Health Policy and Technology 8 (2019) 319–321

Contents lists available at ScienceDirect

Health Policy and Technology

journal homepage: www.elsevier.com/locate/hlpt

Commentary

Digital health: Cybersecurity is a value creation lever, not only a source of expenditure

Hassane Alami[a,b,*], Marie-Pierre Gagnon[c,d,f], Mohamed Ali Ag Ahmed[c,f], Jean-Paul Fortin[c,e]

[a] Institute of Public Health Research & the Department of Health Management, Evaluation and Policy, University of Montreal, Montreal, QC, Canada
[b] Institute for Excellence in Health and Social Services, Montreal, QC, Canada
[c] Research Center on Healthcare and Services in Primary Care, Institute of Health and Social Services in Primary Care, Université Laval (CERSSPL-UL), Quebec, QC, Canada
[d] Faculty of Nursing Science, Université Laval, Quebec, QC, Canada
[e] Department of Social and Preventive Medicine, Faculty of Medicine, Université Laval, Quebec, QC, Canada
[f] Research Centre of the CHU de Quebec-Université Laval, Quebec, QC, Canada

ARTICLE INFO

Article history:
Available online 18 September 2019

Keywords:
Value-based healthcare
Digital health
Health services
Cyberattacks
WannaCry
Cybersecurity
Training

ABSTRACT

Digital technologies have become an essential lever for developing patient-centered services and outcomes while ensuring financial sustainability in healthcare organizations and systems. They contribute to provide high quality, coordinated, and continuing care; to improve practices and support strategies for the management and monitoring of the population health; and to build collective responsibility for healthcare stakeholders to contain costs. However, digital technologies involve significant changes, sometimes breaking with what constitutes known commodities in healthcare organizations and systems (e.g., data governance, inter-operability, security and safety, literacy and training). The recent cyberattacks that have affected and disrupted many healthcare organizations and systems around the world are one of the illustrations. These events show that the issue of cybersecurity should not continue to be considered as a mere source of expenditure but as a source of value creation.

Introduction

Value-based healthcare (VBH) models, which aim to link the reimbursement of health care to the quality of services and patient-reported outcomes, have been proposed in health system reform strategies [1,2]. VBH would allow improving practices, monitoring and management of patients and population, while providing high quality, coordinated, and efficient health care and services [1,2].

The significant advances in digital technologies made in recent years could help to build learning and value-based health organizations and systems [1–3]. Digital technologies in health could be defined as the use of information and communication technologies (ICTs) to exchange information and data on health and its determinants – between clinicians, organizations and citizens/patients – for purposes of promotion, education, prevention, treatment and empowerment of individuals and communities, and this, in order to improve, maintain or restore health and well-being of individuals and the population while ensuring the sustainability of the health system [4].

There is a growing agreement that integrated, mature, secure and safe digital technologies are necessary to carry out health measures and quality follow-up (e.g., with respect to compliance, readmission or unnecessary visits, double examinations, quality, iatrogenic or adverse events, patient experiences) [3–8]. These measures are the bases for the healthcare cycle evaluation, not only to determine the reimbursement of services, but also to improve practices [1,9]. Quality of practice is being precisely recognized as a health system performance determinant [10,11]. The optimal exchange and circulation of data and information between the patient and various service providers, or between providers (i.e., interprofessional and interorganizational collaboration and coordination), are the cornerstone of VBH models.

However, technologies alone have no value in themselves and cannot guarantee the expected value results if a number of factors and conditions are not present in healthcare organizations and systems. Cybersecurity is one of the fundamental aspects to consider for digital technologies to become a real lever for successful transition to VBHs.

* Corresponding author at: Institute of Public Health Research of the University of Montreal, P.O. Box 6128, Branch Centre-Ville, Montreal, QC H3C 3J7, Canada.
E-mail addresses: hassane.alami@umontreal.ca (H. Alami), marie-pierre.gagnon@fsi.ulaval.ca (M.-P. Gagnon), mohamed-ali.ag-ahmed.1@ulaval.ca (M.A. Ag Ahmed), Jean-Paul.Fortin@fmed.ulaval.ca (J.-P. Fortin).

