Balancing Health Information Exchange and Privacy Governance from a Patient-Centred Connected Health and Telehealth Perspective

A Contribution from the IMIA Organizational and Social Issues and Telehealth Working Groups

Craig E. Kuziemsky[1], Shashi B. Gogia[2], Mowafa Househ[3], Carolyn Petersen[4], Arindam Basu[5]
[1] Telfer School of Management, University of Ottawa, Ottawa, Ontario, Canada
[2] Society for Administration of Telemedicine and Healthcare Informatics, New Delhi, India
[3] College of Public Health and Health Informatics, King Saud Bin Abdul Aziz University for Health Sciences, King Abdullah International Medical Research Center, Riyadh, Saudi Arabia
[4] Senior editor at Mayo Clinic, Rochester, Minnesota, United States
[5] University of Canterbury School of Health Sciences, Christchurch, New Zealand

Summary

Objectives: Connected healthcare is an essential part of patient-centred care delivery. Technology such as telehealth is a critical part of connected healthcare. However, exchanging health information brings the risk of privacy issues. To better manage privacy risks we first need to understand the different patterns of patient-centred care in order to tailor solutions to address privacy risks.

Methods: Drawing upon published literature, we develop a business model to enable patient-centred care via telehealth. The model identifies three patient-centred connected health patterns. We then use the patterns to analyse potential privacy risks and possible solutions from different types of telehealth delivery.

Results: Connected healthcare raises the risk of unwarranted access to health data and related invasion of privacy. However, the risk and extent of privacy issues differ according to the pattern of patient-centred care delivery and the type of telehealth being used. Online consumer health telehealth tools pose a particular challenge as they enable the highest degree of connectivity and thus the greatest potential for privacy breaches.

Conclusion: Privacy issues are a major concern in telehealth systems and patients, providers, and administrators need to be aware of these privacy issues and have guidance on how to manage them. This paper integrates patient-centred connected health care, telehealth, and privacy risks to provide an understanding of how risks vary across different patterns of patient-centred connected health and different types of telehealth delivery.

Keywords

Telehealth, privacy, patient-centred care; connected healthcare

Yearb Med Inform 2018:48-54
http://dx.doi.org/10.1055/s-0038-1641195

1 Introduction

Societal and demographic changes coupled with rising costs of healthcare delivery have challenged us to design innovative new models of care delivery to support health and social care in the community. Community-based care delivery is complex due to the need to manage patient care across multiple settings and providers. Thus, a recent focus of health systems research has been the development of new models of care delivery that support the exchange and integration of patient data across providers and settings [1-3]. Central to these new models of care delivery is an emphasis on patient-centred care. Health transformation cannot be viewed solely from a technical or economic perspective but needs to be viewed from a patient-centred perspective where care delivery tasks are coordinated according to relevant patient's needs [4].

However, patient-centred care delivery introduces new challenges. Foremost is the need to integrate patient data across multiple providers and settings. This integration is referred to as *connected health*, defined as "the delivery of process-driven collaborative health management and healthcare practice by individuals, healthcare professionals, patients and/or carers through the support of technology (software and/or hardware)" [5]. Connected health is not a system or a technical infrastructure but rather describes the conceptual underpinning of what is needed for care delivery in different combinations of settings and care delivery models. The basis of connected healthcare delivery is sending and receiving health information (HI) across multiple touchpoints to enable and monitor patient-centred community care delivery over time. However, this introduces several issues including organizational, social, literacy, interoperability, and security and privacy issues [6-9]. Each of these issues presents a unique system design challenge and while research exists on all of them a shortcoming is that many solutions are at a macro level and do not always scale down to the micro level where care delivery is provided [10, 11]. A failure to account for contextual differences in translating from macro solutions to micro implementation is what leads to unintended consequences such as impaired communication, patient safety, or workflow issues [8].

Telehealth, broadly defined as the provision of health care delivery, resources, and education through electronic information and communication technologies [12], is a fundamental part of connected healthcare delivery as it enables the connection of people, processes, and information across different settings. Telehealth is especially important for rural and remote communities where in-person access to services may be limited [13]. Over time, the use of telehealth has evolved and there exist several different ways that telehealth can enable connected healthcare delivery including education, service delivery, care monitoring, and training [12].

