provided the principles referenced above are followed and one of the permitted purposes for the disclosure and sharing of information taking priority over patient confidentiality applies.

Where Medical Professionals can establish that it is in the relevant patient's interest for their medical information to be disclosed to other Medical Professionals, it is important that the Medical Professional establishes what, if any, express patient consent is required in connection with such disclosure. In the first instance the Medical Professional must determine whether the receiving Medical Professional has an existing professional treatment relationship with the patient or not. This will ultimately determine whether patient consent is required for such disclosure and secondly whether the anonymisation of such Patient Data would be an inappropriate and potentially negligent act on the part of the Medical Professionals for not clearly identifying the patient that is being discussed when communicating within the medical team of the patient. This second aspect is emphasised in light of a widespread belief by the Medical Professional community that anonymising Patient Data is always the most appropriate way to utilise Social Media Messaging Services for work related purposes, where they don't want to risk breaching data protection laws and guidance thereto.

Fig.1 – Key questions posed by Medical Professionals prior to sharing patient data, immaterial of the format such patient data is stored or disclosed



The summary chart (above Fig.1) has been produced detailing the questions and steps to be taken by Medical Professionals seeking to share Patient Data with one another

How is Patient Data to be shared between Medical Professionals classified?

Having identified and clearly addressed the circumstances when Medical Professionals may share and disclose Patient Data with one another, it is important to consider how such Patient Data would and should be classified as rightfully so, such classification will impact the technological and security standards to be adopted by any and all third party technology involved in the processing, storage or handling of such data.

The Data Protection Act 1998 ("DPA") S68(2) defines a health record as one consisting of information relating to the physical or mental health or condition of an individual that has been made by or on behalf of a Medical Professional in connection with the care of that individual.

The type of information that may be shared between Medical Professionals on Mobile Messaging Services may qualify as a health record, for which additional security standards will need to be considered and provided by ICT Businesses supporting and providing these services to Medical Professionals.

The Information Governance Alliance stipulates that where Mobile Messaging Services are used as a means of communicating information for business purposes and a record is created through the social media platform then the communication may be deemed a record that needs to be kept by either the disclosing or receiving Medical Professional. The guidance further stipulates that the communications being information that would classify as a health record (in accordance with the DPA definition above) does not in itself mean that the Mobile Messaging Service is required to store

the information but rather that the information must be captured and documented by the Medical Professional on the relevant medical health record for the patient in question possibly by way of transcription or periodic storage. This clarification provided by the NHS provides a degree of comfort to Medical Professionals that they are the persons to establish what, if any, information obtained by way of curb-side consultations with fellow Medical Professionals should be formally recorded in a patient's medical record.

6. TECHNOLOGY AND SECURITY STANDARDS REQUIRED OF ICT BUSINESSES AND MEDICAL MESSAGING SERVICES OPERATING IN THE HEALTHCARE SECTOR

Consumer facing Mobile Messaging Services' target market is not and will not be the healthcare sector. Mobile Messaging Services offering their services to Medical Professionals must adhere to the additional security and privacy standards required of Medical Professionals. NHS Trusts have openly stated that the technology and security standards adopted by Social Media Messaging Services are inappropriate and insufficient with regards to the standards of care required of ICT Businesses operating within the health care sector. In part for these reasons, in addition to the lack of transparency, data storage and backup server locations being outside the EEA or not authorised to process Patient Data, the continued use of Social Media Messaging Services is of increasing concern to NHS Trusts and patients alike.

All operating systems must regularly account for technological developments identifying an individual to be responsible for implementing technological developments and undertaking appropriate security tests and updates. Given the nature of the information processed by Medical Professionals on a daily basis, businesses operating and providing services within the healthcare sector must provide enhanced security and IT standards than consumer facing businesses because of the sensitivity surrounding Patient Data.

It is important that ICT Businesses adopt clear and efficient processes for dealing with technological developments; data storage being restricted to what is strictly necessary, security incidents and breach notification and investigation, security checks and tests and restricted access to any and all information uploaded by Medical Professionals via the platform. ICT Businesses must ensure compliance with information security standards with a clear model for establishing, implementing, operating, monitoring and improving the efficiency of information security management within the business. For the NHS and all NHS related ICT Businesses these standards are stipulated in the NHS Information Governance Toolkit which may be further supported by way of ISO-27001 certification.

