Computing systems, telehealth, and personal data: what is up?

Maria Inês Meurer (iD) *

Universidade Federal de Santa Catarina, Centro de Ciencias da Saude, Florianopolis, SC, BR.

*Corresponding author. E-mail: meurer.m.i@ufsc.br

Dear Editor,

I have read with great interest the comment published by the team coordinated by Prof. Paulo Sergio da Silva Santos (1), where the authors emphasized the importance of dentists (in particular a specialist in Oral Medicine) and Teledentistry strategies in the COVID-19 pandemic. I have been following the work of this nationally recognized team, known for their experience and excellence in the hospital environment, offering qualified dental care for patients with special medical needs. Personally, I have deep respect for their contribution to the multi-professional interaction in healthcare.

Considering the pandemic scenario, the authors highlighted, in their publication, the convenience of telehealth strategies in the exchange of health information. They also suggested the use of non-dedicated instant messaging and video calling applications to enable remote communication.

As an oral medicine specialist and a member of the team that has developed and recently launched a tele(oral) medicine service linked to the Brazilian Unified Public Health System (*Sistema Único de Saúde* - SUS) in the state of Santa Catarina (2), I would like to share some concerns about the use of non-dedicated platforms/softwares/applications for the exchange of health data.

Health data are considered sensitive data under the Brazilian General Data Protection Law (known as *Lei Geral de Proteção de Dados* - LGPD) (3). Sensitive data is a subcategory of personal data that represents a higher risk for the individual due to the discriminatory or harmful potential of its content (4). Similar attention is also given to sensitive data in the European Union (General Data Protection Regulation - GPDR) (5) and in the United States of America (Health Insurance Portability and Accountability Act - HIPAA) (6).

A number of requirements need to be met for the safe transit of sensitive health data through computer networks, which include the guarantee of confidentiality, authenticity, integrity, availability and non-retroactivity (timestamping) (7,8). Some additional processes are also involved depending on the situation, such as those related to digital signature and certification (7). Non-dedicated platforms/softwares/applications, despite their popularity and the eventual support of data encryption, are not the ideal choices for sharing sensitive data as they do not meet most of these requirements (9,10).

Information and communication technologies are increasingly impacting our personal and professional routines. Adapting to the changes imposed by technology requires expanding our field of knowledge (and thinking) beyond the health field.

The Brazilian LGPD comes into effect in September 2020. Since then, the use of systems/softwares/applications that do not meet the security requirements for sharing, archiving and deleting health data can result in major problems for health professionals. Thus, it is essential that we increase our understanding about these issues and change our practices to provide health care safely and ethically, through the virtual environment.

I appreciate the opportunity to respectfully and constructively share my point of view. May we all remain safe and healthy.

■ REFERENCES

1. Telles-Araujo GT, Caminha RDG, Kallás MS, Santos PSDS. Teledentistry support in COVID-19 oral care. Clinics (Sao Paulo). 2020;75:e2030. Available from: https://www.clinicsjournal.com/article/teledentistry-support-in-covid-19-oral-care/
2. Meurer MI, von Wangenheim A, Zimmermann C, Savaris A, Petrolini VA, Wagner HM. Launching a public statewide tele(oral)medicine service in Brazil during COVID-19 pandemic. Oral Dis. 2020. https://doi.org/10.1111/odi.13528
3. Brasil. Lei N° 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados) [Internet]. Brasil; 2018. Available from: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm
4. Kameda K, Pazello M. e-Saúde e desafios à proteção da privacidade no Brasil. In: Keinert TMM, Sarti FM, Cortizo CT, Paula SHB de, editors. Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo: Instituto de Saúde; 2015. p. 49-62. portolivre.fiocruz.br/proteção-à-privacidade-eacesso-às-informações-em-saúde-tecnologiasdireitos-e-ética
5. European Parliament and Council of European Union. Regulation (EU) 2016/679 - General Data Protection Regulations (GDPR) [Internet]. European Union; 2016. Available from: https://gdpr-info.eu/
6. U.S. Department of Health & Human Services. The Health Insurance Portability and Accountability Act of 1996. Pub. L. 104-191. Stat. 1936. [Internet]. 1996. Available from: https://www.hhs.gov/sites/default/files/privacysummary.pdf
7. Nobre LF, Wangenheim A von, Maia RS, Ferreira L, Marchiori E. Certificação digital de exames em telerradiologia: um alerta necessário (Digital certification in Teleradiology: a necessary warning). Radiol Bras. 2007;(6):415-21. https://doi.org/10.1590/S0100-39842007000600011
8. Vivanco CR, Marin H de F, Lira ACO de. Segurança da informação eletrônica em saúde: aspectos físicos, lógicos, éticos e legais. In: Keinert TMM, Sarti FM, Cortizo CT, Paula SHB de, editors. Proteção à privacidade e acesso às informações em saúde: tecnologias, direitos e ética. São Paulo:

Instituto de Saúde; 2015. p. 247-78. portolivre.fiocruz.br/proteção-à-privacidade-eacesso-às-informações-em-saúde-tecnologiasdireitos-e-ética

9. Masoni M, Guelfi MR. WhatsApp and other messaging apps in medicine: opportunities and risks. Intern Emerg Med. 2020;15(2):171-3. https://doi.org/10.1007/s11739-020-02292-5

10. Sabbatini RME. Utilizando WhatsApp e outros comunicadores instantâneos para dispositivos móveis em Medicina: o bonito, o feio e o malvado [Internet]. Revista de Segurança da Informação em Saúde. 2020 [cited 2020 Jul 14]. Available from: https://medium.com/p/315d315d905c