Are app-based platforms safe for communicating patient health Information?

Klaudiusz Stoklosa BSc[1,2]; Roberto V. P. Ribeiro MD PhD(c)[2]; Alun Ackery MD[3]; Bobby Yanagawa MD PhD[2]

[1]Faculty of Medicine, University of Toronto
[2]Divisions of Cardiac Surgery, St. Michael's Hospital, University of Toronto
[3]Emergency Medicine, St. Michael's Hospital, University of Toronto

We live in a post-digital world where photos, videos, and messages can be transmitted instantaneously with the click of a button. From our clinical experiences, many Canadian physicians are still reliant on pagers, fax machines, telephone calls, and hand-written notes for health-related communication. Today, there are a plethora of alternative communications platforms in the form of mobile device applications (Apps). These App-based platforms include WhatsApp (www.whatsapp.com), PageMe (www.pagemeapp.com), Hypercare (www.hypercare.com), ShareSmart (www.sharesmart.ca), Telmediq (www.telmediq.com), and PetalMD (www.petalmd.com), each with unique strengths and weaknesses. Physicians already routinely use WhatsApp and equivalent platforms in their clinical practice in many jurisdictions within Ireland, USA, and the UK among others.[1-3] Here, we argue that an updated telecommunication policy incorporating the use of App-based communications platforms is needed.

In Canada, each provincial and territorial governing body is responsible for overseeing and enforcing access and privacy laws with unique information security safeguard standards (Table 1). In Ontario, the Personal Health Information Protection Act (PHIPA) and Information and Privacy Commissioner (IPC) set

Table 1. Provincial and territorial governing bodies responsible for overseeing and enforcing access and privacy laws

Province/Territory	Governing body responsible for overseeing and enforcing access and privacy laws	Privacy law relating to health records	Website link to privacy law
Alberta	Office of the Information and Privacy Commissioner of Alberta	Health Information Act	http://www.qp.alberta.ca/documents/Acts/H05.pdf
British Columbia	Office of the Information and Privacy Commissioner for British Columbia	E-Health (Personal Health Information Access and Protection of Privacy) Act	http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_08038_01
Manitoba	Office of the Ombudsman	The Personal Health Information Act	http://web2.gov.mb.ca/laws/statutes/ccsm/p033-5e.php
New Brunswick	Office of the Integrity Commissioner for New Brunswick	Personal Health Information Privacy and Access Act	http://laws.gnb.ca/en/showfulldoc/cs/P-7.05//20190819
Newfoundland and Labrador	Office of the Information and Privacy Commissioner Newfoundland and Labrador	Personal Health Information Act	https://www.assembly.nl.ca/legislation/sr/statutes/p07-01.htm
Northwest Territories	Office of the Information and Privacy Commissioner Northwest Territories	Health Information Act	https://atipp-nt.ca/wp-content/uploads/2016/03/Health-Information-Act.pdf
Nova Scotia	Office of the Information and Privacy Commissioner Nova Scotia	Personal Health Information Act	https://nslegislature.ca/legc/bills/61st_2nd/3rd_read/b089.htm
Nunavut	Office of the Information and Privacy Commissioner of Nunavut	Consolidation of Access to Information and Protection of Privacy Act	https://atipp-nu.ca/wp-content/uploads/2018/04/consolidation-of-access-to-informationand-protection-of-privacy-act.pdf
Ontario	Information and Privacy Commissioner of Ontario	Personal Health Information Protection Act	https://www.ontario.ca/laws/statute/04p03
Prince Edward Island	Information and Privacy Commissioner of Prince Edward Island	Freedom of Information and Protection of Privacy Act	https://www.canlii.org/en/pe/laws/stat/rspei-1988-c-f-15.01/latest/rspei-1988-c-f-15.01.pdf
Quebec	Commission d'accès à l'information du Québec	Act Respecting the Protection of Personal Information in the Private Sector	http://legisquebec.gouv.qc.ca/en/pdf/cs/P-39.1.pdf
Saskatchewan	Office of the Saskatchewan Information and Privacy Commissioner	The Health Information Protection Act	https://pubsaskdev.blob.core.windows.net/pubsask-prod/8623/H0-021.pdf
Yukon	Yukon Information and Privacy Commissioner	Health Information Privacy and Management Act	http://www.gov.yk.ca/legislation/acts/hipm_c.pdf