However, the governance of telehealth has not followed the pace of evolution of the different ways used to support healthcare delivery. One example is privacy governance. The protection of patient privacy is a key concern with telehealth-enabled connected healthcare delivery. Privacy and telehealth have been well studied at the macro level such as the frameworks for the Internet of Things, mobile technologies, or population level frameworks for protecting data privacy [14, 15]. However, these macro level approaches do not always scale down effectively to front line micro level care delivery. Li et al. point out that clinicians using telehealth at a micro level often encounter challenges at organizational (meso) or policy (macro) levels because of a lack of alignment between the telehealth policy level and the micro level where front care delivery is provided [16].

While integrating different sources of data (e.g., demographic, lifestyle, and behavioural data) can support both person-centred care delivery and public health decision-making, we also know that achieving this vision can pose serious challenges and threats to security and privacy [17]. To address these challenges and support the translation of macro level policy into micro care delivery settings, health information technology (HIT) designers need to better understand the unique workflow and data requirements in different healthcare contexts [18]. A first step to achieving this is to develop a business model of patient-centred telehealth delivery in order to understand the variations in how health information (HI) exchange differs across various telehealth delivery models. Some of these differences are related to the specific telehealth functions being utilized (e.g., viewing versus editing data, and education versus service delivery) while organizational and location contexts also impact the manner in which telehealth is used.

For the first time in the IMIA *Yearbook*, we examine the above challenge from the combined perspective of two working groups. The Organizational and Social Issues Working Group focuses on socio-technical, organizational, social, and ethical issues surrounding the introduction and use of informatics applications, whereas the Telehealth Working Group has a mandate to collaborate and disseminate research on the use of technology to foster the delivery of telehealth, particularly in low-resource or community-based settings.

The contribution of this paper is to propose the integration of patient-centred connected health, telehealth, and privacy issues in order to develop a business model of patient-centred care via telehealth. Our paper is outlined as follows. Section 2 describes patient-centred connected health. Section 3 describes telehealth and privacy standards. Section 4 integrates the two previous sections to develop a business model for patient-centred connected health via telehealth. Section 5 describes how to operationalize this business model by linking telehealth types, patient-centred HI patterns, and privacy issues and solutions. We conclude with a summary and present the next steps following our findings.

2 Patient-Centred Connected Health

In patient-centred care, practitioners put the patient in the centre of care planning. Donald Berwick coined three slogans about this practice: "*patient's need is the only need*", "*every patient is the only patient*", and "*nothing about me without me*" [19]. These slogans suggest the primacy of patients in patient-centred care and the duty of practitioners to remove barriers to patients' access to their personal HI. Patient-centred care is a broad term that encompasses different types of interactions that vary from one patient to the other based on individual circumstances. Patient-centred care has been defined as care that is "respectful and responsive to individual patient preferences, needs, and values and ensuring that patient values guide all clinical decisions" [20]. Patient-centred care typically involves asking patients about their goals and priorities related to their health and care, giving patients information about their health situation and care options, including them in decisions about care, and working with them after decision making to ensure that their needs are being addressed appropriately.

Some general scenarios (use cases) in which patients can benefit from being able to access personal HI from their medical record include, but are not limited to:

- Checking laboratory and other test results rather than requesting results from a health care provider by telephone or waiting until the next appointment. Results should also be available in a more fruitful physical interaction [21]
- Checking prescriptions to ensure that they are using medication correctly [22]
- Reviewing information in EHRs to identify inaccuracies and inform providers about corrections (e.g., missing symptoms, incorrect dates/dosages) [23]
- Reviewing treatment protocols and schedules for follow-up appointments and related activities [24]
- Checking EHRs to ensure that electronically submitted patient-reported outcomes and patient-generated health data (e.g., motion sensor data) were received and integrated completely and accurately [25]
- For non-custodial parents, regularly checking the EHR for awareness of children's health problems in case they become ill during visitation or at times the custodial parent cannot be reached [26]
- For caregivers/custodians of vulnerable adults (e.g., dementia patients, individuals with intellectual disabilities, persons with severe mental health conditions), checking the EHR to plan and manage medication use, appointment scheduling, and other functions [27].

The above use cases highlight that patient-centred connected health is not one type of connectivity but rather that there are several different contexts of connectivity ranging from one-to-one HI retrieval, to view data, to many-to-many interactions that send and receive data multiple times. Telehealth support for these different contexts of connected health and the governance of these different contexts will also be varied.

