WhatsApp-propriate? A retrospective content analysis of WhatsApp use and potential breaches in confidentiality among a team of doctors at a district hospital, South Africa

G D Meyer,[1,2] MB ChB; **N Meyer,**[1] MB ChB; **J D du Toit,**[1] MB ChB, Dip HIV Man (SA); **P A Mans,**[1,2] MB ChB; **B D Moffett,**[1] MB ChB

[1] *Zithulele Hospital, Eastern Cape Department of Health, Mqanduli, South Africa*
[2] *Department of Family Medicine, Faculty of Health Sciences, Walter Sisulu University, Mthatha, South Africa*

Corresponding author: *G D Meyer (gazmeyer@googlemail.com)*

Background. There has been a steady increase in the use of electronic media and instant messaging among healthcare professionals, where it has been almost universally adopted in the workplace. The use of WhatsApp and its perceived benefits in healthcare have been extensively studied; however, there are concerns regarding the potential for ethical breaches in confidentiality through shared electronic patient information.

Objectives. To identify the usage characteristics and incidence of shared patient information with WhatsApp use in a team of medical doctors in an unobserved and unregulated setting.

Methods. We conducted a retrospective cross-sectional content analysis of WhatsApp messages (n=3 340) among a team of 20 doctors in a South African district hospital over 6 months. All messages found within this time period were allocated unique identifiers. The text and image messages were thematically grouped into four categories, i.e. clinical care, resource allocation, social and administrative. Messages that contained patient-identifying information were included in the analysis.

Results. Of a total of 3 340 messages sent, 220 (6.6%) contained patient-identifying information. Of these, 109 (3.3%) contained non-anonymised patient information, while in 111 (3.3%) messages, the information was anonymised. The likelihood of sharing patient identifiers was proportionally much higher in shared images (odds ratio (OR) 5.1; 95% confidence interval (CI) 3.2 - 8.2; p<0.0001) compared with text messages, and in messages that related to clinical care (OR 9.3; 95% CI 2.2 - 38.8; p=0.0023) compared with those sent for resource allocation, and social or administrative purposes.

Conclusions. Non-anonymised patient identifiers were found in 3.3% of messages, constituting the potential for breaching patient confidentiality. While WhatsApp groups have significant utility in co-ordinating aspects of clinical care, resource allocation, as well as social and administrative functions, the safe use of WhatsApp should be promoted to ensure that patient confidentiality is maintained.

S Afr Med J 2021;111(2):171-175. https://doi.org/10.7196/SAMJ.2021.v111i2.14453

> *Confidentiality cannot but be, factually and morally, an all or nothing proposition.* (M H Kottow)[1]

Instant messaging (IM) is an internet-based service that allows rapid exchange of written messages and media between people using the same service on a computer or mobile device. It has been eagerly adopted by healthcare workers in the clinical setting to facilitate more efficient access to required information and communication between colleagues collaborating on patient management, which in turn has consistently been shown to improve the quality of clinical care delivery.[2-4] IM as a form of communication shares linguistic features of spoken and written language that, in a clinical setting, means it concurrently forms an unregulated stored written medical record, as well as a permanent transcript of conversations between medical professionals. This new form of patient information poses important questions about how to regulate and promote the ethical use of this modality, which is highly susceptible to inadvertent breaches in confidentiality.

The use of smartphone technology is common in the healthcare setting, where clinicians may access web pages and specialised applications (apps) to find information relevant to clinical cases; to aid in the formulation of management plans; to receive alerts or reminders; and to communicate with colleagues via a short message service (SMS) or IM service. WhatsApp is an IM service that is commonly used worldwide and is frequently used by medical practitioners.[5,6] The use of WhatsApp within clinical teams has been researched previously and concerns have been raised regarding the potential for improper disclosure through shared electronic patient information.[7,8]

