

Patient Safety Informatics: Meeting the Challenges of Emerging Digital Health

Ciarán McInerney^{a,b}, Jonathan Benn^{b,c}, Dawn Dowding^d, Ibrahim Habli^e, David A Jenkins^{d,f}, Carolyn McCrorie^b, Niels Peek^{d,f}, Rebecca Randell^{g,h}, Richard Williams^{d,f}, Owen A. Johnson^{a,b}

^a School of Computing, University of Leeds, Leeds, United Kingdom

^b NIHR Yorkshire and Humber Patient Safety Translational Research Centre, United Kingdom

^c School of Psychology, University of Leeds, Leeds, United Kingdom

^d School of Health Sciences, University of Manchester, Manchester, United Kingdom

^e Department of Computer Sciences, University of York, York, United Kingdom

^f NIHR Greater Manchester Patient Safety Translational Research Centre, United Kingdom

^g Faculty of Health Studies, University of Bradford, Bradford, United Kingdom

^h Wolfson Centre for Applied Health Research, Bradford, United Kingdom

Abstract

The fourth industrial revolution is based on cyber-physical systems and the connectivity of devices. It is currently unclear what the consequences are for patient safety as existing digital health technologies become ubiquitous with increasing pace and interact in unforeseen ways. In this paper, we describe the output from a workshop focused on identifying the patient safety challenges associated with emerging digital health technologies. We discuss six challenges identified in the workshop and present recommendations to address the patient safety concerns posed by them. A key implication of considering the challenges and opportunities for Patient Safety Informatics is the interdisciplinary contribution required to study digital health technologies within their embedded context. The principles underlying our recommendations are those of proactive and systems approaches that relate the social, technical and regulatory facets underpinning patient safety informatics theory and practice.

Keywords:

Patient safety; Informatics; Digital Technology

Introduction

The fourth industrial revolution is based on cyber-physical systems and the connectivity of devices. ‘Health care 4.0’ describes the adaptation of health care to this new paradigm by facilitating, for example, physiological monitoring, assisted living, and telemedicine[1]. Health care is already becoming increasingly digital and connected with moves toward fog computing and the Internet of Things[9]. Additionally, at the time of writing, the COVID-19 pandemic is accelerating the conception, design, development and use of digital health technology. Health care providers have quickly responded with rapid widespread adoption of existing technology like video consultation[40]. Other technologies like electronic health records, decision-support tools and handheld medical devices have been widely adopted with reported benefits for patient care along with concerns for patient safety[31]. Patient safety can be threatened by existing digital health technologies becoming ubiquitous with increasing pace and interact in unforeseen ways[5]. Previous work has presented an agenda for safety of digital health[32] to address the outstanding patient safety consequences through systematic study[19]. To achieve these

goals, there is a need for an improved understanding and praxis of patient safety in relation to information technology.

Partially motivated by these concerns, the Patient Safety Translational Research Centres were set up by the UK National Institute for Health Research to translate patient safety knowledge into practice[26]. Beginning in 2020, a series of workshops led by the Centres from both Yorkshire and Humber, and Greater Manchester were set up specifically to explore the interaction between emerging digital health technologies and patient safety. The aim of the workshops was to develop the field of Patient Safety Informatics and establish a platform of Patient Safety Informatics theory for future research and development. In this paper, we discuss the patient safety challenges of emerging digital health that were identified in the workshop, and present recommendations to address the concerns posed by them.

Methods

The lead author undertook a review of the academic, commercial and grey literature to collate an initial set of emerging health information technologies. This initial set was amended by 14 collaborators who represented a diverse range of expertise in the development and evaluation of digital health technologies, including clinicians, commercial developers of digital health technologies, software engineers, medical statisticians, and researchers in applied health, health services, safety science, human factors, health informatics, and clinical decision making.