3 Telehealth and Privacy Standards

Telehealth arose from telemedicine which tried to create access for care processes for those unable to physically access healthcare processes. In telehealth, information created for clinical care may be further utilized for data analytics to enable evaluation and planning of health strategies and achieve other organizational objectives. However, health information has the potential of being misused and the creation and dissemination of information through telehealth can undermine the privacy and confidentiality of patient information. The International Standards Organization (ISO) has created a variety of standards for the protection and management of health information. One has to ensure not only that such information is managed responsibly, but also that the access to health information is allowed to accountable persons who can maintain information security as noted by ISO Standards # ISO/IEC 2382-8:1998 & ISO/IEC 27000:2009 [28, 29].

Several privacy standards and protocols exist that pertain to the exchange of HI via telehealth such as ISO Standards 62304, 82304, and 80001 [30-32], which specifically target health data security as a concern with mention of various stakeholders, whether vendors, hospitals, or patients. These standards are linked to existing standards for specific aspects, for example the Risk Management Process of medical devices, which is addressed by ISO 14971 [33]. Protocols for information security described in ISO 27799 [34] describe the rules for information governance and privacy guidelines for the entire life cycle of information from creation to its eventual destruction, whether entered physically or through electronic means. Unfortunately, increasing amounts of memory, faster speeds, and better methods of access mean that governance and ensuring compliance are both very challenging. Cloud-based systems have eased the access to information but they have also increased privacy risks. Rules and processes concerning pseudonymization of data for analytics have also been created which contain principles for privacy protection of patient health information [35].

Although ISO rules provide a standard to regulate health information collection and dissemination, there is a noticeable difference between various parts of the world in how privacy standards are created, valued, or used. For example, in the United States, in addition to the utilization of ISO standards, the Healthcare Insurance Portability and Accountability Act (HIPAA) (HIPAA; Pub.L. 104–191, 110 Stat. 1936, enacted August 21, 1996) was created to ensure that all health information – not only technology-based information – available to insurance providers is governed properly. Within developing countries, however, privacy is not regarded as a primary concern by healthcare service organizations or professionals because meeting population basic health needs is more important than maintaining high levels of patient privacy and confidentiality [36].

4 Business Model for Patient-Centred Connected Health via Telehealth

While there exist numerous technologies and methods to support connected healthcare delivery, there is a considerable lack of guidance and an inability to establish effective business models to support the design and evaluation of connected health delivery [37]. The previous two sections described patient-centered care delivery and privacy standards relevant for telehealth. Figure 1 shows our business model integrating the two sections. The model illustrates that patient-centered connected care delivered by telehealth encompasses different patterns of HI exchange that will result in different privacy issues and governance implications.

In the two sections below we articulate the two components of the model. First, we define a set of patient-centred connected health patterns and then we describe privacy implications of the patterns.

4.1 Patient-Centred Connected Health Patterns

Section 2 described several different use cases for how technology can support patient-centred connected health. While the different use cases are well described in the literature, the governance of the dif-

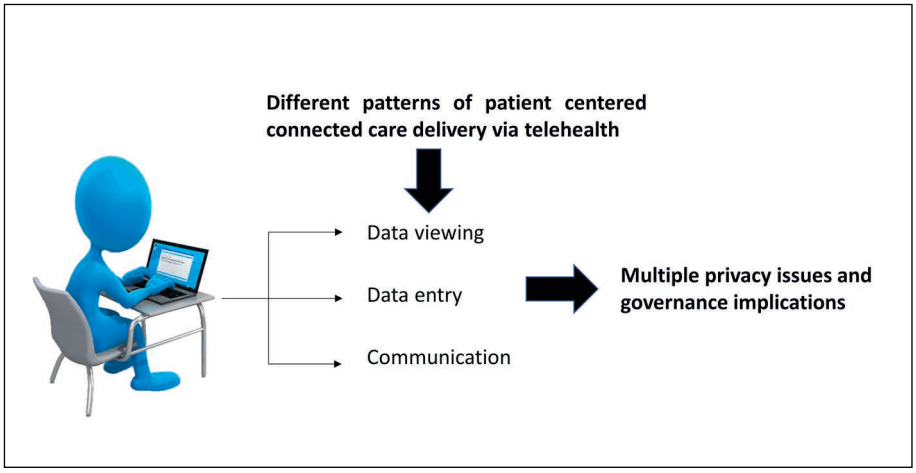

Fig. 1 Business model for patient-centred connected health via telehealth including privacy considerations.

