Internal and Emergency Medicine (2020) 15:171–173
https://doi.org/10.1007/s11739-020-02292-5

IM-POINT OF VIEW

WhatsApp and other messaging apps in medicine: opportunities and risks

Marco Masoni[1] · **Maria Renza Guelfi**[1]

Received: 17 December 2019 / Accepted: 3 February 2020 / Published online: 15 February 2020

Abstract
WhatsApp is a popular messaging application frequently used by physicians and healthcare organizations that can improve the continuity of care and facilitate effective health services provision, especially in acute settings. However WhatsApp does not comply with the rules of the European GDPR and the US HIPA Act. So it is inappropriate to share clinical information via WhatsApp.
For this reason alternatives to Whatsapp are considered. In particular, the features that must have secure messaging apps to be in compliance with GDPR and HIPAA and to protect patient data will be discussed. The aim is to encourage healthcare organizations and physicians to abandon WhatsApp and to adopt one of the many secure messaging apps now available, some of them at no cost.

Keywords WhatsApp · Secure messaging apps · Data confidentiality · Regulation · GDPR · HIPAA

WhatsApp: use and regulatory concerns

WhatsApp is an instant messaging application created in 2009 and acquired by the Facebook family of companies in 2014. Mainly used with mobile devices, it also runs on desktop computers. Although asynchronous as e-mail, most users perceive WhatsApp as a synchronous communication tool.

The WhatsApp installation involves the transmission of the contacts list on Facebook Servers and it is possible to select manually the storage of messages. Communication through end-to-end encryption allows the maintainance of data confidentiality because only the sender and the receiver can decipher the message.

Physicians frequently use WhatsApp to communicate with peers. The clinical utility of this communication tool is now emerging, especially in acute settings [1, 2]. Other more general benefits are reported: communication improvement and streamline workflows, reduction of phone tags, decreased consultation time, promotion of a collaborative environment to improve the level of healthcare provided to patients [3].

As far as the European Community is concerned, the use of WhatsApp must comply with the General Data Protection Regulation (GDPR), which came into force in May 2018, a complex set of rules that allows EU citizens greater control over personal data.

The GDPR does not allow the storage of sensitive data of EU citizens on servers located outside the geographic area of the European Community. Furthermore, faced with a request for access to personal data (Subject Access Request—SAR), organizations are obliged to provide information and to correct or delete it. It is therefore mandatory that hospitals and healthcare centers know where and how the data are stored [4].

The GDPR rules apply to all EU countries without the intervention of national parliaments and they are mainly directed at organizations, which can suffer fines of up to €20 million or 4% of annual turnover. This will encourage hospitals and health organizations to closely monitor their employees so that GDPR rules are respected.

Since the installation of WhatsApp uploads contacts list and storages messages on servers outside the EU area, Facebook is not able to meet the rules of the GDPR and it

✉ Marco Masoni
m.masoni@med.unifi.it

Maria Renza Guelfi
r.guelfi@med.unifi.it

[1] Department of Experimental and Clinical Medicine, University of Firenze, Largo Brambilla 3, 50134 Florence, Italy

is therefore inappropriate to share clinical information via WhatsApp [5].

The same considerations also apply to other apps, such as online calendars, Dropbox and Google Drive, which store data in servers worldwide, making it extremely difficult to comply with the GDPR rules and to respond to SARs.

Obviously, these issues are known by the massive organizations that manage Internet services. WhatsApp has recently tried to tackle the problem by interrupting data sharing for EU users, but has failed to find a longer term solution that allows data sharing in line with the GDPR rules [4].

With regard to the United States, patients' right to data confidentiality is governed by the Health Insurance Portability and Accoutability Act (HIPAA). According to this law, no communication platform completely complies with its rules as this does not depend on how the software is made, but rather on how it is managed by users [6].

The lack of access control with an account, other than the one on the device, is the first obstacle to the use of WhatsApp for keeping patient data confidential. Any person who uses a smartphone can read WhatsApp messages and, if the screen is not locked, can see notifications to messages.

The possibility of deleting messages received and the inability of WhatsApp to keep a record of those sent is contrary to the HIPAA rules as it prevents the possibility of any audit. Furthermore, the replacement of the smartphone determines the impossibility to recover the messages, unless they have been backed up. Finally, if the employee leaves the organization, complete deletion of sensitive data is required. This can be complex and it cannot be performed remotely. The best solution would be to delete the account, an action that the user would probably reject [6].

Given the non compliance of WhatsApp with GDPR and HIPAA, its use puts the physician at risk to make errors in the management of patient data. Some suggestions that can be useful to use WhatsApp in an appropriate way to avoid regulatory investigation for not having taken the necessary steps to keep patient confidentiality are discussed below [7].

Firstly, when sending a message one of the most important precautions is always to make sure that the recipient is the right person. This is particularly true when there is a long list of contacts and there is no different group between contacts linked to the exercise of the profession and the ones that belongs to family and friends.

Secondly, when communicating it is good practice to avoid entering information that could lead to the recognition of the patient such as his name and surname, an identifier, the date of birth or home location. Sometimes a vague phrase like "the patient with autoimmune disease we saw yesterday morning" may suffice to break this rule. To this it should be added that the attempt to anonymize clinical images acquired via smartphone through editing and clipping, it may not be sufficient for the presence of accompanying metadata such as date, time, geographical coordinates together with the model of the mobile device [8].

The limitations of WhatsApp force us to explore alternative software that can be used in the healthcare environment.

Alternatives to WhatsApp

One ot the main limit in the development of messaging apps is that, unlike most internet services, there are no standards and Request For Comments that define a set of communication rules that these applications must respect to communicate. This results in a poor ability to share data between different applications.