The Constitution of the Republic of South Africa (SA) enshrines the right to privacy in the Bill of Rights,[9] which provides the legal framework upon which the National Health Act No. 61 of 2013[10] (NHA) ensures the legal requirement for patient confidentiality. Circumstances under which it is permissible to share patient information include: when the patient gives written consent, a court order to provide the information is issued, or where non-disclosure would represent a serious public threat. The NHA also makes provision for disclosure of patient information to other healthcare providers, as is necessary for any legitimate purpose within the ordinary course and scope of his/her duties where such a disclosure is in the interest of the patient.[10,11] Disclosure outside of these circumstances may hold professional or legal consequences,[11,12] and knowledge of the legal framework could assist in preventing inadvertent or ill-informed unlawful disclosure when using WhatsApp in a clinical setting. The need for specific ethical guidance has prompted the South African Medical Association (SAMA) and the Health Professions Council of South Africa (HPCSA) to issue formal guidelines on the use of social media,[12,13] reaffirming the conditions under which sharing of patient information on social media platforms such as WhatsApp is permitted. The ethical transmission and storage of WhatsApp messages are outlined in the HPCSA guidance on telemedicine, which places the onus on the healthcare practitioner to 'be satisfied that there are appropriate arrangements for the security of personal information when it is stored, sent or received by fax, computer, email or other electronic means'.[14] Practitioners who transmit electronic patient information are also responsible for ensuring that the recipient understands that the information is confidential.[15] Confidentiality is a foundational ethical tenet of the medical profession and should be carefully guarded.

In 2016, WhatsApp implemented a security feature known as end-to-end encryption, protecting users from any third party (including the company itself) accessing or intercepting a private message. However, concerns remain over the storage of messages and images once these have been delivered.[16] Since February 2019, WhatsApp enables password protection of the app – although this is still not an automatic feature. Potential access to messages in the event of a phone being stolen or lost is of concern, and O'Sullivan *et al.*[17] reported that 30% of the medical interns interviewed for their study had lost their smartphones within the preceding year. Images and videos may be stored directly to the smartphones photo cache, which may result in sensitive images being inadvertently downloaded onto the owner's personal computer or uploaded to online Cloud (Google, USA) storage services.

These potential breaches in confidentiality, coupled with the widespread use of WhatsApp in the UK, have resulted in the National Health Service issuing a formal advisory against the use of WhatsApp in clinical practice;[18] nonetheless, there has anecdotally been ongoing use.

The prospective nature of research into clinical use of IM has limited the investigation of the degree and nature of shared electronic patient information in an unregulated and unobserved setting within a single clinical team. It is a sound presumption that patient information is shared in WhatsApp groups in a clinical setting; however, the extent of shared patient-identifying features within these clinical discussions, representing the highest risk for breaches in confidentiality, is not known.

Objectives

The aim of this study was to identify the nature and extent of shared confidential electronic patient information in messages sent by a team of medical doctors within a WhatsApp group in an unobserved and unregulated setting.

Methods

Setting

A team of doctors from an SA hospital who preferentially used a shared IM forum on WhatsApp (referred to hereafter as the 'doctors' group') for communication within the team, was identified to participate in the study. All doctors employed at the hospital during the study period were active members of the group. The members included family physicians, the medical manager, part-time and full-time medical officers, community-service doctors and a dentist. No specific guidelines regarding messages posted on the group were in place prior to or during the study period. No member of the group was aware that the messages would be retrospectively analysed.

Design

This was a cross-sectional qualitative content-analysis study evaluating all WhatsApp messages sent on the doctors' group from 1 January to 30 June 2017.

Data collection and analysis

The group administrator provided a transcript of the group chat during the study period as a Microsoft Word (Microsoft Corp., USA) document using the 'export chat' feature on WhatsApp. All messages sent on the doctors' group during the study period were extracted for analysis. Each message was allocated an individual unique identifier that linked them to an individual thread. After this initial data review, information relating to the sender of the message, length, time and type of message (text, image, video, emoticon), thread length, content and subject matter, and presence of patient-identifying information were recorded on an Excel (Microsoft Corp., USA) database. The content of each message was categorised into one of four main themes, i.e. clinical, resource allocation, administrative and social. These themes were decided iteratively on analysis of the data and agreed upon by consensus between all authors. Messages were double coded by 2 authors to improve reliability of coding, and uncertainties were resolved by discussion among all authors.