ferent use cases is far less described [38, 39]. Privacy is one area where governance needs to be better articulated. A first step to developing privacy governance is to formalize the various ways in which HI is provided during patient-centred connected healthcare delivery. To that end, Rutenberg and Oberle [40] have proposed a supportive care model (SCM) with four different levels of activity: (a) *connecting* with patients, where practitioners establish a rapport with patients; (b) *empowerment* of patients ,where practitioners provide timely information and help patients engage in the clinical workflow; (c) *"doing for"*, where practitioners conduct a skilled assessment of patients' situation and become advocates for patients, and (d) *"finding meaning"*, where practitioners enable patients to understand the significance of the care process and integrate the care plan in their own lives. Others have suggested similar categories of HI exchange and interaction that ranges from information gathering, discussion and empowerment, and engagement [41, 42].

Drawing upon the above literature, we define three main patient-centred connected health patterns:

1. Pattern 1 is one-way HI exchange such as a patient viewing her/his HI through a telehealth application;
2. Pattern 2 is a more extensive 2-way HI exchange where communication or messaging occurs between patients and providers over time;
3. Pattern 3 expands upon pattern 2 and includes 2-way patient HI exchange and communication but also integrates multiple connection points such as EHRs, social media platforms, smartphone applications and Fitbits or other tracking applications.

4.2 Privacy Issues with Connected Health Patterns

The three different connected health patterns present different degrees of privacy issues. At a broad level, Kvedar et al. [43] contend that for telehealth to be effective, it needs to remove the barriers of patient access to HI by putting patients in the centre of the practice and by using connected health tools including mobile devices to connect and share information with patients in real time. Traditional telehealth tools that connect patients and providers in a virtual face to face environment where patients can connect using a tablet or a cell phone would be an illustration of connected health in the context of telecare [43]. However, as telehealth usage moves from connected health pattern 1 to 2 to 3, it increases the degree of HI exchange between patients and care teams (e.g., physicians, nurses, other members of the caregiving team) which also raises the risks of data breach during transmission. The greater the degree of HI exchange, the greater the potential for unauthorized persons gaining access [44]. Privacy issues become more significant when we move from traditional telehealth systems to consumer health and social media platforms (e.g., pattern 3).

Overall, the use and subsequent governance of connected health delivery are very different across these three patterns. Blanket solutions to govern privacy and access will not work as we run the risk of over or under governing connected health delivery depending on the degree of access that is needed. Rather, specific tailoring of privacy solutions to support specific usage patterns are required. In the next section, we start addressing that challenge by operationalizing the three connected health patterns according to different types of telehealth and privacy implications.

5 Operationalizing the Business Model

Our main contribution in this paper is to describe how to operationalize the business model presented in the previous section. Table 1 summarizes our findings as a framework of different types of telehealth delivery, the patent-centred connected health patterns supported, potential privacy issues, and possible solutions for the issues.

As Table 1 shows, there is a wide spectrum of modalities for how telehealth can be delivered and many types of connected health that can be supported. The biggest shift we are seeing in telehealth support of connected healthcare is the move from direct or "traditional" telehealth systems to the use of smartphone applications, social media, and other online platforms. Direct telehealth systems were designed with a dedicated purpose (e.g., to support Pattern 1 – viewing of patient HI for chronic disease management). Design requirements for direct telehealth are well bounded and privacy risks can be identified and managed as part of systems design. As telehealth usage expands into indirect usage, through EHRs and unregulated modes of delivery, it creates privacy complications due to the unknown extent of the type of HI interaction that could occur and the potential for patient HI disclosure beyond what is needed for connected health delivery.