Abbreviations and acronyms:
CMPA - Canadian Medical Protective Association
IPC - Information and Privacy Commissioner
NHS - National Health System
PHI - Personal health information
PHIPA - Personal Health Information Protection Act
VPN - Virtual private network

Corresponding Author:
Klaudiusz Stoklosa
klaudiusz.stoklosa@mail.utoronto.ca

Table 2. WhatsApp application-specific precautions on Apple and Android products with the potential to maximize privacy safeguards

1. Block WhatsApp from downloading media onto mobile device albums This feature allows users to prevent the automatic download of media products, such as pictures of patients' medical presentations. Consequently, all media shared through WhatsApp conversations remains restricted to the secure platform. Users must fulfill all three sets of steps under Apple or both sets of steps under Android
2. Enable screen lock Although WhatsApp does not currently allow password locks on the application, screen lock is an equivalent feature on iPhones. When combined with the "Immediately" option, screen lock will require users to unlock the application using the same biometric (Face ID or Touch ID) they use to unlock their phone. After several attempts users will be able to input the security code used to unlock their iPhone. This feature keeps the conversations on the application secure even if the phone is lost or stolen or if someone outside the circle of care takes the custodian's unlocked iPhone. Although Android does not currently offer screen lock options, it is recommended to download and use a third-party locking application on WhatsApp. This is the equivalent to the iPhone screen lock feature.
3. Disable iCloud and Google Drive backups WhatsApp automatically creates unencrypted backups unless this feature is disabled. Disabling unencrypted cloud backups is the safest thing step that can be done to ensure unencrypted copies of PHI are not created.
4. Enable two-factor authentication Two-factor authentication, also known as two-step verification, adds an additional periodic passcode to a user's WhatsApp. The secure six-digit PIN is requested when logging onto WhatsApp using a different device thereby decreasing chances of someone accessing a user's account without their consent. This feature also periodically requests the PIN after opening WhatsApp. The six-digit PIN cannot be shared with anyone.
5. Continuously check for and update WhatsApp application Updating WhatsApp ensures the application is up-to-date and contains patches for potential vulnerabilities. These updates are released as the company finds security weaknesses, such as following cyberattacks. Regularly checking and updating the application keeps users' conversations safe from security breaches.
6. Disable message previews This feature protects patient privacy since users receive message notifications. The contents of the conversation are not shown. Users must open the WhatsApp conversation to view the message.
7. Set password lock All mobile devices must have a password lock that only the user knows. Passcode must be required immediately upon turning on the device from sleep mode. Smartphone password locks should not be a simple pattern, consecutive numbers, or repetitions of the same digit. Longer number combinations are more secure than shorter combinations. The safest password locks are those that include special characters, numbers, and capital and lower-case letters.
8. Use the official WhatsApp desktop application rather than WhatsApp Web Although WhatsApp Web offers several more features than the official WhatsApp desktop application, it can easily be manipulated and thus has bigger security threats. The official WhatsApp desktop application is safer to use if looking to use WhatsApp on a laptop.
9. Double-check the conversation's end-to-end encryption Although unnecessary, verifying that the end-to-end encryption works is a quick way to provide peace of mind that the privacy safeguards are working in that conversation.
10. Enable security notifications This feature allows for a notification to be sent when a security code changes. Security codes change when a new phone or laptop accesses an existing chat such as when one of the conversation participants switches their WhatsApp to a new phone. Always double-check the conversation's end-to-end encryption following a change in the security code.
11. Beware of phishing scams The most common phishing scams originate from unfamiliar phone numbers and discuss a premium version of WhatsApp (WhatsApp Gold) or the user account's expiring. There are no premium versions of the application and WhatsApp will always be free of charge. Users should contact WhatsApp for more information about suspicious messages.
12. Protect your privacy on WhatsApp This option prevents non-contacts from being able to learn information about users. This also prevents other people from being able to reverse image search a user's profile photo to learn more information about the custodian. It is best to keep "Read Receipts" enabled (i.e. "on") to facilitate other custodians knowing if their messages have been read.
13. Audit group conversation membership Users should regularly audit the participants of a group chat, particularly if the user is the group chat admin, to check for unauthorized members such as people not within the circle of care.