Each message was also coded for whether or not it contained patient-identifying information, i.e. whether it referred to a specific patient. This was further divided into anonymised patient identifiers, i.e. messages referring to a patient who could not be identified directly by the content of the message (e.g. 'There is a 34-year-old male patient with a pneumothorax in the red room'); and non-anonymised patient identifiers, i.e. patient-identifying information was included in the message (e.g. 'Please book transport for Mr J Doe for surgery outpatients tomorrow'). Messages referring to groups of patients were not considered to be part of patient information, e.g. 'There are 20 patients waiting in casualty'. Once identified, messages containing patient-identifying information were further grouped by the type of information contained therein.

Ethical approval

Ethical approval was granted in 2017 by the Faculty of Health Sciences Postgraduate Education, Training, Research and Ethics Unit, Walter Sisulu University (ref. no. 048/2017). The site of research is not disclosed to protect the confidentiality of the clinicians involved. Consent was obtained from all participants prior to data collection.

Results

A total of 3 340 messages within 1 304 distinct conversations (or 'threads') were sent over a 6-month period – from 1 January to 30 June 2017 – by 20 participants in the doctors' group. The messages were analysed and categorised according to type of message, theme of message and whether they contained patient-identifying information (Fig. 1).

Of the 3 340 messages sent, 6.6% made reference to a specific patient (*n*=220), with 111 messages not expressly identifying a patient and 109 containing patient-identifying information. Only 3 of the 109 messages with patient identifiers were reported to have been sent with the patient's informed consent; therefore, 106 (3.2%) messages over the 6-month period could be considered as having the potential for a breach in patient confidentiality. Messages with patient-identifying information were a feature in every category, with 67 (3.6%) in the resource category, 33 (4.9%) in the clinical category, 7 (1.6%) in the social category and 2 (0.6%) in the administrative category. Of the patient-identifying messages, 25 were of images (12.8% of all images) and 84 were text messages (2.8% of all text messages). No videos or audio messages contained patient identifiers. The majority of text messages containing patient identifiers were requests for transport to a specialist clinic to be written in a centralised booking book (resource category: *n*=59). These messages contained the patient's name, the clinic and the date booked. Messages were more likely to have patient identifiers if they were images as opposed to text messages, with an odds ratio (OR) of 5.1 (95% confidence interval (CI) 3.2 - 8.2; *p*=0.0001). Clinically themed messages when compared with non-clinically themed messages, i.e. resources, social and administrative, were also more likely to have patient identifiers, with an OR of 1.8 (95% CI 1.2 - 2.7; *p*=0.0068) (Table 1).

A description of types of information in messages with patient identifiers could be grouped into:

- pictures of groups of patients with identifiable faces, e.g. in a waiting room
- photographs of patient records or hospital stationary, with visible patient details
- pictures of specific patients with either a question regarding clinical presentation or feedback on clinical outcome
- messages with patient details to trace the patient's location or clinical outcome
- messages to streamline bookings for referral services, which included the patient's name and the specialist clinic where they were booked, and date of booking.

Discussion

The chief concern with the use of WhatsApp for routine communication in clinical teams is the extent to which patient-identifying electronic information is shared in the group and stored on unsecured personal devices, posing a potential for breach of confidentiality. There is also the concern that being a consumer service with no user service agreement, WhatsApp has no relevant data security certification.[7] The degree and nature of shared patient-identifying information in an unregulated medical team IM group have not previously been investigated. However, it is generally presumed to be significant enough to dissuade the use of IM platforms in clinical settings. Despite these concerns, there is ongoing WhatsApp use among teams of healthcare providers.

