

DEBATE

Open Access



Weighing benefits and risks in aspects of security, privacy and adoption of technology in a value-based healthcare system

Edward Meinert^{1,5*} , Abrar Alturkistani², David Brindley¹, Peter Knight³, Glenn Wells⁴ and Nick de Pennington³

Abstract

Background: Technology can potentially enable the implementation of a value-based healthcare system, where the impact of quality of care is offered at optimised cost for maximised patient benefit. Technology can deliver value by aiding in data collection to evaluate outcomes and measure costs on a patient and population level. Healthcare organisations, however, face several challenges and risks that result almost exclusively from the use of these technologies.

Discussion: Some challenges associated with healthcare technology include their unsustainability, due to lack of scale-up plans and timely evaluations. Other risks include noncompliance with data protection policies, inadequate data governance, and overestimated expectations resulting from the rapid introduction of new technologies.

Conclusion: Organisations need to consider the risks and challenges associated with the use of technology and develop comprehensive strategies that mitigate factors leading to non-adoption and to realise benefits for achieving a value-based healthcare system.

Keywords: Delivery of health care, Value-based healthcare, Technology adoption

Background

Value, in a value-based healthcare system, refers to the delivery of the best quality care in the most cost-efficient way [1]. Technology, defined as the use of information systems for the administrative management and delivery of care, is one of the three enablers of a value-based system [1], but there remains a significant gap between the current use of technologies for this purpose and the potential they could offer [2]. Health technologies are developing at a rapid pace and while it is possible to envisage ways in which they can impact cost-effectiveness (in comparison to legacy paper-driven approaches and other more manual methods), they also subject systems to new risks

and challenges. The way these issues impact a perceived notion of value requires further consideration. Questions also remain regarding the sustainability of healthcare technologies. Several sources agree that often the key challenge with health technologies is not in the design or the innovation itself, but in the lack of policies and frameworks that can enable adoption, sustainability and scalability [2–4]. Security and privacy-related challenges also remain one of the most significant concerns for creating a technology-led value-based healthcare system. An increase in data collection and sharing creates patient privacy concerns due to the potential of unintended use – digital systems can be subject to non-compliance with information governance regulations, data breaches and cyber-attacks. This article will explore some of the risks and challenges associated with the use of technology to consider what impact they could have on the measurement of value. Perspectives on the way in which these impact management and planning in value-based healthcare are derived from

* Correspondence: e.meinert14@imperial.ac.uk;

edward.meinert@paediatrics.ox.ac.uk

¹Healthcare Translation Research Group, Department of Paediatrics, University of Oxford, Oxford OX3 9DU, UK

⁵Global Digital Health Unit, Department of Primary Care and Public Health, Imperial College London, London W6 8RP, UK

Full list of author information is available at the end of the article



the authors experiences in the delivery and management of healthcare IT.

Discussion

As healthcare systems leverage technologies to create a value-based system, assessment and evaluation of such technologies are paramount for their continuation and improvement. However, evaluation of healthcare technology is not straightforward, as it requires examination of factors including engineering, strategic implementation, uptake and cost. Suppose we consider a fundamental aspect of value centred on the economic benefit derived from more efficient systems and broad adoption. While on one hand it may seem straight forward to capture this through implementation of a quantitative model, on the other hand there are many other variables which impact medium to long-term sustainability and use. These dimensions involve the use of agile implementation approaches that do not necessarily lend themselves to modelling which is static or predictable. For example, technology “scale-up” plans need to be implemented in the design process and technologies need to be tailored to users’ needs to ensure sustainability [4]. The ability to measure such plans, either in time to implement, resources required, quality and other factors is subjective and highly variable depending on organisational priorities and needs. Additionally, it is argued that abandonment of technologies can occur due to the deficiency in creating a “policy framework” alongside the innovation itself to provide effective and safe use of the technology [2] – developing such frameworks are a significant undertaking in their own right, and easily overlooked when emphasis can be centred on the design, development and implementation of a new technology. Since health information technologies evolve and are produced at a fast pace, evaluations and assessments of the technologies may not occur at the same rate of change indicating a need for more rapid assessment [5]. Assumptions change over time; a system installed today is likely to be out of date in a short period later, so in contrast to systems with longer lifecycles, this makes benefit modelling more difficult. For sustainability of technologies in creating a value-based healthcare system, it is suggested to introduce the technology in “manageable increments” while considering long-term arrangements [1]; these approaches are combinations of methods which make its perceived impact on value one which is hard to record consistently. While an information technology professional may see value in reduction of manual processes, a clinician may see a loss of value in loss of direct contact with patients and a policy maker may take different positions dependent on the use case. This variability in perception of what defines, and influences value make the concept difficult to memorialise.