forth requirements for administrative, physical, and technical safeguards, including encryption, to keep personal health information (PHI) secure on mobile devices.[4,5] However, the onus is on healthcare practitioners, hospitals, and community health facilities to determine whether a given communication platform is compliant, safe, and secure.[6] As such, there is much discordance across the country with regards to which messaging platforms are secure for the transmission of PHI.

Through consulting with Information Technology Departments of several Canadian hospitals, we found that most groups favoured the so called 'trusted' modalities – fax machines, hospital pagers, and encrypted email servers – for communication between and amongst physicians and trainees. Many institutions currently discourage or ban App-based communication platforms due to privacy concerns. Their concerns include the lack of control over who can access conversations, as well as the fear that companies could mine or sell sensitive PHI. However, such concerns surrounding the confidentiality of PHI using these platforms may stem in part from our lack of understanding of how these applications store and transmit information.[7] Significant security and privacy gaps are often overlooked and downplayed when comparing traditional communication technologies to new platforms. For example, fax machines allow healthcare providers to share patient information with one another as many electronic health record systems are not interoperable. Although fax machines may be difficult for outside users to hack electronically, sensitive PHI can be mistakenly sent to the wrong fax number or faxes could be picked up by unintended persons, thereby breaching patient privacy. Likewise, hospital pagers may transmit critical messages, particularly in acute emergencies, but are nonetheless time-consuming, unencrypted, and easily intercepted.[8] Furthermore, pagers lengthen consult and referral wait times; this disrupts the flow of communication within circles of care since users are often unaware of the content or urgency of pages and whether the other party has received the message. Although encrypted email servers, such as eHealth Ontario's ONE Mail, may provide expedited communication, they require secure transmission and cooperation between sender and receiver to be safe. Only emails sent from one clinician's ONE Mail account to another ONE Mail user are secure. Moreover, sensitive emails can be unintentionally, albeit permanently, sent to an incorrect recipient.

We are currently addressing health-related communication in a 21st-century technological world with 20th century tools. Today, safe communication alternatives that adhere to provincial and

Table 3. Steps on Apple and Android products to enact WhatsApp application-specific precautions