Data were analysed retrospectively to mitigate the possibility of participants altering their messaging behaviour as a result of being observed. Of the 3 340 messages sent during the study period by the team of 20 participants, 220 contained information pertaining to specific patients and just fewer than half of these (3.3%; 109/3 340) contained patient-identifying information. This confirms that patient information is shared in an unregulated setting, but to a lesser degree than might have been expected.

This study did not attempt to adjudicate whether disclosure was justifiable in messages that contained patient information. Circumstances under which it would be acceptable to share patient information are laid out in the HPCSA handbook on confidentiality.[15] These circumstances could include disclosure of information to others who provide care, if the patient's express consent was given, or if the information was anonymised for the purpose of education. The study did not attempt to differentiate between patient information that was purposefully or inadvertently shared; to assess whether consent to share the information was given by the patient; or to assess the management of the information stored on the participants' devices. Shared patient information does not automatically equate to unlawful disclosure, and according to Opperman *et al.*,[11] 'the decision is very rarely made to share information on WhatsApp without the patient's consent or legal justification'.

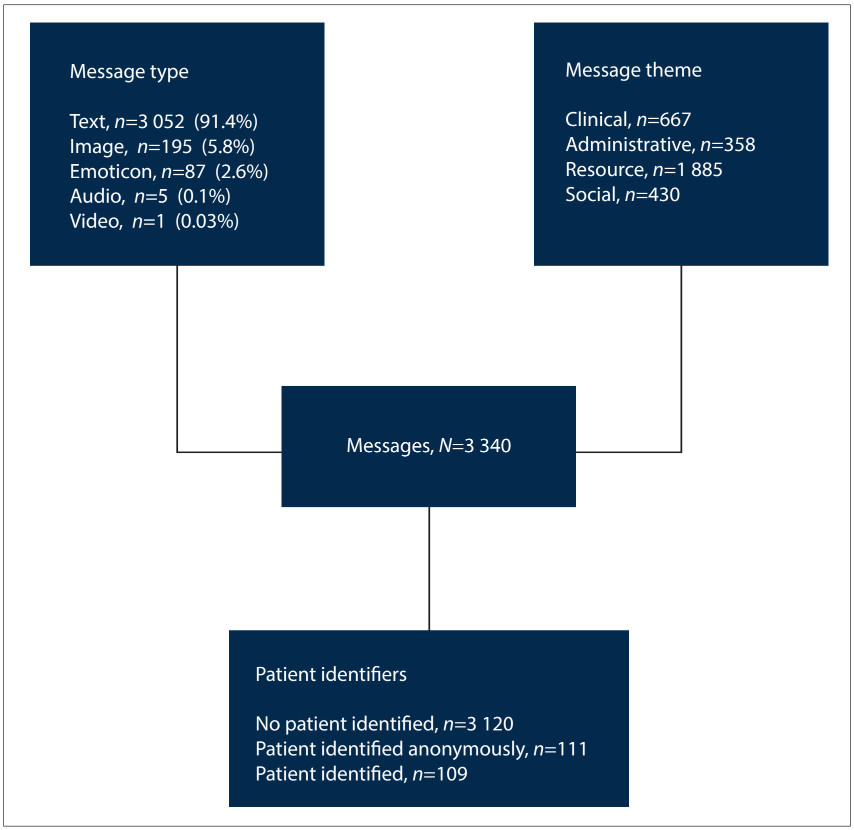

Fig. 1. Message categories of the doctors' WhatsApp group.

Table 1. Proportion of messages containing patient-identifying information

	Messages with patient identifiers	Messages, *n*	OR (95% CI)	*p*-value	Number needed to harm
Message by format					
Images	25	195	5.1 (3.2 - 8.2)	<0.0001	10
Texts	85	3 052	1		
Message by category					
Clinical	33	667	9.3 (2.2 - 38.8)	0.0023	23
Resource	67	1 885	6.6 (1.6 - 26.9)	0.0090	33
Social	7	430	2.9 (0.6 - 14.3)	0.18	94
Administrative	2	358	1		

OR = odds ratio; CI = confidence interval.