The 14 collaborators convened an expert, interdisciplinary workshop to discuss the challenges associated with the aforementioned emerging technologies, and the consequences for patient-safety. Output from the workshop informed a rapid scoping review of the literature that explored the challenges and consequences that were raised, and additionally explored recommendations to mitigate and avert them. Similar to a Delphi method, the lead author then facilitated the iterative development of a set of challenges, consequences and recommendations by synthesising contributions from the expert collaborators with subsequent reviews of the literature.

Results

Table 1 summarises recommendations to address patient-safety concerns posed by the challenges of emerging digital health.

Table 1– Summary of recommendation to address safety concerns posed by the challenges of emerging digital health. P = practical applications; T = theory development

Challenge	Consequence	Recommendation
Difficult to conceptualise threats to patient safety from non-physical innovations	Inadequate consideration of threats to patient safety	Systems approach to conceptualising risk ^T ; Safety cases ^P ; Sociotechnical perspective
Difficult to build and maintain trust in health information systems that are obscure and complex	Misinformation and disinformation threaten patient safety	Sociotechnical perspective ^T ; FactSheets ^P
Unclear how to sensibly integrate and interpret new and voluminous data streams	Missed opportunity to use data; Inappropriate use of data; Biased use of data	Dynamic and causal modelling continuously surveilling performance ^P ; Middleware for interoperability ^P ; Standards for linkage and exchange of health care data ^P ; Automated anomaly detection ^P
Reactive regulatory- and standards-based approaches to safety	Avoidable harm is experienced before mitigations are put in place	Gradual approval of medical devices ^P ; Systems approach to conceptualising risk ^T
Emergent patient-safety consequences in health information systems	Hazards cannot be completely foreseen	Systems approach to conceptualising risk ^T ; Systems approach to patient safety ^T ; Safety cases ^P ; Sociotechnical perspectives ^T ; Gradual approval of medical devices ^P
Solutionism inappropriately simplifies problems and predicaments	Unfit interventions and assurances	Sociotechnical perspective ^T ; Systems approach to conceptualising risk ^T

Discussion

Challenge 1: Conceptualising digital threats

It is challenging to conceptualise threats to patient safety from digital influences. Much of the innovation in digital health technologies is not physical, instead manifesting as software, systems architecture and communication protocols. These newer innovations lack the tangibility so foundational to trust in digital and robotic systems[12]. Implementing digital technologies with their associated interconnections can increase system complexity, reduce transparency of cause-and-effect and reduce the traceability of failures in the system. Patient safety might be facilitated by the use of dynamic, multi-view safety cases for digital health technology and for health care services[10,14,35].

Challenge 2: Trust in increasingly-complex digital health technology

Introducing new technologies into health care processes can challenge trust between patients, health care professionals and health care organisations. Trust is integral to patient care and is, partly, a function of inter-personal behaviours between patients, health care professionals, and digital health-technology developers[33,36]. The growth in web-based health information has introduced alternative sources of advice for patients, which can threaten patient safety with the risk of misinformation and disinformation[38]. Also, technology is often implemented in a top-down process in which health care professionals must find ways to make the technology work for them[22]. These influences can lead to technology abandonment[24] due to concerns over patient safety[22].

Practically, developers and vendors of emerging digital health technologies should include supplier declarations of conformity to industry standards and work to co-develop products and user information with user communities to promote trust [2]. A sociotechnical approach can also facilitate transparency as a foundation for trust in technology and its implementation, in line with the Transparency for Trust initiative[41].

Challenge 3: Integrating and interpreting data sources

Inadequate integration of data sources can lead to misuse, abuse, and non-use of data. Increasing the availability of data increases opportunity to support the provision of high quality and safe health care but only if the data are coherent and interpretable to health care decision makers and practitioners. Appropriate integration is needed to avoid misuse, abuse and non-use of data, which has been implicated in patient deaths[3].