Online consumer health telehealth tools (telehealth Type 5 in Table 1) pose a much bigger privacy risk because they were not designed or evaluated specifically for the purpose of HI exchange and therefore the relevant privacy considerations, as well as training and patient awareness of privacy issues, were less likely to be considered at the time of systems design. Further, online or social media tools enable connected health Pattern 3 (viewing and communication using multiple data sources) which provides the highest degree of connectivity and thus the highest potential for privacy breaches. Connected health Pattern 3, which utilizes multiple data touch points, has stimulated an increased demand for online health information through websites, blogs, wikis, social media, instant messaging, mobile health applications, and telemedicine technologies [45]. Many privacy and confidentiality concerns have surfaced as a result of the increasing use of social media and internet and thus there is an increase in: (a) risks of privacy and confidentiality breaches for patient information shared through unregulated social media and internet platforms and (b) a deficiency in communication between health providers and patients [46]. Denecke et al., discuss the ethical implications of sharing health information through social media platforms where patients share clinical information with other patients and with healthcare providers without giving any informed consent [47]. The authors also cite the example of a crowdsourcing health platform site breaching the confidentiality

Table 1 Framework of telehealth types, patient-centred care patterns, privacy issues, and possible solutions.

	Telehealth Types	Supported Patient-Centred Connected Health Pattern	Potential Privacy Issues	Possible Solutions
1	Telehealth – Direct	1, 2, 3	Direct transmission to unwanted locations. Leakage or hacking.	Controlled access. Creation only as per need and early destruction ISO 27799.
2	Telehealth – Indirect	1	Possibility of access beyond requirements for usage.	Awareness and adherence of ISO protocols such as 62304/82304.
3	Telehealth / EHR	1, 2	Security and privacy requirements of EHR systems for use in conformity assessment.	Adherence to standards for privacy and security of EHRs that also offer asynchronous telehealth (e.g., ISO 14441).
4	Telehealth - Unregulated	1, 2, 3	Telehealth usage is at the behest of the patient making regulation a challenge and offering potential for privacy issues.	Wide publicity of this issue to raise the awareness of the risks involved. Provision of applicable privacy guidelines.
5	Consumer Health	1, 2, 3	Patients sharing data inappropriately resulting in App providers having access to more information than required.	Better patient awareness of the risks of inappropriate disclosure and licensing system for Apps. (e.g., ISO 25238, 62304, 80001, 82304).

and privacy of health information concerning vulnerable populations such as children by posting their picture as well as their clinical information [47]. Furthermore, Asiri et al. [48] and Househ [49] investigated the sharing of sensitive health information online and found that Facebook users posted sensitive health information related to sexually transmitted diseases, genetic disorders, and psychological issues.

Overall, there is a need to better understand the implications of telehealth-enabled connected health delivery to ensure that telehealth systems undergo appropriate privacy evaluation. To that end, we need to provide guidance according to the level of data that needs to be disclosed for different connected health needs. Figure 1 offers a spectrum of how data can be used for different healthcare tasks with the privacy characteristics of the different tasks. Operational direct patient care (e.g., telehealth Type 1 from Table 1) requires the most disclosure of individual patient records which exposes to the greatest risk of privacy breaches. Tasks such as service planning, policy design, or research (e.g., telehealth Type 2 from Table 1) require less than full data disclosure through pseudo-anonymized or fully anonymized data.

The biggest need moving forward is to inform all relevant parties about different telehealth types and the privacy risks attached to each of them. As connected health and telehealth use shifts from traditional telehealth systems to consumer health and social media platforms, we run the risk of losing control of the balance between HI exchange and necessary privacy considerations. On one hand, patients become empowered and engaged with Internet, iPhone smartphone applications, and social media platforms. But on the other hand, these online telehealth tools pose substantial risks because they enable connectivity without due consideration of the unintended consequences of that connectivity. Balancing privacy considerations with the online sharing and use of clinical and/or health information will be a challenging task for policy makers, health consumers, and developers of healthcare platforms. Raising the public's awareness and intensifying informational and educational campaigns on the risks and harmful impacts of sharing clinical and/or health information online are also needed.