Images and clinically themed messages had the highest potential for containing patient-identifying information. The distribution of messages sent in this specific WhatsApp group is likely to have affected the extent of shared patient information, and in teams where more clinically themed messages and images are sent, a different rate may emerge. Awareness of these patterns could help inform users, managers and policymakers to guide the rational use of IM to minimise risk to patient information.

Images are also at highest risk of being saved to the personal image cache that may ultimately mistakenly be downloaded onto other personal devices, which further risks breaching patient confidentiality. Analysis of images with patient identifiers included images of results with visible patient details, photographs of groups or individual patients, images of patient notes and images of administrative documents, with patient names visible. An evaluation of text messages with patient identifiers showed that the majority included names of patients who requested transport booking in a centralised book (59 of 109 messages).

IM users should be aware of these risks, and steps to limit such risks should become commonplace.

Minor changes in WhatsApp use in clinical groups may result in significant reductions in potential ethical breaches (Box 1). The designated group administrator should be responsible for clearly stipulating the purpose and scope of the group, ensuring that the group has a code of conduct that is clearly understood by all members and that only essential members are included in the WhatsApp group, with prompt removal on leaving the department. A code of conduct should be clearly stipulated and agreed upon by all members of the group. Group members should be made aware of pitfalls in sharing sensitive patient-identifying information and be equipped with skills to avoid this, e.g. using the image-editing function on WhatsApp to obscure sensitive information. Group members should also ensure that their phones and WhatsApp applications are password protected and that sensitive information is not inadvertently downloaded onto other personal devices through the auto-download function. Unscheduled audits of the group WhatsApp feed should be conducted by the group administrator and/or other members of the group to ensure that the code of conduct is being upheld and to identify usage patterns that increase the burden of patient identifiers. These findings should be constructively fed back to the group and changes can be made to address these issues. For example, in this data set, as the majority of messages with patient identifiers were related to a WhatsApp co-ordinated booking system, an alternative booking system could drastically reduce the extent of messages with patient-identifying information.

Conclusions

The WhatsApp group in this study was used extensively by all members of the team, primarily as a team co-ordination tool, but also for clinically themed, administrative and social messages. Patient-identifying information was shared in an unregulated and unobserved WhatsApp group, and 3% of messages had patient identifiers. Images and clinically themed messages carry the highest risk of containing patient-identifying information. However, with good governance and the institution of clear WhatsApp use guidelines, the risks of sharing sensitive patient information may be minimised so that clinical teams may benefit from these shared IM platforms without risking breaches in patient confidentiality.

Study limitations

This study was limited to group discussions within a team of doctors that represents a portion of the total use of WhatsApp in a clinical setting; the total extent of patient information shared on IM in clinical practice falls beyond the scope of this research. As in the case of previous studies on the use of WhatsApp, this study was limited to messaging behaviours of a specific group chat involving a single team of doctors, and the findings may not represent widespread messaging behaviour.

Box 1. Practice points to optimise WhatsApp/IM groups in the clinical setting

Designated group administrator

- Clearly state purpose/scope of group
- Ensure 'group hygiene': making sure only essential members are part of the group
- Ensure that the code of conduct is upheld

Group members to agree on a code of conduct

- Confidentiality agenda to be agreed upon
- All phones should be password protected
- Auto-download feature should be turned off
- Consent to share information should be obtained before information is sent and should include the reason for sharing the information, what it may and may not be used for and to whom it will be sent. The conditions of consent should be made explicit to the receiving parties
- There must be strict guidelines on sending images, e.g. patient-identifying features to be obscured

Unscheduled audits of IM/WhatsApp feed

If regular sharing of sensitive information is a necessity, consider using more secure technology, e.g. Siilo (Siilo, The Netherlands)

IM = instant messaging.

Declaration. None.

Acknowledgements. We thank the staff at the participating hospital for their willingness to be involved in the research.