To mitigate these hazards, safe development and use of middleware – software that interfaces systems and applications – will be essential to provide an intermediary between heterogeneous health care data[8]. Other contributing solutions include distributed architectures to integrate electronic health records[29], methods that respect the latent processes that generate health care data[34], dynamic modelling of the data[18], and progress in artificial intelligence, particularly anomaly detection[20].

Challenge 4: Reactive regulations and standards

As the pace of innovation accelerates, the current reactive (rather than proactive) regulatory- and standards-based approaches to safety will be increasingly ineffective at assuring patient safety. The consequence of reactive regulations and standards is that avoidable harm might be experienced before mitigations are put in place. We recommend synchronising the

development and evaluation of digital health technologies. Existing frameworks include the Idea-Development-Exploration-Assessment-Long term study (IDEAL) framework[30] and the US Food and Drug Administration's Software Pre-Cert Pilot Program[37]. Such frameworks also address other concerns about the increased administrative burden of more-stringent regulations, which might delay products that are imperfect but practically useful.

We also recommend that regulators and developers of standards adopt a systems approach to conceptualising risk to appropriately reflect the complex adaptive nature of health care[15]. Practically, this would be reflected in the guidance and requirements relating to risk assessments, which might help to increase sensitivity to safety during development.

Challenge 5: Emergent patient safety consequences

Focusing on technologies in isolation does not consider the patient safety consequences that emerge when technologies interact. Health care systems are complex with a diversity of organisational forms, interdependence, and feedback effects[4]. Interactions between digital health technologies can make threats to patient safety more visible, change the nature of risk, and introduce new failure modes/incident types[22]. Sufficient theoretical and practical guidance is needed to navigate the novelty of emergent consequences and to understand how, through interaction, technologies and users anticipate outcomes and act to influence them[39].

Health care systems are holarchical – nested systems of systems – as exemplified by the Heimdall framework of learning health systems[23] and Carayon et al.'s[6] model of workplace safety. Systemic and holarchical conceptualisations of health care processes and patient-safety consequences can help to reveal factors underlying systems' unpredictability. For example, the framework of Non-adoption, Abandonment, and Challenges to the Scale-Up, Spread, and Sustainability (NASSS) can help to identify uncertainties and interdependencies of technology-supported change in health care[13].

As noted by Weicks[39], resilience is an emerging ability of a system to respond to unexpected demands such that normal operations can continue. Thus, our theoretical recommendations are to use systems-based definitions of risk and of resilience[15,16] to complement a systems approach to patient safety. Practically, we recommend the aforementioned safety cases and gradual approval of medical devices as appropriate approaches to handle the limited capacity to predict the behaviour of complex systems.

Challenge 6: Solutionism

Techno-optimism and technology push can drive ineffective and adverse digital health interventions. Solutionism is an ideology that inappropriately recasts "complex social situations...as neatly defined problems with definite, computable solutions...if only the right [technologies] are in place"[25]. Examples include diet apps that inappropriately simplify body composition as merely a function of calorie consumption[21], and downplaying the unimproved quality of life of patients treated for neurological disorders just because treatment improves easily-measured variables of motor control[11]. Such techno-optimism might arise from differences of perceived risk or perceived capacity for control[17].

In addition to earlier recommendations of adopting sociotechnical perspective and a systems approach to conceptualising risk, solutionism can be addressed by adopting a systemic approach to patient safety. Ravitz et al. describe such an approach with a case study on medication infusion pumps[28], and the

Systems Engineering Initiative for Patient Safety model provides a framework for understanding the structures, processes and outcomes in health care, more generally[7]. These approaches can help to sensitise developers and users of digital health to the relationships within health care systems that might facilitate unintended consequences.

Limitations

Although the workshop convened collaborators with international experience, the recommendations herein could be improved by contemporary international input.

Conclusions

The intention of this paper was to contribute to the process of developing the theoretical and practical foundations of Patient Safety Informatics, answering calls for practical progress in safety science[27]. The intersection between the established and broad disciplines of digital technology, safety science and clinical practice give rise to applied research and practice in patient safety informatics.