While privacy and confidentiality laws exist for traditional telehealth systems, laws that prevent health consumers from sharing their personal clinical information on social media or other online tools (e.g., Twitter, Facebook) with other patients or healthcare practitioners are almost non-existent. Household recommends that a health consumer e-awareness assessment model

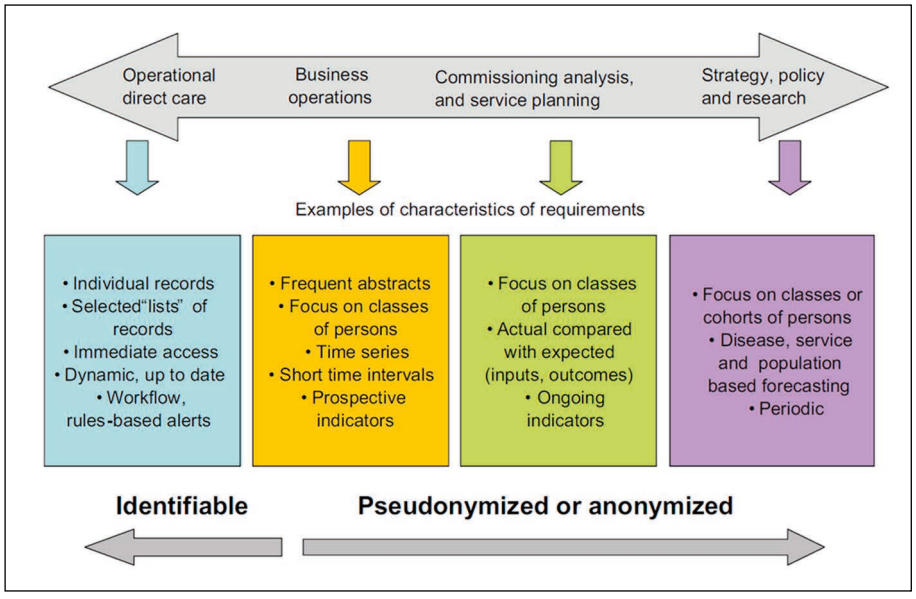

Fig. 2 "Different types of information use" taken from ISO/TS 29585:2010, Health informatics -- Deployment of a clinical data warehouse, reproduced with the permission of the International Organization for Standardization, ISO. This standard can be obtained from any ISO member and from the website of the ISO Central Secretariat at the following address: www.iso.org.

be created where patients are educated about the sharing and use of health information online [50]. Calling the attention of internet-based health platforms to share their privacy regulations openly with health consumers is needed in addition to government oversight. While protecting privacy and confidentiality in unregulated online platforms ia a major challenge for western countries, for developing countries where health care access may be limited, a bigger challenge would be to ensure that health consumers and/or patients do not fall prey to unscrupulous individuals and healthcare organizations [51]. The creation of international policies to protect and inform health consumers on how to use and share clinical and/or health information online is needed as more health consumers use online platforms in the search for advice and health information.

In summary, this paper helps address the above challenges by developing a business model of patient-centered care via telehealth and using it to identify three patterns of patient-centered connected health. The three patterns help informaticians, practitioners, government, and policy makers to understand how different types of telehealth can support different connected health patterns of HI exchange and the privacy issues and possible solutions that emerge from telehealth-enabled connectivity.

6 Conclusion

Telehealth can play a vital role in enabling patient-centred connected healthcare delivery. However, while telehealth delivery has expanded through different types of modalities, the implications for data sharing and privacy have not kept pace with the technological innovation. By integrating patient-centred connected health care, telehealth, and privacy risks, we can understand how risks vary across different patterns of patient-centred connected health and different types of telehealth delivery. Future work must focus on educating patients about the risk of sharing health information and on building a better understanding and governance of unregulated telehealth modalities and consumer health applications.