https://doi.org/10.1016/j.hlpt.2019.09.002
2211-8837/

Recent global cyberattacks have exposed the vulnerability and inadequacy of data security strategies in many healthcare organizations and systems worldwide. The *WannaCry* cyberattacks, which resulted in the shutdown of several hospitals of the *United Kingdom (UK) National Health Service*, reportedly caused the cancellation of about 600 surgeries and more than 19,000 appointments [12]. Such attacks can lead to significant direct costs (e.g., paying large ransoms to pirates, paying reparations for affected patients, cessation of the activity) or indirect costs through an alteration of the image and reputation of the organization that could also have a negative impact on its attractiveness and activity afterwards. On this point, the UK Department of Health and Social Care has estimated that these cyberattacks cost about £92 million, especially because of the loss of output and ICT cost during and after the incident [13]. In addition, according to a UK study conducted after these cyberattacks and various consumer data breach scandals, a total of 79% of respondents would ask their families and friends to boycott organizations that are unable to protect their personal data and some 60% said they would post negative comments on the topic online [14]. In the same vein, the Canadian Medical Protective Association reported that the activity of several medical clinics was disrupted as a result of the *WannaCry* cyberattacks. After each incident, restoring the ICT system would take between two to three days. During this time, clinicians were unable to access electronic records to ensure the care and monitoring of patients. These events led to the cancellation or suspension of consultations or surgeries, as it was the case in the UK [15,16]. These examples show that cybersecurity is a source of value for organizations and health systems, not just expenditure.

These events could become more frequent, more sophisticated, and will inevitably have major impacts and affect the ability of clinicians and organizations to meet the needs of their patients (e.g., unavailability of medical record data, disruption of clinical processes, interruptions of logistic flows). For example, currently, there are at least two data breaches or theft events affecting at least 500 patients each week in the USA [17]. This situation could be explained, in part, by the fact that only 50% of health organizations have sufficient human and financial resources to deal with cyberattacks [18,19]. In this regard, only 50% of organizations devote more than 5% of their spending to ICT security (vs. 12% in the banking and financial sectors) [18,19]. Otherwise, according to a global survey on safety in healthcare organizations, 96% feel vulnerable to data threats and 63% acknowledge having already experienced a data breach in the past, with about 20% reporting a breach in the last year [20]. In Canada, according to a survey after the *WannaCry* cyberattacks, 85% of managers believe that their organizations are fairly or very vulnerable to cyberattacks [21].

With the proliferation of connected objects, providers of medical devices are also facing the same problem. Some connected medical devices (e.g., pacemakers and defibrillators, drug pumps) can transmit information and clinical data that may be vulnerable to cyberattacks [22]. These so-called auxiliary connected technologies continue to receive little attention in cybersecurity plans and strategies [23]. The increasing use of mobile apps and connected objects for monitoring or care purposes requires refocusing cybersecurity strategies on consumers and clinicians, not just on structures (e.g., utilization of a public Wi-Fi network to transmit clinical data). In addition, the growing interest in the "bring your own device (BYOD)" approach further highlights the importance of privacy and cybersecurity issues [24]. Today, a patient could tell his clinician: "(…) in my house we have three iPads. I don't want another iPad to be honest. (…), just tell me what app I need" [25]. In this regard, in some countries (e.g., Canada), clinicians are already able to prescribe mobile apps for their patients (e.g., health education, monitoring) [26]. However, according to a European study, some 80% of the most used mobile health apps available on Android present risks related to the misuse and dissemination of consumer data [27].

Creating a digital culture: the imperative of training

In light of this new reality, it is important to train and raise awareness of all stakeholders involved in the health care and services chain on basic cybersecurity culture and best practices. Organizations could avoid many cyberattacks. For example, the *UK-National Audit Office* reported that the *WannaCry* cyberattacks was relatively unsophisticated and could have been prevented by basic ICT security best practices [12]. According to a recent US survey, 37% of employees in the healthcare sector have ICT practices that present serious risks for security and confidentiality, and 24% of healthcare professionals exhibit a lack of awareness of suspicious emails (e.g., phishing). For their part, about 50% of physicians do not comply with good cybersecurity and confidentiality practices, which could have serious negative impacts on their organizations [28].

