**Title**

Patient Safety Informatics: Meeting the challenges of emerging digital health

**Authors**

*Name*: Ciarán D. McInerney [CORRESPONDING AUTHOR]

*Degree*: PhD

*Affiliation*: NIHR Yorkshire and Humber Patient Safety Translational Research Centre; University of Leeds

*Full address*: University of Leeds, Woodhouse, Leeds, LS2 9JT

*Email*: [c.mcinerney@leeds.ac.uk](mailto:c.mcinerney@leeds.ac.uk)

*Phone*: n/a

*Name*: Jonathan Benn

*Degree*: PhD

*Affiliation*: NIHR Yorkshire and Humber Patient Safety Translational Research Centre; School of Psychology, University of Leeds

*Full address*: University of Leeds, Woodhouse, Leeds, LS2 9JT

*Name*: Dawn Dowding

*Degree*: PhD

*Affiliation*: Division of Nursing, Midwifery and Social Work, School of Health Sciences, University of Manchester

*Full address*: Jean McFarlane Building, University of Manchester, Oxford Rd, Manchester M13 9PL

*Name*: Ibrahim Habli

*Degree*: PhD

*Affiliation*: University of York

*Full address*: University of York, Deramore Lane, York, YO10 5GH

*Name*: David Jenkins

*Degree*: MSc

*Affiliation 1*: NIHR Greater Manchester Patient Safety Translational Research Centre; University of Manchester

*Affiliation 2:* Division of Informatics, Imaging and Data Science, School of Health Sciences, Faculty of Biology, Medicine and Health, University of Manchester

*Full address*: University of Manchester, Oxford Rd, Manchester M13 9PL

*Name*: Niels Peek

*Degree*: PhD

*Affiliation 1*: NIHR Greater Manchester Patient Safety Translational Research Centre; University of Manchester

*Affiliation 2:* Division of Informatics, Imaging and Data Science, School of Health Sciences, Faculty of Biology, Medicine and Health.

*Full address*: University of Manchester, Oxford Rd, Manchester M13 9PL

*Name*: Rebecca Randell

*Degree*: PhD

*Affiliation*: University of Bradford; Wolfson Centre for Applied Health Research

*Full address*: University of Bradford, Richmond Rd, Bradford, BD7 1DP

*Name*: Richard Williams

*Degree*: MA (Cantab)

*Affiliation 1*: NIHR Greater Manchester Patient Safety Translational Research Centre; University of Manchester

*Affiliation 2:* Division of Informatics, Imaging and Data Science, School of Health Sciences, Faculty of Biology. Medicine and Health, University of Manchester

*Full address*: University of Manchester, Oxford Rd, Manchester M13 9PL

*Name*: Owen Johnson

*Degree*: MSc

*Affiliation*: NIHR Yorkshire and Humber Patient Safety Translational Research Centre; University of Leeds

*Full address*: University of Leeds, Woodhouse, Leeds, LS2 9JT

# Abstract

…This article is the result of a workshop identify patient-safety challenges associated with emerging health information technologies. It was held remotely online in April 2020 bringing together a national, expert collaboration led by the …

# Introduction (750 words)

The fourth industrial revolution is based on cyber-physical systems and the connectivity of devices. ‘Healthcare 4.0’ describes the adaptation of healthcare to this new paradigm by facilitating, for example, physiological monitoring, assisted living, and telemedicine.1 Healthcare is already becoming increasingly digital and connected with moves toward fog computing and the Internet of Things.2 Additionally, at the time of writing, the COVID-19 pandemic is occurring and accelerating the conception, design, development and use of digital health technology. Healthcare providers have quickly responded with rapid wide-spread adoption of existing technology like video consultation.3 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.4 It is currently unclear what the consequences are for patient’s safety as existing health information technologies become ubiquitous with increasing pace and interact in unforeseen ways.5 There is a need for an improved understanding and praxis of patient safety in relation to information technology.