A primary concern in using data to support value-based approaches results from information governance. Both the

European Union’s General Data Protection Regulation (GDPR) [6] and the USA’s Health Insurance Portability and Accountability Act (HIPAA) [7] advocate heavy penalties for organisations who fail to store and secure their user’s data appropriately. However, frequently there appears to be a misuse of patient data or non-adherence to policies. For example, in 2017, a National Health Service (NHS) hospital, Royal Free, shared patient data of more than a million patients with an independent data processing organisation, DeepMind Health [8]. The Trust shared patient data without explicit patient consent for this kind of implementation case, in contravention of data protection laws and information commissioner guidance [8]. While it was recognised that both organisations undertook the data sharing in the pursuit of improved patient care, this example demonstrated the risk to confidence from inadequately obtaining patient consent. Even if data sharing is performed for the sake of “public interest”, not achieving explicit patient consent could exasperate concerns about data collection [9]. This is especially true since many patients may not mind the sharing of their data as long as they are properly informed [9]. Assuming such issues concerning access, can be addressed, what impact does this form of data sharing have on value? While the ability to use aggregate population-level data to create insight has clear cost-benefit potential, in what ways does the principle of value translate to the ethical and reputational issues advanced by information governance concerns?

With increased storing and sharing of patient data, maintenance of cybersecurity is imperative. Cyber-attacks are a key challenge that organisations storing patient and hospital data face. Cyber-attacks can happen when entities from outside or inside the system disrupt or interfere with networks for access and are especially concerning if the whole system is impacted; an example of such attacks is through use of malware [10]. With healthcare systems aiming to create value-based systems, increased population-wide patient data from multiple resources are being collected. While patient data from different sources including technologies such as the Internet of Things (IoT) and aggregated data insight collected from sources using Artificial Intelligence (AI) methods have the potential to significantly improve healthcare outcomes [11, 12], they can also subject organisations to become targets for cyber-attacks. In addition, compared to other industries, healthcare systems are generally lagging behind in human-centred countermeasures through effective employee training and prevention of access to malicious external documents/files [13]. An example of a recent cyber-attack was the WannaCry malware incident which affected 80 NHS trusts and more than 600 different National Health Service (NHS) organisations in England [14]. Computer use, patient care and even medical equipment were all hindered by this security vulnerability [15]. Although it was possible to prevent access

to patient data from this malware, such attacks raise concerns about the security of electronically recorded data and may affect patients' and the public's trust in data sharing and highlight a need for increased vigilance, training and safeguarding against this kind of security threat.

New technology has a particular life cycle that determines its sustainability as described in Gartner's hype cycle, which suggests that it is likely that a technology can be abandoned even after being linked to significant system-wide benefits [16]. There are many examples of technologies that were developed for use in healthcare settings but were eventually abandoned for different reasons such as non-adoption, unsustainable funding and inability to create scalable technologies [3, 4]. For example, in 2013 IBM Watson, a cognitive computing system which allows clinicians to enter both structured and unstructured data and uses these inputs for problem solving and providing informed-decision making [17] was announced to be used with by a leading cancer research institute, MD Anderson [18]. Previously, the IBM system had gained popularity as a result of winning the trivia game "Jeopardy", demonstrating its ability to use computational processes to defeat human competitors [19]. The general premise of the use of the system was that such computing processes could be used to augment and extend capabilities in cancer detection and diagnosis; doctors and researchers at the institute used Watson to assist in diagnosis in the personalized treatment of cancer [17]. In less than six years' time, these plans were put on hold, revealing several faults in the project implementation [18]. While Watson does herald potential to improving health research through its implementation of sophisticated computational process, in this instance it fell short on meeting research needs and being a viable ongoing concern. The key issues included challenges in data integration, engagement, cost of delivery and project scope. [18]. Making sure these kind of projects are sustainable and designed effectively requires much more than technological innovation, but a lifecycle approach to ensure projects meet objectives. Value must be understood in view of benefits but also examining the mechanisms necessary for system enablement. These issues demonstrate the challenges of the rapid adoption of technology and potential unintended consequences.