We presented 6 challenges posed by emerging digital health, described the consequences for patient safety, and recommended theoretical and practical mitigations. A key implication of considering the challenges and opportunities for Patient Safety Informatics is the interdisciplinary contribution required to study digital health technologies within their embedded context. While some recommendations are specific to challenges, the underlying principles are that of prospective action and a systems perspective that relates the social, technical and regulatory facets. These ideas will be further explored in subsequent workshops in our series that will address the consequences of contemporary safety theory for digital innovation, sociotechnical evaluation of digital health, and digital health interventions designed to improve patient safety.

Acknowledgements

This research is partly funded by the National Institute for Health Research (NIHR) Yorkshire and Humber Patient Safety Translational Research Centre (NIHR Yorkshire and Humber PSTRC) and NIHR Greater Manchester PSTRC. The views expressed in this paper are those of the authors and not necessarily those of the NHS, the NIHR, or the Department of Health and Social Care.

Authors have no conflicts of interest to declare. We would like to acknowledge the contribution of other workshop attendees to informing the content of this paper: Dr Sarah Darley, University of Manchester; Ms Yan Jia, University of York; Dr Aseem Mishra, University of Manchester; Mr Richard Dodd, University of Manchester.

References

- [1] G. Aceto, V. Persico, and A. Pescapé, Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing, *J. Ind. Inf. Integr.* **18** (2020) 100129. doi:10.1016/j.jii.2020.100129.
- [2] M. Arnold, D. Piorkowski, D. Reimer, J. Richards, J. Tsay, K.R. Varshney, R.K.E. Bellamy, M. Hind, S. Houde, S. Mehta, A. Mojsilovic, R. Nair, K.N. Ramamurthy, and A. Olteanu, FactSheets: Increasing trust in AI services through supplier's declarations of conformity, *IBM J. Res. Dev.* **63** (2019).