Healthcare is a safety-critical industry9 that must approach safety by concurrently avoiding, managing and embracing risk.10 This sets healthcare apart from other safety-critical industries – like aviation and offshore oil production – that predominantly focus on only one of these approaches. Another distinction is that the healthcare must consider the safety of patients in addition to the safety of staff. Although no consensual definition exists, patient safety can be considered to be the “*avoidance, prevention and amelioration of adverse outcomes or injuries stemming from the process of healthcare*”.7 It is sometimes conceptualised as a balance between risks of harm, resource use, and improving patient health.8

While the patient-safety perspective on digital health is not novel11,12 the types of patient-safety challenges and our capacity to address them are constantly in flux. Health information technologies are becoming increasingly networked in line with the fourth industrial revolution13, posing novel safety issues as technologies interact.14 This is because when health information technologies interact, they form a health information system15, or what some have referred to as information infrastructures16, the success or failure of which is partly due to emergent rather than planned change resulting from local improvisation.17 These health information systems are the inevitable structure of how digital health is evolving1,2, and will require a systemic perspective from developers, users and patient-safety researchers to mitigate emergent challenges to patient safety.18

Markus6 provides a framework to map the ways that digital health could evolve. Markus6 implies a 2x2 model describing the risks associated with both novel and existing technologies and their application (table 1). *Technochange* refers to the highest-risk of combining *novel* applications of *new* technologies. This high-risk path for digital health is driven by the relationship between vendors who want to be first to market and buyers who want to be seen to innovate. These incentives can encourage high risks for associated large rewards but sometimes at the cost of patient safety. It is important to note that health information systems are complex adaptive systems19 embedded within healthcare – itself a complex adaptive system. Whether technology is introduced via familiar or novel applications, it is likely to have unforeseeable consequences.

Whether digital health evolves along high, moderate or low risk paths, many challenges posed by increasingly-complex digital health are similar20: innovations are unlikely to be equally affordable and available for all21–24; algorithms and models are of transient relevance25; there has been a continued lack of sufficient testing, despite early calls26; societal challenges like an aging population27; and legal and political jurisdiction.28 Each of these challenges are associated with known and unknown consequences for patient safety, which need to be addressed for responsible provision of healthcare. Hence, there is a need for rigorous study of the relationship between emerging digital health and patient safety, i.e. a Patient Safety Informatics.

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. Beginning in 2020, a series of workshops led by the Centres from both Yorkshire and Humber and Greater Manchester was set up specifically to explore the interaction between emerging digital health technologies and patient safety. The aim of the workshops was to define the field of Patient Safety Informatics and establish a platform of Patient Safety Informatics theory for future research and development. The first workshop in the series was convened to identify the patient-safety challenges associated with emerging health information technologies. This paper discusses the identified challenges and recommendations to address the patient-safety concerns posed them.

# Method (<350 words)

The lead author reviewed the academic, commercial and grey literature relating to emerging health information technologies to inform a representative set. The set of technologies were characterised by personalisation, decentralisation, a systemic orientation, and a move toward a user-led/patient-centred experience (Appendix 1). The review and set of representative technologies acted as a primer to frame a national, expert, multidisciplinary workshop that was convened in April 2020. The purpose of the workshop was to identify the patient-safety challenges associated with emerging digital health technologies. The 14 workshop participants represented a diverse range of expertise in the development and evaluation of digital health technologies. Participants included clinicians, commercial developers of health information technologies, software engineers, medical statisticians, and researchers in applied health, health services, safety science, human factors, health informatics, and clinical decision making.

During the workshop, participants discussed the challenges posed by the set of health information technologies, from all four quadrants of Markus’6 technochange table (table 1). Participants were then asked to discuss the patient-safety consequences of those challenges. The challenges and consequences outputted from the workshop informed a further review of the literature and both were combined to produce a draft report. In subsequent meetings, workshop participants refined the characterisation of the challenges and consequences, and recommend approaches to address the concerns for patient safety. The lead author wrote a draft paper that was iteratively reviewed by a core writing team who volunteered from the workshop.

# Results

## Toward a definition of Patient Safety Informatics

Although there is no official definition of Patient Safety Informatics, the International Medical Informatics Association working group on ‘Health Informatics for Patient Safety’ consider their role as “[promoting] *patient safety of health information systems and their associated medical devices* [and focusing on] *how healthcare information systems can improve patient safety, as well as identifying and rectifying safety issues*”.29 Patient Safety Informatics may therefore be considered to address both the questions of: 1) whether newly developed or adopted digital health technologies are inherently safe, and 2) how technologies can be designed and applied specifically to improve patient safety. This scope is exemplified in Singh and Sittig’s Health Information Technology Safety Measurement Framework, which defines three safety domains embedded in a socio-technical work system: safe health information technology, safe use of health information technology, and using health information technology to improve safety.30 We, thus, propose Patient Safety Informatics to be the study of patient-safety-related information in healthcare systems.

