Telecommunications: The Disconnect Between Medical Practice and Medical Education

Rebecca Afford[1]

Citation: UBCMJ. 2019: 10.2 (29-30)

Abstract

Innovations in telecommunications have reinvented the delivery of medical education, but the change in medical curricula may be lagging behind the rapid expansion of the use of these technologies in medical practice. Specifically, the use of smartphones is a mainstay for communicating between colleagues and to inform clinical decision–making. Medical education must therefore inform students of the risks associated with securing patients' confidential information. By analyzing the current state of personal electronic device usage by medical trainees clinically, practical solutions to secure patient information and protect healthcare professionals can be implemented into undergraduate and graduate medical programs.

Telecommunication is continuously expanding its niche in medicine. Not only is it changing medical education by connecting learners hundreds of kilometers away to their peers and mentors, it is also shaping the practice of medicine by connecting professionals and patients virtually instantly. Personal devices are used almost ubiquitously to inform clinical practice and maintain communication. Because of this popularity, medical learners begin using personal devices early in their training. Medical education should prepare learners for their future medical practice, but how is the prospective use of telecommunications being taught now?

Virtual connectedness has changed the medical profession as personal devices are at arm's reach in scrub pockets and beside call–room beds. They have become reference tools and a means of communication. In a 2018 study by Guo et al., medical learners at the University of British Columbia (UBC) from all stages in their education were surveyed regarding their use of personal cellphones.[1] Out of the respondents, 98% stated that they have used text messaging as a part of their medical training, but 9.1% were not aware of the security settings on their phones.[1] Furthermore, 27% said their phone was backed up to a cloud while 30.5% were unsure of their backup settings.[1] The location of the cloud in question was not further specified. The study only asked about the utilization of cellular devices in practice, not tablets nor laptops. A similar survey was completed by fourth–year medical students at the University of Toronto, yielding the following results: 26% of students not having any security features on their phones, 68% believing that personal devices pose a risk for patient privacy and confidentiality, and 22% communicating patient–identifiable information via their devices.[2] Although the majority of learners are using password protection or encryption on their phones, text messaging can also be forwarded to other devices such as tablets, laptops, and desktops in real–time. This creates an added layer of complexity to protecting patient information. Moreover, the use of applications or "apps" was not a part of these questionnaires. A multitude of apps have been developed for exchanging and obtaining clinical information as well as informing clinical decision–making. They have become pocket resources for trainees to develop differential diagnoses, determine investigations, and guide management. Some apps allow users to communicate in groups with the added benefit of encryption, such as WhatsApp. Unfortunately, some of these apps, including the aforementioned, use servers located outside of Canada to store information which, by means of the British Columbia Personal Information Protection Act, is a breach of patient confidentiality if messages contain identifying information.[3] Furthermore, these studies only captured students at two universities. Without formal, public data published for most medical schools across the country or open access to the curriculum of each school, it is difficult to compare how Canadian medical programs are addressing this topic. The University of Alberta outlines required privacy and confidentiality training for clinical, non–clinical, and research staff, but not for trainees.[4] On the East Coast, Memorial University's Medical Student Code of Conduct states, "The discussion of a patient and the handling of their medical record shall not violate their confidence."[5] This objective is clear, but relies upon the judgment of the student, which potentially may not be informed by privacy and confidentiality policies. The use of devices is inevitable and becoming increasingly more prevalent, dependent upon in practice, but with this comes increasingly more complex safeguards to protect private information.

The prevalence of telecommunications in medicine has been addressed by the Canadian Medical Protection Agency (CMPA). The CMPA recognizes the "pervasiveness and convenience" of communication via text messaging and email, but also warns that these modalities are prone to misdirecting to the wrong recipient as well as having information held in databases outside of Canada.[6] Governing bodies, such as the BC College of Physicians and Surgeons, have released similar standpoints.[7] Overall, the Canadian medical community recognizes the concerns associated with the prevalence of personal devices in clinical practice, but the benefits of efficiency may outweigh the perceived risks. This sentiment has been echoed by patients.[8] Patients generally prioritize communication and rapid access to healthcare over the protection of their personal information.[8] Despite this, the risks of confidentiality breaches are not zero. Since medical students receive clinical exposure early on in their education, medical curricula should continue to reinforce the importance of technological stewardship in medical practice.