Precaution	Steps on Apple & Android Products
Block WhatsApp from downloading media onto mobile device albums	1. Apple: WhatsApp>Settings>Data and Storage Usage>Media auto-download>Never>Tap onto each of these four to disable auto-downloads: photos; audio; videos; documents. 2. Apple: Settings>WhatsApp>Photos>Never. 3. Apple: WhatsApp>Tap on conversation>Tap on group/member name in the chat window>Save to Camera Roll>Never. 1. Android: WhatsApp>Settings>Data and Storage Usage>Media auto-download>Disable auto-downloads>Tap onto each of these three to disable auto-downloads: when using cellular data; when connected on Wi-Fi; when roaming. 2. Android: WhatsApp>Tap on conversation>Tap on group/member name in the chat window>Media visibility>No.
Enable screen lock	Apple: WhatsApp>Settings>Privacy>Screen Lock>Require Face ID/Touch ID>Immediately. Android: Download and use a third-party locking application.
Disable iCloud and Google Drive backups	Apple: WhatsApp>Settings>Chats>Chat Backup>Auto Backup>Off. Android: WhatsApp>Menu>Settings>Chats>Chat Backup>Backup to Google Drive>Never.
Enable two-factor authentication	Apple: WhatsApp>Settings>Chats>Chat Backup>Auto Backup>Off. Android: WhatsApp>Menu>Settings>Chats>Chat Backup>Backup to Google Drive>Never.
Continuously check for and update WhatsApp application	Apple: Appstore>Updates>WhatsApp>Update (if WhatsApp is already updated the button will say "Open" otherwise it will say "update"). Android: Google Play Store>Menu icon (top-left corner)>My Apps & Games>WhatsApp>Update (WhatsApp will only appear on the list of apps to be updated only if an update is available).
Disable message previews	Apple: WhatsApp>Settings>Notifications>Show Preview. Flip the toggle to white (i.e. "off"). Android: Settings>Apps>WhatsApp>Notifications>Message Notifications>On the lock screen>Hide sensitive notification content.
Set password lock	Apple: Settings>Touch ID/Face ID & Passcode>Passcode. On the Touch ID/Face ID & Passcode page: Require Passcode>Immediately. Android: Settings>Security>Screen lock.
Use the official WhatsApp desktop application rather than WhatsApp Web	Apple & Android: Visit whatsapp.com/download and click on the "supported versions" that is appropriate for your laptop.
Double-check the conversation's end-to-end encryption	Apple & Android: Start conversation in WhatsApp>Tap contact's name in chat window>Encryption>QR code and 40-digit security code. Manually verify if the 40-digit security code is the same for all users in the conversation either in person or using a different messenger application (i.e. not WhatsApp). Alternatively, ask the contact to scan your QR code using the WhatsApp application or you scan their QR code using the "Scan Code" button.
Enable security notifications	Apple & Android: WhatsApp>Settings>Account>Security>Show security notifications. Flip the toggle to green (i.e. "on").
Beware of phishing scams	Apple & Android: Do not open the message if it is from an unfamiliar number. Delete the suspected message.
Protect your privacy on WhatsApp	Apple & Android: WhatsApp>Settings>Account>Privacy. For maximum efficiency and security set Profile Photo and About to "Nobody" and Last Seen and Status to "My Contacts".
Audit group conversation membership	Apple & Android: WhatsApp>Tap on conversation>Tap on the group chat name in chat window>View the participants to check for unauthorized members within the group. To delete unauthorized members the group admin must: WhatsApp>Tap on conversation>Tap on the group chat name in chat window>Tap on unauthorized participant (under "Participants" section)>Remove from Group.

territorial privacy laws exist and should be considered as adjuncts to our traditional communication armamentarium. WhatsApp is one such example. WhatsApp is currently the most commonly used messaging application worldwide, with over 1.5 billion accounts and 500 million daily users.[9,10] Clinicians can send medical photos to colleagues, see the moment their messages are opened, and instantly receive real-time feedback, all at no charge. It should therefore come as no surprise that our informal multi-hospital survey of 50 Canadian residents and clinicians found the use of WhatsApp to communicate PHI despite the platform often being prohibited by hospitals. When used securely, WhatsApp can potentially support patient care by facilitating rapid communication, encouraging interprofessional collaboration, and flattening hierarchies by allowing junior trainees to propose management plans and ask questions critical for their learning.[11] WhatsApp also has a potential role in helping coordinate healthcare teams with tasks such as managing acute medical crises, including trauma cases, to ongoing public health concerns, such as coordinating care during the COVID-19 pandemic. Delivery notifications and read receipts, including the exact time a message was read, offer accountability in communication.[12] WhatsApp therefore allows for accountable, efficient, and instantaneous interdisciplinary communication that would otherwise be difficult or even impossible through fax machines, pagers, and encrypted emails.

WhatsApp incorporates security features that allow users to enable in-app precautionary features to maximize privacy safeguards to levels compliant with province- and territory-specific health record privacy laws.[13] It employs default end-to-end encryption based on Signal Protocol with advanced encryption standard key lengths of 256-bits, which exceed the 128-bit minimum currently set by the PHIPA and IPC.[4,14] These security algorithms are designed to prevent anyone, inside and outside the company, from creating master keys to decrypt and read conversations, or mine and sell PHI. The application also allows users 4096 seconds (68 minutes, 16 seconds) to permanently delete sensitive messages that were unintentionally sent to individuals outside the circle of care.[15] Despite being targeted by large-scale security breaches in the past, WhatsApp ultimately offers stronger barriers against hacking and interception of PHI than our current hospital communication platforms. Properly following specific security precautions can help further maximize WhatsApp's compliance with current provincial and territorial regulations (Table 2 and Table 3) and keep PHI safe.[13,16-19] Canadian app-based platforms specially created for medical use, including PageMe, Hypercare, ShareSmart, Telmediq, and PetalMD, provide potentially even safer alternatives. Unlike WhatsApp, these app-based platforms can only be used by healthcare workers in clinical settings. This helps prevent medical messages being sent to non-healthcare professionals. Regardless of the encrypted communication platform chosen, safety of PHI should remain front and center. This can be done using encrypted mobile devices and a virtual private network (VPN) when using unsecured Wi-Fi networks. As with any tool, these platforms