*Informatics* is the interdisciplinary study of information and its environment31 with information flow recognised as key to system safety, as a vital resource, and as a reflection of safety culture.32 Safety informatics is a relatively new concept with a proposed definition as a scientific discipline studying safety information and its mechanisms to address the lack of safety information in safety management.33 For Wang and colleagues, safety information refers to safety-related data that shows systems’ safety state and its changes.34,35 There have been calls to bridge the gap between research and practice in the safety of systems36 but, despite theoretical and practical progress in safety informatics, it has yet to be applied substantially to healthcare and patient safety, in particular.

Bakken, Cimino and Hripcask37 explored how informatics can promote patient safety and provided recommendations like integrating informatics into healthcare curricula and the evaluation of digital health from health-economic, clinical and administrative perspectives. While welcomed, these recommendations, and the challenges they purport to address, concern health information technologies in isolation and their function in promoting patient safety, only. As described earlier, emerging digital health must also consider the safety of health information systems and their safe use.30 A thorough exploration and instantiation of Patient Safety Informatics is thus still lacking.

It is for these reasons that the aim of our workshop series was to develop the theoretical and practical foundations of Patient Safety Informatics by exploring the theory and praxis of applying safety informatics to patient safety. Our first workshop focused on the challenges and patient-safety consequences of, and recommendations to address, emerging digital health.

## Challenges posed by emerging digital health

During the workshop, we highlighted six challenges that emerging digital health pose, each with consequences for patient safety. Table 2 summarises the challenges and our theoretical and practical recommendations to address the safety concerns. Each is briefly presented below..

### Challenge 1: Difficulty conceptualising threats to patient safety

Much of the innovation in digital health technologies is not physical, instead manifesting as software, systems architecture and communication protocols, which lack the tangibility so foundational to trust in digital and robotic systems.38 It is challenging to conceptualise threats to patient safety from these non-physical influences because it requires more-abstract consideration of interactions and effects. This can lead to inadequate consideration of threats to patient safety. The challenges posed by the intangible nature of many of the factors that might interact to contribute to a failure in health care delivery are not specific to the digital component. Considerable work has been undertaken to develop “systems” approaches to understand adverse events, for example. Introducing digital technologies with the associated interconnections can increase system complexity, reducing transparency in cause and effect and the potential traceability of failures in the system. Structured safety cases might be a useful tool to help map the relationship between abstract influences and consequences. Safety cases are structured arguments supported by evidence that are used to justify why a system or a service is acceptably safe within a particular context.39 In safety-critical industries, particularly in the UK, these cases are an established means by which confidence in the safety of the system is communicated to, and scrutinised by, the diverse stakeholders, including users, regulators and policy makers. In the UK National Health Service, compliance with the clinical safety standards DCB0129 and DCB0160 requires a safety case for HITs. The process involves an exposition of risk to encourage proactive safety management.9 The preparation of safety cases guides reflexivity that can be insightful when combined with a systems approach to conceptualising risk and safety.40,41 Thus, patient safety might be facilitated by the use of dynamic42, multi-view43 safety cases for HIT44,45 and for healthcare services.46

### Challenge 2: Unclear how to integrate and interpret data streams

More data of a greater variety can be collected with greater ease and speed, but it is not clear how this data can be sensibly integrated and interpreted.47 There is a risk that opportunities will be missed to use data to improve safety, and there are risks of inappropriate or biased use of data that threatens patients’ safety.

To mitigate these hazards, safe development and use of middleware will be essential to provide an intermediary “*to abstract* [the] *heterogeneity* [of health information technologies] *… to achieve a seamless integration*”.48 Proposed solutions include standards for exchanging electronic health records (see 49,50 for application in epilepsy data), distributed architectures to integrate electronic health records51–53, and 3rd-party infrastructure for linkage and querying of electronic health records, e.g. the CSIRO Health Data Integration tool.54

Other contributing solutions include dynamic modelling of the data25, which can provide a solution to the transient relevance of predictive models. Similarly, progress continues to be made developing models that respect the latent, data-generating processes underlying the phenomena of interest55, which might clarify ‘Big healthcare data’.56 Finally, progress in artificial intelligence (particularly anomaly detection) might help to mitigate problems arising from data errors.57,58 For example, to minimise inappropriate decisions due to poor data quality, Sako et al59 provides a conceptual framework for automated assessment of data quality and information integrity. These methods are examples of how developments in digital health can be used to improve patient safety as well as help with its safe use.

### Challenge 3: 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 patients’ safety (Xplaceholder – OJ and CMc paperX). The consequence is that avoidable harm might be experienced before mitigations are put in place.