References

1. Kannampallil TG, Schauer GF, Cohen T, Patel VL. Considering complexity in healthcare systems. J Biomed Inform 2011;44(6):943-7.
2. Kuziemsky C. Decision-making in healthcare as a complex adaptive system. Healthc Manage Forum. 2016;29(1):4-7.
3. Tulchinsky TH, Varavikova EA. 2 - Expanding The Concept of Public Health. The New Public Health. San Diego: Academic Press; 2000. p. 55-112.
4. Porter ME. What Is Value in Health Care? N Engl J Med 2010;363(26):2477-81.
5. Carroll N, Kuziemsky C, Richardson I. Software engineering for connected health (journal first session). Proceedings of the 2017 International Conference on Software and System Process; Paris, France. 3087675: ACM; 2017. p. 3-4.
6. Hosseini M, Jones J, Faiola A, Vreeman DJ, Wu H, Dixon BE. Reconciling disparate information in continuity of care documents: Piloting a system to consolidate structured clinical documents. J Biomed Inform 2017;74:123-9.
7. Kuperman GJ, McGowan JJ. Potential unintended consequences of health information exchange. J Gen Intern Med 2013;28(12):1663-6.
8. Kuziemsky CE. Review of Social and Organizational Issues in Health Information Technology. Healthc Inform Res 2015;21(3):152-60.
9. Mackert M, Mabry-Flynn A, Champlin S, Donovan EE, Pounders K. Health Literacy and Health Information Technology Adoption: The Potential for a New Digital Divide. J Med Internet Res 2016;18(10):e264.
10. Bodolica V, Spraggon M, Tofan G. A structuration framework for bridging the macro-micro divide in health-care governance. Health Expect 2016;19(4):790-804.
11. Carroll N. Key Success Factors for Smart and Connected Health Software Solutions. Computer 2016;49(11):22-8.
12. Toh N, Pawlovich J, Grzybowski S. Telehealth and patient-doctor relationships in rural and remote communities. Can Fam Physician 2016;62(12):961-3.
13. Gagnon M-P, Duplantie J, Fortin J-P, Landry R. Implementing telehealth to support medical practice in rural/remote regions: what are the conditions for success? Implement Sci 2006;1(1):18.
14. Anwar M, Joshi J, Tan J. Anytime, anywhere access to secure, privacy-aware healthcare services: Issues, approaches and challenges. Health Policy Technol 2015;4(4):299-311.
15. Reinsmidt E, Schwab D, Yang L, editors. Securing a Connected Mobile System for Healthcare. 2016 IEEE 17th International Symposium on High Assurance Systems Engineering (HASE); 2016 7-9 Jan. 2016.
16. Li J, Robertson T. Physical space and information space: studies of collaboration in distributed multi-disciplinary medical team meetings. Behav Inf Technol 2011;30(4):443-54.
17. Heart T, Ben-Assuli O, Shabtai I. A review of PHR, EMR and EHR integration: A more personalized healthcare and public health policy. Health Policy Technol 2017;6(1):20-5.
18. Weber-Jahnke JH., Price M, Williams J, editors. Software engineering in health care: Is it really different? And how to gain impact. 5th International Workshop on Software Engineering in Health Care (SEHC); 2013 20-21 May 2013.
19. Berwick DM. What 'Patient-Centered' Should Mean: Confessions Of An Extremist. Health Aff (Millwood) 2009;28(4):w555-w65.
20. Institute of Medicine Committee on Quality of Health Care in A. Crossing the Quality Chasm: A New Health System for the 21st Century. Washington (DC): National Academies Press (US) Copyright 2001 by the National Academy of Sciences. All rights reserved; 2001.
21. Perrotta PL, Karcher DS. Validating Laboratory Results in Electronic Health Records: A College of American Pathologists Q-Probes Study. Arch Pathol Lab Med 2016;140(9):926-31.
22. Ding H, Fatehi F, Russell AW, Karunanithi M, Menon A, Bird D, et al. User Experience of an Innovative Mobile Health Program to Assist in Insulin Dose Adjustment: Outcomes of a Proof-of-Concept Trial. Telemed J E Health 2017 Dec 20.
23. Esch T, Mejilla R, Anselmo M, Podtschaske B, Delbanco T, Walker J. Engaging patients through open notes: an evaluation using mixed methods. BMJ Open 2016;6(1).
24. Kruse SC, Argueta AD, Lopez L, Nair A. Patient and Provider Attitudes Toward the Use of Patient Portals for the Management of Chronic Disease: A Systematic Review. J Med Internet Res 2015 e40.
25. Lai AM, Hsueh PS, Choi YK, Austin RR. Present and Future Trends in Consumer Health Informatics and Patient-Generated Health Data. Yearb Med Inform 2017;26(1):152-9.
26. Bush RA, Connelly CD, Fuller M, Perez A. Implementation of the Integrated Electronic Patient Portal in the Pediatric Population: A Systematic Review. Telemed J E Health 2015.
27. Hattink B, Droes R-M, Sikkes S, Oostra E, Lemstra, AW. Evaluation of the Digital Alzheimer Center: Testing Usability and Usefulness of an Online Portal for Patients with Dementia and Their Carers. JMIR Res Protoc 2016;5(3):e144.
28. Standardization IOf. ISO/IEC 2382-8:1998 - Information technology -- Vocabulary -- Part 8: Security. 1998.
29. Standardization IOf. ISO/IEC 27000:2009 Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary; 2009.
30. Standardization IOf. IEC 62304:2006. Medical device software—Software life cycle processes; 2006
31. Standardization IOf. IEC 80001-1:2010 - Application of risk management for IT-networks incorporating medical devices -- Part 1: Roles, responsibilities and activities; 2010.
32. Standardization IOf. IEC 82304-1:2016 - Health software -- Part 1: General requirements for product safety; 2016.
33. Standardization IOf. ISO 14971:2007 - Medical devices -- Application of risk management to medical devices; 2007.
34. Standardization IOf. ISO 27799:2016 - Health informatics -- Information security management in health using ISO/IEC 27002; 2016.