ICT Businesses operating within the healthcare sector, and more specifically offering Medical Messaging Services, must clearly detail and enforce procedures on timely and regular information and record deletion and exportation. If an ICT Business or Medical Messenger Service can offer secure, transparent mechanism to export communications or extracts of communications between Medical Professionals, a complete and secure service would be available to Medical Professionals, better supporting their ability to fulfil their duties to record and (where appropriate) transpose relevant curb-side consultation communication onto a patient's health record.

7. NHS APP APPROVAL AND ACCREDITATION

Recent NHS Information Governance Bulletins have noted that there is no valid reason why only apps that have been specifically approved by NHS England should be used or supported by Medical Professionals. However, this is an area of ongoing development and consideration and whilst guidance is somewhat limited, NHS Digital offers app developers focusing on the healthcare sector the opportunity to obtain NHS approval (see http://developer.nhs.uk/apps/).

The NHS approval process involves a review of the technical specifications, integration and interoperability with NHS IT infrastructure. Approval is ideally gained within a short timeframe (as little as four weeks) by involving all relevant NHS bodies, including IT Security teams. If an app is approved, it will classify as an appropriate app for use by any and all NHS Trusts and bodies. Furthermore, approval will result in the app being placed on the NHS Apps Library.

The establishment and approval of apps by NHS Digital remains, to a degree, uncharted territory. However, it would be sensible for any business looking to provide technology and/or app offerings to the healthcare sector to obtain or seek app approval from NHS Digital.

8. MEDICAL PROFESSIONALS' AND ICT PROFESSIONALS' RESPONSIBILITY FOR THE SECURITY STANDARDS IMPLEMENTED IN CONNECTION WITH MOBILE MESSAGING SERVICES

The Public Records Act 1958 expressly states that employees are responsible for any records they create or use in the course of their duties, including Medical Professionals creating records during the course of their employment and treatment of patients. Furthermore, the Information Security Management NHS COP expressly states that "all individuals who work within, or under contract to, an NHS organisation have a general responsibility for the security of information that they create or use in the performance of their duties. For example, security expectations may be described within any combination of contracts". The NHS guidance clearly states that all Medical Professionals, the trusts they work for and ICT Businesses offering Medical Messaging Services must adhere to appropriate and extensive security standards and that Medical Professionals are not in a position to relinquish their responsibilities to patients in respect of Patient Data security.

The responsibility of NHS Trusts, employers and Medical Professionals with regards to the security of Patient Data and ensuring appropriate technology and security standards are made available by the ICT Professionals, apps and platforms utilised by such Medical Professionals does not remove the ICT Professional's responsibility associated with implementing appropriate technology and security standards and ensuring appropriate tests and processes are in place to deal with any potential data breaches or attacks.

Provided a Medical Messaging Service does nothing or little more than providing a platform on which Medical Professionals can share Patient Data with fellow Medical Professionals on a safe, secure and technologically appropriate network, then the ICT Business offering the Medical Messaging Service would operate as a Data Processor in respect of any and all Patient Data uploaded by the Medical Professional onto the platform. The Medical Professional and their employers (whether a private practice or NHS Trust) would remain responsible for any and all compliance with all legislation and regulations that govern their actions in respect of patients and Patient Data and as such would be responsible as Data Controller to ensure Patient Data was processed and handled in accordance with data protection legislation.

The use of an appropriate and secure Medical Messaging Service tailored for use within the healthcare sector to better assist Medical Professionals when assessing and treating patients and providing curb-side consultations is nothing more than a new application of a well-established non-contentious custom and practice.

Backup of information by ICT Businesses

The current position on the storage and location of backup centres for identifiable Patient Data is not a clear cut one due to conflicting guidance and statements made by various Departments of Health. In a 2013 statement the Department of Health stated that there was no prohibition on health organisations processing data offshore provided the relevant risk assessments have been applied and implemented and DPA compliant. Ultimately Patient Data must not be transferred or stored outside the EEA unless the relevant data protection standards for such a transfer are met.

9. GDPR AND WHAT THIS MEANS FOR MEDICAL PROFESSIONALS AND ICT PROFESSIONALS

With the upcoming enforcement of the General Data Protection Regulation (the "GDPR") in May 2018, it is important that NHS Trusts, Medical Professionals and ICT Professionals are aware of their obligations under the GDPR as well as the increased risks associated with data protection breaches, both reputationally and financially.

The GDPR is centred on the principles of accountability, governance and transparency. All entities involved in the processing of data, with a particular concern in respect of sensitive and health related information, must put in place proportionate governance measures internally and with any contractors so as to minimise the risk of breaches.