We recommend synchronisation of the development and evaluation of health information technologies, similar to the IDEAL framework.60 The IDEAL framework champions gradual approval of medical devices rather than the one-shot approval of CE marking61, which would allow “*graded, responsible, but earlier patient access*”.60,62 Such frameworks simultaneously address concerns that the increased administrative burden of more-stringent regulations might delay products that are imperfect but practically useful.63

We also recommend that regulators and developers of standards adopt a systems approach to conceptualising risk40 to appropriately reflect the complex adaptive nature of healthcare.64 It is hoped that these recommendations might help to manage increased sensitivity to safety during development.

### Challenge 4: Trust in opaque and complex systems

Trust has long been a part of patient care65,66 but it is threatened by the way that digitisation and complexification of digital health can hinder the intimacy of care. Trust in healthcare is partly a function of inter-personal behaviours67 with the gatekeeping and competing incentives of actors within a health information system potentially jeopardising this trust.68,69 Without trust in expert and reliable sources, patients’ safety is under threat from misinformation and disinformation from sources more intimate and familiar.70

A further challenge to trust is when an illusion of safety is partly incentivised by short-term returns. In addition to the illusion of patient safety arising from ignorance or lack of engagement71,72, ‘safety/security theatre’ describes deliberate safety-related activities intended to provide feelings of improved safety regardless of whether they actually influence safety.73 With public wariness of technology like artificial intelligence74, developers of digital health are incentivised to promote their products persuasively with, for example, focus on short rather than long-term benefits.38 Patients’ safety is threatened directly by misdirection of attention and indirectly from allocation of limited resources to support the distraction.

We suggest that a socio-technical perspective will help all stakeholders in healthcare to acknowledge the systemic nature of digital health systems. Such a perspective can support an awareness and transparency as a foundation of trust75, in line with the Transparency for Trust initiative.76 Socio-technical models like the Systems Engineering Initiative for Patient Safety77,78 relate the components of healthcare systems, which also map to the determinants of trusting relationships with technology (cf. figure 2 in 74).

Practically, developers and vendors of emerging health information technologies could consider supplier declarations of conformity to industry and community co-developed ‘FactSheets’.79 Such an approach also contributes to proactive, community-led regulation of digital health. A socio-technical perspective has the potential to address all three domains of HIT patient safety as proposed by Singh and Sittig30 - safe HIT, safe use of HIT, and using HIT to improve safety.

### Challenge 5: Emergent patient-safety consequences

Although health information technologies are being developed to leverage health information systems, e.g. the Internet of Things13, safety considerations are often focused on the technologies in isolation. This reductionist approach leads to a myopic view of the technologies’ effects that does not consider the emergent, patient-safety consequences. Healthcare systems are complex with a diversity of organizational forms, interdependence, and feedback effects.80 They are also holarchical – a nested system of systems – as exemplified by the Heimdall framework of learning health systems81 and Carayon et al’s82 model of workplace safety.

We recommend a systemic and holarchical conceptualisation of healthcare processes and patient-safety consequences to complement the complex, holarchical structure of healthcare. To this end, Haimes40 describes a complexity definition of risk, which would be essential to a systems-based discussion of patient safety. Of particular note, is a systems-based conceptualisation of resilience as a variable state of a system whose variability is the key performative and protective feature.83

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.84 Such complexity approaches will also be useful in addressing the question of how emerging challenges will interact with the existing challenges alluded to in Section 1.

### Challenge 6: Solutionism

Related to the challenge of reductionism, is solutionism, which 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”*.85 Examples include diet apps that inappropriately simplify body composition as merely a function of calorie consumption86, and the legal and ethical consequences of treatments like deep brain stimulation.87 The consequences for patient safety are that digital health interventions might be unfit for the true hazards that they present because of distraction by techno-optimism or technology push. Techno-optimism might arise from differences of perceived risk or perceived capacity for control88, which relate to existing problems of inequality in technical education and access to digital health, respectively.89

In addition to earlier recommendations of adopting socio-technical perspective and a systems approach to conceptualising risk, solutionism can be addressed by adopting a systemic approach to patient safety. Ravitz et al.41 describe such an approach with a case study on medication infusion pumps, while the Systems Engineering Initiative for Patient Safety model provides a framework for understanding the structures, processes and outcomes in healthcare, more generally.77,78 These approaches can help to sensitise developers and users of digital health to the relationships within healthcare systems that might facilitate unintended consequences.