The issue of computer literacy and clinical informatics skills is also a major concern. The mastery of computing has become essential to be able to provide quality services for patients [29]. In fact, there is an important need to provide training in order to help clinicians to develop a digital culture. It is not a matter of training clinician-scientists who know how to do computer development, but a basic culture that allows them to adopt and integrate technologies into their practices, while having the ability to prevent, avoid, or limit cybersecurity breaches and attacks. In addition, this would help them to better adapt and align technologies to their clinical and organizational contexts.

Traditional training programs, based mainly on "universal" techniques (e.g., compliance with policies and procedures), are not always adapted to the particularity and complexity of the health field (e.g., workload and alert fatigue as cybersecurity issues) [30–32]. There is a need to develop personalized training both for students (e.g., mandatory courses integrated into curricula at the university) and for professionals (e.g., continuing medical education, regular information sessions). In this regard, training and information strategies should adopt a hybrid clinical/informatics perspective [32,33]. Indeed, research has reported that the clinicians' perspective is often absent in cybersecurity actions and strategies [34,35]. In addition, since cybersecurity is an issue of patient and population trust and safety, training should focus on the patient's care pathway [34,36]. Training and awareness-raising of patients on cybersecurity best practices are also essential, within an empowerment and accountability perspective.

Conclusion

Digital technologies are now recognized as an important lever to improve access, continuity and quality of healthcare and services. In this vein, cybersecurity is an essential condition for developing learning and value-based health organizations and systems. However, a substantive work needs to be done to make policymakers and managers aware that it is not only a source of expenditure, but also a source of value creation for patients, clinicians, organizations and for the health system as a whole.

Acknowledgment

H. Alami is supported by the "Canadian Institutes of Health Research's (CIHR) Health System Impact Fellowship". This program is led by CIHR's Institute of Health Services and Policy Research (CIHR-IHSPR), in partnership with the Fonds de recherche du Québec –Santé (FRQS) and the Institut national d'excellence en santé et services sociaux (INESSS).

Author Statements

Funding: None

Competing interests: None declared

Ethical approval: Not required

Authors' contributions: HA produced the first draft of this manuscript, and received input from MPG, MAAA, and JPF. All authors read and approved the final manuscript.

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.hlpt.2019.09.002.