should be incorporated into clinical practice with appropriate user training for safe application use. The Canadian Medical Protective Association (CMPA) does not have an official position on this issue, but advises clinicians using App-based platforms to follow provincial and territorial privacy standards indicating that electronic exchanges are explicit forms of communication and must therefore be included in the patient's medical record.

It is our position that a blanket ban on the use of all app-based communication platforms risks their off-label use, which places patient's privacy in far greater danger compared to finding ways to integrate this technology into clinical settings safely. A recent US study found 'inconvenience' as the most significant self-reported barrier to compliance with communication policy, with 58% of residents having violated regulatory standards by sending PHI through unencrypted text messages.[20] Another survey reported 30-50% of medical professionals are already routinely using messaging applications in their clinical practice.[2] Given the impact of COVID-19, the United States Department of Health and Human Services recently liberalized privacy law compliance guidelines allowing the use of encrypted app-based platforms, such as WhatsApp, iMessage, and Zoom, for telehealth purposes.[21] It is important to acknowledge that our widespread reliance on telemedicine during the COVID-19 pandemic, both in Canada and the United States, will likely continue long after social distancing measures subside. Therefore, our professional societies must understand the strengths and weaknesses of each platform and provide guidance to safe usage of communication platforms so that we can safely embrace and benefit from the newest innovations, while simultaneously upholding patient privacy.

The current speed of advances in app-based communication technology is remarkable. We call on our provincial regulatory bodies and professional medical societies to continually reassess and offer guidance to healthcare professionals on the safe use of app-based communication platforms for medical purposes as part of a technological vision for the future. In the United Kingdom, the National Health System (NHS) has already made great strides towards a fully digitized NHS, a critical part of their Technological Vision and NHS Long Term Plan.[22,23] To this end, the NHS is phasing out the use of fax machines and hospital pagers for non-emergency medical communications by 2020 and 2021, respectively, with a transition to their in-house messaging application.[24,25] We need a multidisciplinary working group of experts and stakeholders – health professionals, technological specialists, patient advocates, lawyers, ethicists, and others – to outline a Canadian telecommunication vision for the future with patient privacy and security front and center. Such a group could continuously monitor cybersecurity advancements and test new applications against up-to-date security standards to provide healthcare custodians with a verified list of secure communication apps and instructions on safe usage. Overall, finding ways to safely integrate app-based platforms into clinician's communication toolboxes will bring us closer towards a modernized healthcare system.