35. Standardization IOf. ISO 25237:2017 Health informatics -- Pseudonymization; 2017.
36. Centre PENftIDR. Protecting medical information in eHealth projects London School of Economics and PoliticalScience; 2010.
37. Mettler T, Eurich M, editors. What is the business model behind e-health? A pattern-based approach to sustainable profit. ECIS 2012 - Proceedings of the 20th European Conference on Information Systems; 2012.
38. Townsend A, Leese J, Adam P, McDonald M, Li LC, Kerr S, et al. eHealth, Participatory Medicine, and Ethical Care: A Focus Group Study of Patients' and Health Care Providers' Use of Health-Related Internet Information. J Med Internet Res 2015;17(6):e155.
39. Ozkaynak M, Brennan PF, Hanauer DA, Johnson S, Aarts J, Zheng K, et al. Patient-centered care requires a patient-oriented workflow model. J Am Med Inform Assoc 2013;20(e1):e14-6.
40. Rutenberg C, Oberle K. Ethics in Telehealth Nursing Practice. Home Health Care Manag Pract 2008;20(4):342-8.
41. Canada H. The Health Canada Policy Toolkit for Public Involvement in Decision Making. Corporate Consultation Secretariat, Health Policy and Communications Branch; 2000. Report No.: 0-662-29243-X.
42. Society HIaMS. HIMSS Patient Engagement Framework; 2014.
43. Kvedar J, Coye MJ, Everett W. Connected health: a review of technologies and strategies to improve patient care with telemedicine and telehealth. Health Aff (Millwood) 2014;33(2):194-9.
44. Gogia SB, Maeder A, Mars M, Hartvigsen G, Basu A, Abbott P. Unintended Consequences of Tele Health and their Possible Solutions: Contribution of the IMIA Working Group on Telehealth. Yearb Med Inform 2016(1):41-6.
45. Fiksdal AS, Kumbamu A, Jadhav AS, Cocos C, Nelsen LA, Pathak J, et al. Evaluating the process of online health information searching: a qualitative approach to exploring consumer perspectives. J Med Internet Res 2014;16(10):e224.
46. Demiris G, Oliver DP, Courtney KL. Ethical considerations for the utilization of tele-health technologies in home and hospice care by the nursing profession. Nurs Adm Q 2006;30(1):56-66.
47. Denecke K, Bamidis P, Bond C, Gabarron E, Househ M, Lau AYS, et al. Ethical Issues of Social Media Usage in Healthcare. Yearb Med Inform 2015;10(1):137-47.
48. Asiri E, Asiri H, Househ M. Exploring the concepts of privacy and the sharing of sensitive health information. Stud Health Technol Inform 2014;202:161-4.
49. Househ M. Sharing sensitive personal health information through Facebook: the unintended consequences. Studi Health Technol Inform 2011;169:616-20.
50. Househ M. Re-examining perceptions on healthcare privacy: Moving from a punitive model to an awareness model. HEALTHINF 2012 - Proceedings of the International Conference on Health Informatics; 2012.
51. Asiri E, Khalifa M, Shabir SA, Hossain MN, Iqbal U, Househ M. Sharing sensitive health information through social media in the Arab world. Int J Qual Health Care 2017;29(1):68-74.

Correspondence to:
Craig Kuziemsky
Telfer School of Management
University of Ottawa
Ottawa, ON
Canada
Tel: +1 613 562 5800 ext 4792
E-mail: Kuziemsky@telfer.uottawa.ca