References

[1] Porter ME. A strategy for health care reform—toward a value-based system. N Engl J Med 2009;361(2):109–12.
[2] Porter ME. What is value in health care? N Engl J Med 2010;363(26):2477–81.
[3] Bashshur RL, Shannon G, Krupinski EA, Grigsby J. Sustaining and realizing the promise of telemedicine. Telemed J: E Health 2013;19(5):339–45.
[4] Agboola SO, Bates DW, Kvedar JC. Digital health and patient safety. JAMA 2016;315(16):1697–8.
[5] Wickramasinghe N, Schaffer J. Realizing value driven e-health solutions. IBM Center for The Business of Government; 2010 http://www.businessofgovernment.org/sites/default/files/Realizing%20Value%20Driven%20e-Health%20Solutions.pdf [verified on august]; 2018.
[6] Mars M, Scott RE. Global e-health policy: a work in progress. Health Aff 2010;29(2):237–43.
[7] Kvedar J, Coye MJ, Everett W. Connected health: a review of technologies and strategies to improve patient care with telemedicine and telehealth. Health Aff 2014;33(2):194–9.
[8] World Economic Forum. Value in healthcare: laying the foundation for health system transformation. 2017. http://www3.weforum.org/docs/WEF_Insight_Report_Value_Healthcare_Laying_Foundation.pdf [verified on august]; 2018.
[9] McHugh M, Joshi M. Improving evaluations of value-based purchasing programs. Health Serv Res 2010;45(5p2):1559–69.
[10] Bodenheimer T, Sinsky C. From triple to quadruple aim: care of the patient requires care of the provider. Ann Fam Med 2014;12(6):573–6.
[11] Sikka R, Morath JM, Leape L. The quadruple aim: care, health, cost and meaning in work. BMJ Qual Saf 2015;24(10):608.
[12] The Comptroller and Auditor General of the National Audit Office (UK). Investigation: WannaCry cyber-attack and the NHS. UK Department of Health; 2017 https://www.nao.org.uk/wp-content/uploads/2017/10/Investigation-WannaCry-cyber-attack-and-the-NHS.pdf [verified on august]; 2018.
[13] Department of Health and Social Care (UK). Securing cyber resilience in health and care: Progress update October 2018. 2018 <https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/747464/securing-cyber-resilience-in-health-and-care-september-2018-update.pdf> [verified on december]; 2018.
[14] Miliard M. Interoperability also posing big challenges in the UK. 2018. <http://k6.re/orJox> [verified on august]; 2018.
[15] Canadian Medical Protective Association. The ransomware threat: are you prepared? 2017. <https://www.cmpa-acpm.ca/en/advice-publications/browse-articles/2017/the-ransomware-threat-are-you-prepared> [verified on december]; 2018.
[16] Boisvert T. 'Vulnerable' Canadian hospitals may struggle to fend off cyber-attacks. 2017. <https://www.cbc.ca/news/canada/toronto/vulnerable-canadian-hospitals-may-struggle-to-fend-off-cyberattacks-1.4116976> [verified on december]; 2018.
[17] U.S. Department of Health and Human Services Office for Civil Rights. Breach portal: notice to the secretary of HHS breach of unsecured protected health information. <https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf> [verified on august]; 2018.
[18] Snell E. Incentivize cybersecurity best practices for data security. 2017. <http://k6.re/yfHKs>. [verified on august]; 2018.
[19] HIMSS. Cybersecurity survey. 2016. <https://www.himss.org/sites/himssorg/files/2016-cybersecurity-report.pdf>. [verified on august]; 2018.
[20] Vormetric Data Security (Via Cision). 2016 vormetric data threat report – healthcare edition. 2016. <http://k6.re/BYJm0> [verified on august]; 2018.
[21] Healthcarecan. Cybersafe Healthcare. Options for strengthening cybersecurity in Canada's health sector. 2018. <http://www.healthcarecan.ca/wp-content/themes/camyno/assets/document/Cyber%20Security/Options%20Brief%20Summit%20Report.pdf> [verified on December]; 2018.
[22] Abdollah T, Perrone M. Hackers could remotely control defibrillator or pacemaker, U.S. warns. 2017. <https://www.cbc.ca/news/world/cybersecurity-heart-devices-implantable-1.3930997> [verified on august]; 2018.
[23] Pratt N. 2018: Shifting healthcare's mindset to the mobile patient. 2017. <https://mobilehealthmatters.com/2017/12/04/2018-shifting-healthcares-mindset-to-the-mobile-patient/> [verified on august]; 2018.
[24] Marshall S. IT consumerization: a case study of byod in a healthcare setting. TIM Review 2014;4(3).
[25] Wade VA, Taylor A, Kidd MR, Carati C. Transitioning a home telehealth project into a sustainable, large-scale service: a qualitative study. BMC Health Serv Res 2016;16(1):183.
[26] Gheorghiu B. Myth: digital health apps are not evidence-based and do not work. Canada Health Infoway; 2017 https://www.infoway-inforoute.ca/en/what-we-do/blog/consumer-health/7544-myth-digital-health-apps-are-not-evidence-based-and-do-not-work [verified on december]; 2018.
[27] Papageorgiou A, Strigkos M, Politou E, Alepis E, Solanas A, Patsakis C. Security and privacy analysis of mobile health applications: the alarming state of practice. IEEE Access 2018;6:9390–403.
[28] Mediapro. State of Privacy and Security Awareness: Healthcare Industry Insights. 2018. <http://k6.re/CXDkN> [verified on august]; 2018.
[29] Gürdaş Topkaya S, Kaya N. Nurses' computer literacy and attitudes towards the use of computers in health care. Int J Nurs Pract 2015;21:141–9.
[30] Torres HG, Gupta S. The misunderstood link: information security training strategy. AMCIS 2018;x:1–5.
[31] Zafar H. Cybersecurity: role of behavioral training in healthcare. AMCIS 2016;x:1–5.
[32] Ghazvini A, Shukur Z. Review of information security guidelines for awareness training program in healthcare industry. ICEEI 2017;x:1–6.
[33] Kim L. Cybersecurity awareness: protecting data and patients. J Nurs Manag 2017;48(4):16–19.
[34] American Medical Association. Physician cybersecurity. 2019. <https://www.ama-assn.org/practice-management/sustainability/physician-cybersecurity> [verified on august]; 2019.
[35] Jarrett MP. Cybersecurity—a serious patient care concern. JAMA 2017;318(14):1319–20.
[36] Coventry L, Branley D. Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 2018;113:48–52.