So, what can be done? Legislation regarding privacy and confidentiality puts the onus on the custodian of sensitive information to regulate its security.[6] Therefore, as medical professionals it is our

[1]MD Program, Faculty of Medicine, University of British Columbia, Vancouver, BC, Canada

Correspondence
Rebecca Afford (r.afford@alumni.ubc.ca)

responsibility to not only be guardians of our patients' wellness, but also of their privacy and personal information. Currently, the Faculty of Medicine at UBC provides introductory modules as well as lectures during transitioning periods of medical education to address issues regarding personal devices and personal information of patients. UBC Information Technology has created the Privacy and Information Security Management (PrISM) Program, which provides online modules that provide step–by–step, device–specific instructions to encrypt and secure personal devices, as well as an overview of privacy and confidentiality policies.[9] These modules are available to any UBC student or staff. As of August 2018, all UBC employees, including clinical clerks, are now required to complete these modules.[10] As most Canadian medical programs have adopted cased–based or problem–based learning sessions into their curriculum, application of safe telecommunication practices may be woven into these regular small–group sessions. Furthermore, attending physicians and residents have the opportunity to impart conceptual and practical knowledge to students during clinical experiences. Physicians in these leadership positions can role model and reinforce secure telecommunication practices to encourage students to consolidate previous teaching on the clinical use of personal devices. Practical experience handling patient information electronically is especially pertinent for the clerkship and elective years. The next generation of healthcare professionals will need to adapt to an evolving tech–savvy climate, which is providing an exciting, innovative means of connecting patients and providers.

Personal devices, especially smartphones, are proving to be just as, if not more pervasive than a stethoscope in modern medicine. Current medical education has relied mainly on didactic learning to present this information to medical trainees. Unlike the practical physical examination and procedural skills that are routine in medicine, the practical training to safely use telecommunications is lacking. By practicing technological stewardship, we can further foster a trusting relationship with our patients and further explore the possibilities of these devices in medical practice.

References

1. Guo D, Phan N, Ho K, Pawlovich J, Kitson N. Clinical texting among medical trainees of the University of British Columbia. *J Cutan Med Surg*. 2018 Jul/Aug;22(4):384-389.
2. Tran K, Morra D, Lo V, Quan S, Abrams H, Wu R. Medical students and personal smartphones in the clinical environment: the impact on confidentiality of personal health information and professionalism. *J Med Internet Res*. 2014 May;16(5):e132.
3. Personal Information Protection Act, BC [Internet]. Chapter 63 [cited 2018 Oct 7]. Available from: http://www.bclaws.ca/EPLibraries/bclaws_new/document/ID/freeside/00_03063_01
4. University of Alberta Faculty of Medicine and Dentistry. Privacy and security training requirements by role [Internet]. 2018 [cited 2018 Nov 25]. Available from: https://cloudfront.ualberta.ca/-/media/medicine/aboutus/informatics/privacy-and-security-training-requirements-by-role-nov-12-2015.pdf
5. Memorial University Faculty of Medicine. Medical Student Code of Conduct [Internet]. 2018 [cited 2018 Nov 25]. Available from: https://www.med.mun.ca/getdoc/baacb6b5-c2af-4647-9b15-5532af540643/Medical-Student-Code-of-Conduct.aspx
6. Canadian Medical Protective Association. Using electronic communications, protecting privacy [Internet]. 2013 [updated 2016 Jan; cited 2018 Oct 7]. Available from: https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2013/using-electronic-communications-protecting-privacy
7. British Columbia College of Physicians and Surgeons. Practice Standard. Telemedicine [Internet]. 2015 [updated 2018 Mar; cited 2018 Oct 7]. Available from: https://www.cpsbc.ca/files/pdf/PSG-Telemedicine.pdf
8. Walker J, Ahkern DK, Le LX, Delbanco T. Insights for internists: "I want the computer to know who I am". *J Gen Intern Med*. 2009 Jun 24(6):727-732.
9. The University of British Columbia. Privacy Matters @ UBC. Fundamentals Training. [cited 2018 Oct 7]. Available from: https://privacymatters.ubc.ca/fundamentals-training
10. Ono S. Data security – new requirements for UBC faculty and staff [Internet]. The University of British Columbia; 2018 Oct 11 [cited 25 Nov 2018]. Available from: https://faculty-staff.ubc.ca/2018/10/11/data-security-new-requirements-for-ubc-faculty-and-staff/