- doi:10.1147/JRD.2019.2942288.
- [3] K. Baker, E. Dunwoodie, R.G. Jones, A. Newsham, O.A. Johnson, C.P. Price, J. Wolstenholme, J. Leal, P. McGinley, C. Twelves, and G. Hall, Process mining routinely collected electronic health records to define real-life clinical pathways during chemotherapy, *Int. J. Med. Inform.* **103** (2017) 32–41. doi:10.1016/j.ijmedinf.2017.03.011.
- [4] J.W. Begun, B. Zimmerman, and K. Dooley, Health Care Organizations as Complex Adaptive Systems, in: S.M. Mick, and M. Wyttenbach (Eds.), *Adv. Heal. Care Organ. Theory*, 1st ed., Jossey-Bass, San Francisco, CA, 2003: pp. 253–288.
- [5] H. Benbya, N. Nan, H. Tanriverdi, and Y. Yoo, Complexity and Information Systems Research in the Emerging Digital World, *Manag. Inf. Syst. Q.* **44** (2020) 1.
- [6] P. Carayon, P. Hancock, N.G. Leveson, I. Noy, L. Sznclwar, and G. van Hootegeem, Advancing a sociotechnical systems approach to workplace safety—developing the conceptual framework, *Ergonomics*. **58** (2015) 548–564. doi:10.1080/00140139.2015.1015623.
- [7] P. Carayon, A. Wooldridge, P. Hoonakker, A.S. Hundt, and M.M. Kelly, SEIPS 3.0: Human-centered design of the patient journey for patient safety, *Appl. Ergon.* **84** (2020) 103033. doi:10.1016/j.apergo.2019.103033.
- [8] M. Díaz, C. Martín, and B. Rubio, State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing, *J. Netw. Comput. Appl.* **67** (2016) 99–117. doi:10.1016/j.jnca.2016.01.010.
- [9] B. Farahani, F. Firouzi, V. Chang, M. Badaroglu, N. Constant, and K. Mankodiya, Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare, *Futur. Gener. Comput. Syst.* **78** (2018) 659–676. doi:10.1016/j.future.2017.04.036.
- [10] M. Flood, and I. Habli, Multi-view safety cases, *IET Conf. Publ.* **2011** (2011) 1–6. doi:10.1049/cp.2011.0260.
- [11] J. Gardner, and N. Warren, Learning from deep brain stimulation: the fallacy of techno-solutionism and the need for ‘regimes of care,’ *Med. Heal. Care Philos.* **22** (2019) 363–374. doi:10.1007/s11019-018-9858-6.
- [12] E. Glikson, and A.W. Woolley, Human Trust in Artificial Intelligence: Review of Empirical Research, *Acad. Manag. Ann.* (2020). doi:10.5465/annals.2018.0057.
- [13] T. Greenhalgh, J. Wherton, C. Papoutsis, J. Lynch, G. Hughes, C. A’Court, S. Hinder, N. Fahy, R. Procter, and S. Shaw, 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.* **19** (2017). doi:10.2196/jmir.8775.
- [14] I. Habli, S. White, M.A. Sujun, S. Harrison, and M. Ugarte, What is the safety case for health IT? A study of assurance practices in England, *Saf. Sci.* **110** (2018) 324–335. doi:10.1016/j.ssci.2018.09.001.
- [15] Y.Y. Haimes, On the Complex Definition of Risk: A Systems-Based Approach, *Risk Anal.* **29** (2009). doi:10.1111/j.1539-6924.2009.01310.x.
- [16] Y.Y. Haimes, On the Definition of Resilience in Systems, *Risk Anal.* **29** (2009) 498–501. doi:10.1111/j.1539-6924.2009.01216.x.
- [17] P. Harris, and W. Middleton, The illusion of control and optimism about health: On being less at risk but no more in control than others, *Br. J. Soc. Psychol.* **33** (1994) 369–386.
- [18] D.A. Jenkins, M. Sperrin, G.P. Martin, and N. Peek, Dynamic models to predict health outcomes: current status and methodological challenges, *Diagnostic Progn. Res.* **2** (2018) 1–9. doi:10.1186/s41512-018-0045-2.
- [19] M.O. Kim, E. Coiera, and F. Magrabi, Problems with health information technology and their effects on care delivery and patient outcomes: a systematic review, *J. Am. Med. Informatics Assoc.* **24** (2017) 246–260. doi:10.1093/jamia/ocw154.
- [20] C. Macrae, Governing the safety of artificial intelligence in healthcare, *BMJ Qual Saf.* **28** (2019) 495–498. doi:10.1136/bmjqs-2019-009484.
- [21] A. Maturo, Fatism, self-monitoring and the pursuit of healthiness in the time of technological solutionism, *Ital. Sociol. Rev.* **4** (2014) 157–171. doi:10.13136/isr.v4i2.80.
- [22] C. McCrorie, J. Benn, O.A. Johnson, and A. Scantlebury, Staff expectations for the implementation of an electronic patient record system: A qualitative study Corresponding author, *BMC Med. Inform. Decis. Mak.* **19** (2019) 1–14. doi:10.1186/s12911-019-0952-3.
- [23] S. Mclachlan, H.W.W. Potts, D. Kudakwashe, D. Buchanan, S. Lean, O.A. Johnson, B. Daley, W. Marsh, and N. Fenton, The Heimdall framework for supporting characterisation of learning health systems, *J Innov. Heal. Inf.* **25** (2018). doi:http://dx.doi.org/10.14236/jhi.v25i2.996.
- [24] C. Morland, and I.J. Pettersen, Translating technological change—new technology and practices in a hospital, *Int. J. Product. Perform.* **67** (2018) 1000–1015.
- [25] E. Morozov, To Save Everything, Click Here: The Folly of Technological Solutionism, PublicAffairs, New York, 2013.
- [26] National Institute for Health Research, £17 million invested in NIHR Patient Safety Translational Research Centres, (2017). <https://www.nihr.ac.uk/news/17-million-invested-in-nihr-patient-safety-translational-research-centres/12278> (accessed March 26, 2021).
- [27] A. Rae, D. Provan, H. Aboelssaad, and R. Alexander, A manifesto for Reality-based Safety Science, *Saf. Sci.* **126** (2020). doi:10.1016/j.ssci.2020.104654.
- [28] A.D. Ravitz, A. Sapirstein, J.C. Pham, and P.A. Doyle, Systems approach and systems engineering applied to health care: Improving patient safety and health care delivery, *Johns Hopkins APL Tech. Dig. (Applied Phys. Lab.* **31** (2013) 354–365.
- [29] A. Roehrs, C. Andr, R. Righi, S. Jos, and M.H. Wichman, Toward a Model for Personal Health Record Interoperability, *IEEE J. Biomed. Heal. Informatics.* **23** (2019) 867–873.
- [30] A. Sedrakyan, B. Campbell, J.G. Merino, R. Kuntz, A. Hirst, and P. McCulloch, IDEAL-D: a rational framework for evaluating and achieve this goal, *BMJ.* **353** (2016) 1–7. doi:10.1136/bmj.i2372.
- [31] D.F. Sittig, A. Wright, E. Coiera, F. Magrabi, R. Ratwani, D.W. Bates, and H. Singh, Current challenges in health information technology—related patient safety, *Health Informatics J.* **26** (2020) 181–189. doi:10.1177/1460458218814893.
- [32] D.F. Sittig, A. Wright, E. Coiera, F. Magrabi, R. Ratwani, D.W. Bates, and H. Singh, Current challenges in health information technology—related