References

1. O'Reilly MK, Nason GJ, Liddy S, et al. DOCSS: doctors on-call smartphone study. Ir J Med Sci. 2014;183:573-577.
2. Visvanathan A, Hamilton A, Brady RRW. Smartphone apps in microbiology – is better regulation required? Clin Microbiol Infect. 2012;18:218-220.
3. Thomas K. Wanted: a WhatsApp alternative for clinicians. BMJ. 2018;360:k622.
4. Fact sheet: health-care requirement for strong encryption [Internet]. Information and Privacy Commissioner of Ontario. 2010 [cited 2019 Apr 15]. Available: www.ipc.on.ca/wp-content/uploads/resources/fact-16-e.pdf.
5. Fact sheet: communicating personal health information by email [Internet]. Information and Privacy Commissioner of Ontario. 2016 [cited 2019 Apr 15]. Available: www.ipc.on.ca/wp-content/uploads/2016/09/Health-Fact-Sheet-Communicating-PHI-by-Email-FINAL.pdf.
6. Personal health information protection act, 2004, S.O. 2004, chapter 3, schedule A. Ministry of Health and Long-Term Care. 2004 [cited 2019 Apr 15]. Available: www.ontario.ca/laws/statute/04p03#top.
7. Kamel Boulos MN, Giustini DM, Wheeler S. Instagram and WhatsApp in health and healthcare: an overview. Future Internet 2016;8(37).
8. Unencrypted hospital pager messages intercepted and viewed by radio hobbyist. HIPAA Journal. 2018 [cited 2019 May 12]. Available: www.hipaajournal.com/unencrypted-hospital-pager-messages-intercepted-viewed-radio-hobbyist.
9. Clement J. Number of daily active WhatsApp status users from 1st quarter 2017 to 1st quarter 2019 (in millions). Statista. 2019 [cited 2019 Jul 13]. Available: www.statista.com/statistics/730306/whatsapp-status-dau.
10. Giordano V, Koch H, Godoy-Santos A, et al. WhatsApp messenger as an adjunctive tool for telemedicine: an overview. Interact J Med Res 2017;6(2):e11.
11. De Benedictis A, Lettieri E, Masella C, et al. WhatsApp in hospital? An empirical investigation of individual and organizational determinants to use. PLoS ONE 2019;14(1):e0209873.
12. Johnson L. 22 WhatsApp hacks to turn you into a messaging master. Digital Spy; 2019 [cited 2019 Aug 14]. Available: www.digitalspy.com/tech/apps/a780553/whatsapp-tips-and-tricks-to-turn-you-into-a-messaging-master.
13. Patkar M. 8 tips to make WhatsApp more secure and private. MakeUseOf. 2017 [cited 2019 May 2]. Available: www.makeuseof.com/tag/whatsapp-secure-tips.
14. WhatsApp encryption overview: technical white paper. WhatsApp. 2016 [cited 2019 Apr 22]. Available: www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf.
15. Griffin A. WhatsApp to allow people to delete messages for everyone long after they are sent. Independent. 2018 [cited 2019 May 12]. Available: www.independent.co.uk/life-style/gadgets-and-tech/news/whatsapp-unsend-delete-for-everyone-how-to-long-time-minutes-hour-show-chat-a8241981.html.
16. Phillips G. WhatsApp breached: update your app to stay safe. MakeUseOf. 2019 [cited 2019 Jul 15]. Available: www.makeuseof.com/tag/whatsapp-breached-update-stay-safe.
17. Zhukova A. How safe are my photos on WhatsApp? MakeUseOf. 2019 [cited 2019 May 2]. Available: www.makeuseof.com/tag/safe-photos-whatsapp.
18. Patwegar W. How to disable WhatsApp message previews on Android phone. Techbout. [cited 2019 Aug 14]. Available: www.techbout.com/disable-whatsapp-message-previews-on-android-phone-30713.
19. Mohan K. How to stop WhatsApp from sharing your data with Facebook. Gadgets Now. 2018 [cited 2019 May 2]. Available: www.gadgetsnow.com/how-to/how-to-stop-whatsapp-from-sharing-your-data-with-facebook/articleshow/63766022.cms.
20. McKnight R, Franko O. HIPAA compliance with mobile devices among ACGME programs. J Med Syst 2016;40(129).
21. FAQs on Telehealth and HIPAA during the COVID-19 nationwide public health emergency. US Department of Health and Human Services Office for Civil Rights. 2020 [cited 2020 May 17]. Available: https://www.hhs.gov/sites/default/files/telehealth-faqs-508.pdf.
22. The future of healthcare: our vision for digital, data and technology in health and care. Department of Health & Social Care 2018. [cited 2019 Aug 15]. Available: www.gov.uk/government/publications/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care/the-future-of-healthcare-our-vision-for-digital-data-and-technology-in-health-and-care.
23. NHS long term plan. NHS. [cited 2019 Aug 15]. Available: www.longtermplan.nhs.uk.
24. Health and social care secretary bans pagers from the NHS. Gov.uk. 2019 [cited 2019 Aug 15]. Available: www.gov.uk/government/news/health-and-social-care-secretary-bans-pagers-from-the-nhs.
25. NHS to phase out pagers by end of 2021. HIPAA Journal. 2019 [cited 2019 Jul 17]. Available: www.hipaajournal.com/nhs-phase-out-pagers-by-end-of-2021.