With regards to Patient Data transferred and processed on a Mobile Messaging Service, the ICT Business (here being the Mobile Messaging Service company) would operate as a Data Processor. Processing information on behalf of a Data Controller must be stipulated in a processor agreement or in accordance with other permitted purposes set out under applicable data protection legislation together with relevant policies clearly identifying the roles, responsibilities and data security standards expected of the Data Controllers and Data Processors alike, transparency being key.

The key change to come into effect under the GDPR as opposed to the current legal framework for ICT Professionals handling and processing personal data on behalf of a Data Controller (in the current example the Data Controllers being the Medical Professionals or NHS Trust) would be that the Data Processors now have direct obligations in respect of the data and data processing activities undertaken on or via their platform. These obligations do not require the Data Processor to act or operate as a Data Controller but rather to maintain clear records of the types of processing activities undertaken by each Data Controller and notifying the Data Controller in the event of a breach. Which, amongst other things, is covered in the processor agreement between Data Controller and Data Processor.

Under the GDPR, fines associated with data protection breaches will be tiered, allowing for fines for some breaches of up to the greater of 4% of annual worldwide turnover and EUR 20m (although the Information Commissioner has publically stated that the highest level of fine will only be considered appropriate in exceptional circumstances). Specified breaches of data protection would attract fines of up to the greater of 2% of annual turnover and EUR 10m. The Information Commissioner has stated that the nature, gravity, duration of the infringement and whether basic principles such as consent have been sought by the Data Controllers would play an important part when considering what would be an appropriate fine for the breach in question. Ultimately, fines may be imposed immaterial of whether any harm or unauthorised information disclosure undertaken. The fine is intended to reflect the data protection breach.

For Trusts, simply forbidding the use of Social Media Services, which are still used by Medical Professionals in respect of Patient Data will not be enough – they need to take more active steps, and providing a compliant alternative will help show that they have taken appropriate steps to protect the Patient Data for which they are responsible.

10. LEGAL ANNEX

Public Body Guidance

- Caldicott review: information governance in the health and care system (26 April 2013)
- Department of Health, Information Security Management NHS COP (April 2007)
- General Medical Council – Confidentiality: good practice in handling patient information (January 2017 – in effect from 25 April 2017)
- General Medical Council – Consent: patients and doctors making decisions together (2 June 2008)
- General Medical Council – Doctor's use of Social Media (25 March 2013 – in effect from 22 April 2013)
- Health & Social Care Information Centre - Code of practice on confidential information (December 2014)
- Information Governance Alliance – Records Management Code of Practice for Health and Social Care (July 2016)
- Information Governance Review – Information: To share or not to share? (September 2013)
- NHS Digital – Acceptable Use User Guide (23 May 2017)
- NHS Digital – Data Handling: good practice guide (22 May 2017)
- NHS Digital – Telecommunications Security User Guide (23 May 2017)
- NHS Digital – Use of Social Media User Guide (23 May 2017)
- NHS England Information governance
- NHS Information Governance Bulletin 21 (January 2015)
- Royal College of General Practitioners – Social Media Highway Code (23 February 2013)

Legislation

- Data Protection Act 1998
- General Data Protection Regulation (2016)
- Health and Social Care Act 2012
- Health and Social Care (Safety and Quality) Act 2015
- Human Rights Act 1998
- National Health Service Act 2006
- Public Records Act 1958

Key links to obtaining NHS approval of a technology and security standards of a healthcare app

- https://developer.nhs.uk/apps/
- https://developer.nhs.uk/digital-tools/submit-your-app/
- https://developer.nhs.uk/testcentre/
- https://developer.nhs.uk/testcentre/itk-accreditation/
- https://developer.nhs.uk/testcentre/itk-cda-mesh-validator/
- https://digital.nhs.uk/codes-of-practice-handling-information
- https://www.england.nhs.uk/ourwork/tsd/ig/
- https://www.hhs.gov/hipaa/

11. CONTRIBUTORS

Adam Rose
Mishcon de Reya
adam.rose@mishcon.com
+44 20 3321 7197

Stefania Littleboy
Mishcon de Reya
stefania.littleboy@mishcon.com
+44 20 3321 7038

Dr Joost Bruggeman
Siilo
jbruggeman@siilo.com
+44 20 3868 7868

Arvind Rao
Siilo
arao@siilo.com
+44 20 3868 7868

Mishcon de Reya LLP
Africa House
70 Kingsway
London WC2B 6AH

T +44 20 3321 7000
F +44 20 7404 5982
E contactus@mishcon.com