Similar to Whatsapp, many other messaging apps exist [8]. Some are linked to Social Networking Sites (for example Facebook Messenger), while others (for example Telegram, and Vibes) are stand alone applications that do not need other software for their operation.

The main problem of these commercial messaging apps is that they are owned by companies whose main aim is to collect data from their users. For this reason it is difficult to imagine a future where these applications can satisfy the requests concerning the processing of personal health data both at european and US level. So WhatsApp, Messenger and Telegram seems only workarounds [9].

What healthcare systems need are Secure Messagging Apps (SMA) specifically dedicated to keep confidentiality of patient data. Beyond encrypting data within a private communication network, SMA must prevent data being sent outside the healthcare organization's network. Saving of sensitive data to external hard-drives or outside the organization's network must be avoided and administrative control must be available, deleting messages if the smartphone is stolen or lost (remote wipe) or after a predetermined period of time [10].

Siilo is an interesting SMA for the healthcare area. It is GDPR compliant and freely available from Apple and Google Play stores. It can save images, ECGs and other sensitive patient data in an encrypted manner on the personal mobile device, overcoming the restriction of storing information on remote servers. For this and other functionalities, many organizations are adopting Siilo as a tool for communication between employees. Hospify is another free SMA GDPR compliant, available from Apple and Google Play Store.

As far as HIPAA compliant messaging apps are concerned, an interesting Web site that compare features of different software is available at the URL: https://www.g2.com/categories/hipaa-compliant-messaging.

To date SMA are poorly interoperable with EHR systems. This makes difficult the simple transfer of messages containing diagnostic and therapeutic information to the

Table 1 Comparison of features of different secure messaging apps

Secure messaging apps	HIPAA or GDPR compliant	Cost	Integration with EHR
Siilo	GDPR compliant	Free	No
Hospify	GDPR compliant	Free (not Hub version)	No
Simple practice	HIPAA compliant	Not free	Yes
Oncall health	HIPAA and GDPR compliant	Not free	Yes
Tiger connect	HIPAA compliant	Not free	Yes
Trillian	HIPAA compliant	Not free	Yes

digital medical record. For this reason the communication left in the smartphone remains compartmentalized and in any case cannot be used formally. Some HIPAA compliant SMA come bundled with Clinical Communication and Collaboration Platforms that allow the integration of documents, images and messages with EHR systems [8]. Examples of this type of platforms are Trillian, SimplePractice, Tiger Connect and OnCall Health. Table 1 summarizes the main features of SMA discussed before.

As we see, many companies and start-ups are involved on implementing SMA, but their adoption among healthcare organizations is still scarce. Despite the uncertainties that accompany the use of WhatsApp, it continues to spread among physicians and healthcare workers [6]. Perhaps this seems tolerated due to the low occurrence of related adverse events to this date. Convenience seems to overcome mantainance of confidentiality of personal health data [9].

The use of SMA integrated with EHR could be an important step forward in the management of patient data. Healthcare organizations should implement policies related to the use of mobile devices and communications via messaging apps to be followed by physicians and other professionals. The switch to the use of these types of SMA should not be difficult because they are all user-friendly and work in a way similar to WhatsApp.

Conclusion

Compliance with the legislative provision related to the exchange of sensitive data must be considered equally important compared with the sharing of information that can improve the delivery of effective care. So WhatsApp is not an adequate tool to share clinical information due to its non compliance with the GDPR and HIPAA rules. Consequently healthcare organizations and physicians should abandon WhatsApp moving towards SMA able to keep confidentiality and security of patient data.

Compliance with ethical standards

Conflict of interest The authors declare that they have no conflict of interest.

Statement of human and animal rights This article does not contain any study with human and animals by any of the authors.

Informed consent For this type of study, formal consent is not required.

References

1. Johnston MJ, King D, Arora S, Behar N, Athanasiou T, Sevdalis N, Darzi A (2015) Smartphones let surgeons know WhatsApp: an analysis of communication in emergency surgical teams. Am J Surg 209(1):45–51
2. Astarcioglu MA, Sen T, Kilit C, Durmus HI, Gozubuyuk G, Kalcik M et al (2015) Time-to reperfusion in STEMI undergoing inter hospital transfer using smartphone and WhatsApp messenger. Am J Emerg Med 33(10):1382–1384
3. De Benedictis A, Lettieri E, Masella C, Gastaldi L, Macchini G, Santu C et al (2019) WhatsApp in hospital? An empirical investigation of individual and organizational determinants to use. PLoS ONEne 14(1):e0209873
4. John B (2018) Are you ready for General Data Protection Regulation? BMJ 360:k941
5. Hawkes N (2018) Sixty seconds on … Whatsapp. BMJ 360:K1041
6. Calleja-Castillo JM, Gonzalez-Calderon G (2018) WhatsApp in stroke systems: current use and regulatory concerns. Front Neurol 9:388
7. Mistry K (2018) Information governance considerations for staff on the use of instant messaging software in acute clinical settings. NHS. https://digital.nhs.uk/binaries/content/assets/website-assets/data-and-information/ig-resources/information-governance-considerations-for-individuals-on-the-use-of-instant-messaging-software-in-acute-clinical-settings.pdf. Accessed 20 Jan 2020
8. Thomas K (2018) Wanted: a WhatsApp alternative for clinicians. BMJ 360:k622
9. Bergeron D, Iorio-Morin C (2019) In reply to the letter to the editor "other apps beyond WhatsApp". World Neurosurg 130:568
10. HIPAA Journal. Secure messaging app. https://www.hipaajournal.com/healthcare-messaging-app/. Accessed 20 Jan 2020