Conclusions

To create a health system that is striving to deliver value through the use of technology, there are several challenges and risks that need to be addressed. The impact that these issues has on the definition of value is one which must be considered, otherwise the impact of technology could be overestimated, and benefits reduced due to changing circumstances. Digitising an organisation with the size and complexity of those in the healthcare

creates a considerable challenge in setting realistic goals and timelines while managing the adaptive change required of the existing individuals, systems and processes in the organisation. The risks and challenges associated with technologies do not infer the need to set technology aside and try to improve care without it. In contrast, technology immersion in healthcare is inevitable and is needed more than ever. The increased incentives worldwide to adopt healthcare technologies and the fact that other industries are gaining advanced benefits from them are all drivers for increased utilisation [20]. For these reasons, it is essential to recognise the challenges and risks associated with the use of technologies to be able an approach to utilise them in the best way possible.

Abbreviations

AI: Artificial Intelligence; GDPR: General Data Protection Regulation; HIPAA: Health Insurance Portability and Accountability Act; IoT: Internet of Things; NHS: National Health Service

Acknowledgements

The authors thank colleagues in the Department of Paediatrics, University of Oxford and the Department of Primary Care and Public Health, Imperial College London for fruitful discussions/feedback on risks and issues in the implementation of VBC.

Funding

This work was supported by the Sir David Cooksey Fellowship in Healthcare Translation, the SENS Research Foundation and the Oxford Academic Health Science Centre.

Availability of data and materials

Not applicable.

Authors' contributions

EM, AA and NdP, wrote the first draft of the manuscript. DB, PK and GW contributed to the writing of the manuscript. All authors read and approved the final manuscript.

Authors' information

EM is a Sir David Cooksey Fellow in Healthcare Translation at the University of Oxford and is an Honorary Research Fellow at Imperial College London. AA is a Research Assistant at the Department of Infectious Disease Epidemiology at Imperial College London. DB is a Senior Research Fellow and Principal Investigator of the Healthcare Translation Research Group, Department of Paediatrics at the University of Oxford. PK is the Executive Director and Chief Information Officer at the Oxford University Hospitals NHS Foundation Trust. GW is the Chief Operating Officer at the Oxford Academic Health Science Centre. NdP is the Population Health Lead and Digital Officer at the Oxford University Hospitals NHS Foundation Trust.

Ethics approval and consent to participate

Not applicable.

Consent for publication

Not applicable.

Competing interests

The authors declare that they have no competing interests.

Publisher's Note

Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Author details

¹Healthcare Translation Research Group, Department of Paediatrics, University of Oxford, Oxford OX3 9DU, UK. ²Department of Infectious Disease Epidemiology, Faculty of Medicine, School of Public Health, Imperial College London, London W6 8RP, UK. ³Oxford University Hospitals NHS Foundation Trust, John Radcliffe Hospital, Headley Way, Headington, Oxford OX3 9DU, UK. ⁴Oxford Academic Health Science Centre, Oxford OX4 4GA, UK. ⁵Global Digital Health Unit, Department of Primary Care and Public Health, Imperial College London, London W6 8RP, UK.