Author contributions. All authors were involved in developing the study protocol, collecting and analysing the data and editing the manuscript.

Funding. None.

Conflicts of interest. None.

1. Kottow MH. Medical confidentiality: An intransigent and absolute obligation. J Med Ethics 1986;12(3):117-122. https://doi.org/10.1136%2Fjme.12.3.117
2. Fernández-Valencia JA, Egea J, Pinyol MC, Orench M, Salas E, Gallart X. WhatsApp messenger for team coordination in surgical areas. Initial experience of a hip team in a third level hospital. Int J Adv Joint Reconstr 2015;2(1):23-25.
3. Martinez R, Rogers A, Numanoglu A, Rode H. Burns 2018;44(4):947-955. https://doi.org/10.1016/j.burns.2017.11.005
4. Astarcioglu MA, Sen T, Kilit C, et al. Time-to-reperfusion in STEMI undergoing interhospital transfer using smartphone and WhatsApp messenger. Am J Emerg Med 2015;33(10):1382-1384. https://doi.org/10.1016/j.ajem.2015.07.029
5. Statistica. Most popular mobile messaging apps worldwide as of July 2018, based on number of monthly active users (in millions). 2018. https://www.statista.com/statistics/258749/most-popular-global-mobile-messenger-apps/ (accessed 18 June 2018).
6. Wakefield J. Use of WhatsApp in NHS 'widespread', say doctors. BBC News, 6 July 2017. http://www.bbc.com/news/technology-40507440 (accessed 10 July 2017).
7. Johnston M, King D, Darzi A. Reply to the letter: WhatsApp with patient data transmitted via instant messaging? Am J Surg 2016;211(1):301-302. https://doi.org/10.1016/j.amjsurg.2015.06.005
8. Kubheka B. Ethical and legal perspectives on the medical practitioners use of social media. S Afr Med J 2017;107(5):386. https://doi.org/10.7196/samj.2017.v107i5.12047
9. South Africa. Bill of Rights, chapter 2, 1996.
10. South Africa. National Health Act No. 61 of 2003.
11. Opperman CJ, Janse van Vuuren M. WhatsApp in a clinical setting: The good, the bad and the law. S Afr J Bioethics Law 2018;11(2):102-103. https://doi.org/10.7196/SAJBL.2018.v11i2.643
12. Health Professions Council of South Africa. Professional Conduct and Ethics: Booklet 16. Ethical Guidelines on Social Media. Pretoria: HPCSA, 2019. https://www.hpcsa.co.za/Conduct/Ethics (accessed 10 February 2020).
13. South African Medical Association. Using social media: Practical and ethical guidance for doctors and medical students. https://www.samedical.org/nles/Guideline%20for%20Drs%20Using%20Social%20Media%20febr015.pdf (accessed 16 February 2020).
14. Health Professions Council of South Africa. Professional Conduct and Ethics: Booklet 10. Telemedicine. Pretoria: HPCSA, 2014. https://www.hpcsa.co.za/Conduct/Ethics (accessed 10 February 2020).

15. Health Professions Council of South Africa. Professional Conduct and Ethics: Booklet 5. Confidentiality: Protecting and Providing Information. Pretoria: HPCSA, 2016. https://www.hpcsa.co.za/Conduct/Ethics (accessed 10 July 2017).
16. Is WhatsApp HIPAA compliant? 2017. https://www.hipaajournal.com/whatsapp-hipaa-compliant/ (accessed 9 February 2020).
17. O'Sullivan DM, O'Sullivan E, O'Connor M, Lyons D, McManus J. WhatsApp Doc? BMJ Innovations 2017;3(4):238-239. https://doi.org/10.1136%2Fbmjinnov-2017-000239
18. National Health Service. Information Governance Bulletin No. 21, 2015. https://webarchive.nationalarchives.gov.uk/20160606050915/http://www.england.nhs.uk/wp-content/uploads/2015/01/ig-bull-21.pdf (accessed 10 July 2017).

Accepted 5 August 2020.