- patient safety, *Health Informatics J.* (2018) 1–9. doi:10.1177/1460458218814893.
- [33] J. Song, and F.M. Zahedi, Trust in health infomediaries, *Decis. Support Syst.* **43** (2007) 390–407. doi:10.1016/j.dss.2006.11.011.
- [34] M. Sperrin, D. Jenkins, G.P. Martin, and N. Peek, Explicit causal reasoning is needed to prevent prognostic models being victims of their own success, *J. Am. Med. Informatics Assoc.* **26** (2019) 1675–1676. doi:10.1093/jamia/ocz197.
- [35] M.A. Sujjan, P. Spurgeon, M. Cooke, A. Weale, P. Debenham, and S. Cross, The development of safety cases for healthcare services: Practical experiences, opportunities and challenges, *Reliab. Eng. Syst. Saf.* **140** (2015) 200–207. doi:10.1016/j.res.2015.03.033.
- [36] S.E. Thorne, and C.A. Robinson, Reciprocal trust in health care relationships, *J. Adv. Nurs.* **13** (1988) 782–789. doi:10.1111/j.1365-2648.1988.tb00570.x.
- [37] US Food and Drug Administration, Digital Health Innovation Action Plan, (2017). <https://www.fda.gov/media/106331/download>.
- [38] C. Wardle, and H. Derakhshan, Information Disorder: Toward an interdisciplinary framework for research and policy making, *Rep. to Counc. Eur.* (2017) 108. <https://rm.coe.int/information-disorder-toward-an-interdisciplinary-framework-for-research/168076277c>.
- [39] K.E. Weick, *Sensemaking in organizations*, SAGE, 1995.
- [40] J. Wherton, S. Shaw, C. Papoutsis, L. Seuren, and T. Greenhalgh, Guidance on the introduction and use of video consultations during COVID-19: important lessons from qualitative research, *BMJ Lead.* (2020). doi:10.1136/leader-2020-000262.
- [41] T. Wykes, and S. Schueller, Why reviewing apps is not enough: Transparency for trust (T4T) principles of responsible health app marketplaces, *J. Med. Internet Res.* **21** (2019). doi:10.2196/12390.

Address for correspondence

Ciarán McInerney, c.mcinerney@leeds.ac.uk