Received: 15 June 2018 Accepted: 26 October 2018

Published online: 13 November 2018

References

- Porter ME, Teisberg EO. Redefining Health Care: Creating Value-based Competition on Results. Harvard Business Press; 2006.
- Adler-Milstein J, Embi PJ, Middleton B, Sarkar IN, Smith J. Crossing the health IT chasm: considerations and policy recommendations to overcome current challenges and enable value-based care. *J Am Med Inform Assoc*. 2017. <https://doi.org/10.1093/jamia/ocx017>.
- van Limburg M, van Gemert-Pijnen JE, Nijland N, Ossebaard HC, Hendrix RM, Seydel ER. Why Business Modeling is Crucial in the Development of eHealth Technologies. *J Med Internet Res*. 2011. <https://doi.org/10.2196/jmir.1674>.
- Greenhalgh T, Wherton J, Papoutsis C, Lynch J, Hughes G, A'Court C, et al. Beyond Adoption: A New Framework for Theorizing and Evaluating Nonadoption, Abandonment, and Challenges to the Scale-Up, Spread, and Sustainability of Health and Care Technologies. *J Med Internet Res*. 2017. <https://doi.org/10.2196/jmir.8775>.
- Garber S, Gates SM, Keeler EB, Vaiana ME, Mulcahy AW, Lau C, et al. Redirecting Innovation in U.S. Health Care [Internet]. 2014 [cited 2018 May 17]. Available from: https://www.rand.org/pubs/research_reports/RR308.html.
- EU GDPR Information Portal [Internet]. EU GDPR Portal. [cited 2018 May 17]. Available from: <https://eugdpr.org/the-regulation/>.
- Health Information Privacy [Internet]. HHS.gov. 2015 [cited 2018 May 17]. Available from: <https://www.hhs.gov/hipaa/index.html>.
- Powles J, Hodson H. Google DeepMind and healthcare in an age of algorithms. *Health Technol*. 2017. <https://doi.org/10.1007/s12553-017-0179-1>.
- Mouton Dorey C, Baumann H, Biller-Andorno N. Patient data and patient rights: Swiss healthcare stakeholders' ethical awareness regarding large patient data sets – a qualitative study. *BMC Medical Ethics*. 2018. <https://doi.org/10.1186/s12910-018-0261-x>.
- Ulsch M, Ulsch NM. Cyber Threat! How to Manage the Growing Risk of Cyber Attacks [Internet]. Somerset, UNITED STATES: Wiley; 2014 [cited 2018 May 4]. Available from: <http://ebookcentral.proquest.com/lib/imperial/detail.action?docID=1742833>.
- Islam SMR, Kwak D, Kabir MH, Hossain M, Kwak KS. The Internet of Things for Health Care: A Comprehensive Survey. *IEEE Access*. 2015. <https://doi.org/10.1109/ACCESS.2015.2437951>.
- Price WN II. Artificial Intelligence in Health Care: Applications and Legal Implications. *Sci Tech Lawyer*. 2017;14:5.
- Kruse CS, Frederick B, Jacobson T, Monticone DK. Cybersecurity in healthcare: A systematic review of modern threats and trends. *Technology and Health Care*. 2017. <https://doi.org/10.3233/THC-161263>.
- Mayor S. Sixty seconds on . . . the WannaCry cyberattack. *BMJ*. 2018. <https://doi.org/10.1136/bmj.k1750>.
- Ehrenfeld JM. WannaCry, Cybersecurity and Health Information Technology: A Time to Act. *J Med Syst*. 2017. <https://doi.org/10.1007/s10916-017-0752-1>.
- O'Leary DE. Gartner's hype cycle and information system research issues. *Int J Account Inf Syst*. 2008. <https://doi.org/10.1016/j.accinf.2008.09.001>.
- Lee H. Paging Dr. Watson: IBM's Watson Supercomputer Now Being Used in Healthcare. *J AHIMA*. 2014;85:44–7.
- Schmidt C. M. D. Anderson Breaks With IBM Watson, Raising Questions About Artificial Intelligence in Oncology. *J Natl Cancer Inst* [Internet]. 2017 [cited 2018 Jun 7];109. Available from: <https://academic.oup.com/jnci/article/109/5/djx113/3847623>
- Keim B. Dr. Watson will see you... someday. *IEEE Spectrum*. 2015. <https://doi.org/10.1109/MSPEC.2015.7115575>.
- Ettinger WH. Using Health Information Technology to Improve Health Care: Emphasizing Speed to Value: Comment on "Supratherapeutic Dosing of Acetaminophen Among Hospitalized Patients." *Arch Intern Med*. 2012. <https://doi.org/10.1001/2013.jamainternmed.607>.

Ready to submit your research? Choose BMC and benefit from:

- fast, convenient online submission
- thorough peer review by experienced researchers in your field
- rapid publication on acceptance
- support for research data, including large and complex data types
- gold Open Access which fosters wider collaboration and increased citations
- maximum visibility for your research: over 100M website views per year

At BMC, research is always in progress.

Learn more biomedcentral.com/submissions



Copyright © 2018. This work is licensed under <http://creativecommons.org/licenses/by/4.0/> (the “License”). Notwithstanding the ProQuest Terms and Conditions, you may use this content in accordance with the terms of the License.