# Discussion

\*\*

# Conclusion

To the authors’ knowledge, this is the first paper in the field of Patient Safety Informatics that has provided a definition and explored its rationale. The intention of this article was to begin the process of developing the theoretical and practical foundations of Patient Safety Informatics, answering calls for practical progress in safety science90 and a unifying theory91. We presented six challenges posed by emerging digital health, described the consequences for patient safety, and recommended theoretical and practical mitigations. These challenges, consequences and recommendations were gathered at a workshop of health informatics researchers focused on exploring the theoretical and practical foundations of Patient Safety Informatics. Subsequent workshops in our series will address the consequences of contemporary safety theory for digital innovation, socio-technical evaluation of digital health, and digital health interventions designed to improve patient safety92.

# References

1. Aceto G, Persico V, Pescapé A. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing. *J Ind Inf Integr*. 2020;18:100129. doi:10.1016/j.jii.2020.100129

2. Farahani B, Firouzi F, Chang V, Badaroglu M, Constant N, Mankodiya K. Towards fog-driven IoT eHealth: Promises and challenges of IoT in medicine and healthcare. *Futur Gener Comput Syst*. 2018;78:659-676. doi:10.1016/j.future.2017.04.036

3. Wherton J, Shaw S, Papoutsi C, Seuren L, Greenhalgh T. 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

4. Sittig DF, Wright A, Coiera E, et al. Current challenges in health information technology–related patient safety. *Health Informatics J*. 2018;(2):1-9. doi:10.1177/1460458218814893

5. Benbya H, Nan N, Tanriverdi H, Yoo Y. Complexity and Information Systems Research in the Emerging Digital World. *Manag Inf Syst Q*. 2020;44(1):1.

6. Markus ML. Technochange management: Using IT to drive organizational change. *J Inf Technol*. 2004;19(1):4-20. doi:10.1057/palgrave.jit.2000002

7. Vincent C. *Patient Safety*. 2nd ed. Oxford: Wiley-Blackwell; 2010.

8. Cook R, Rasmussen J. “Going solid”: A model of system dynamics and consequences for patient safety. *Qual Saf Heal Care*. 2005;14(2):130-134. doi:10.1136/qshc.2003.009530

9. Sujan MA, Habli I, Kelly TP, Pozzi S, Johnson CW. Should healthcare providers do safety cases? Lessons from a cross-industry review of safety case practices. *Saf Sci*. 2016;84:181-189. doi:10.1016/j.ssci.2015.12.021

10. Vincent C, Amalberti R. Approaches to Safety: One Size Does Not Fit All. In: *Safer Healthcare: Strategies for the Real World*. Springer; 2016:27-38. doi:10.1007/978-3-319-25559-0

11. Kostkova P. Grand challenges in digital health. *Front Public Heal*. 2015;3(134):1-5. doi:10.3389/fpubh.2015.00134

12. Gómez-González E, Gomez E, Márquez-Rivas J, et al. Artificial intelligence in medicine and healthcare: a review and classification of current and near-future applications and their ethical and social Impact. *arXiv*. 2020. http://arxiv.org/abs/2001.09778.

13. Wickramasinghe N, Bodendorf F, eds. *Delivering Superior Health and Wellness Management with IoT and Analytics*. Springer; 2020. doi:10.1007/978-3-030-17347-0

14. Paxton NC, Branca DL. Managing the Risks of Emerging IoT Devices. In: Wickramasinghe N, Bodendorf F, eds. *Delivering Superior Health and Wellness Management with IoT and Analytics*. Springer; 2020:447-467. doi:10.1007/978-3-030-17347-0\_22

15. Onik MFA, Fielt E, Gable GG. Complex Adaptive Systems Theory in Information Systems Research - A Systematic Literature Review. In: Ling SC, Bahri S, Finnegan P, eds. *Pacific Asia Conference on Information Systems (PACIS)*. ; 2017:1-14. https://eprints.qut.edu.au/111589/1/pacis - 2017 - Complex Adaptive Systems Theory in Information Systems Research - A Systematic Literature Review.pdf.

16. Aanestad M, Grisot M, Hanseth O, Vassilakopoulou P. *Information Infrastructures within European Health Care: Working with the Installed Base*. Springer; 2017. doi:10.1007/978-3-319-51020-0

17. Heeks R. Health information systems: Failure, success and improvisation. *Int J Med Inform*. 2006;75(2):125-137. doi:10.1016/j.ijmedinf.2005.07.024

18. Friedman CP, Rubin JC, Sullivan KJ. Toward an Information Infrastructure for Global Health Improvement. 2017:16-23.

19. Johnson OA. General System Theory and the Use of Process Mining to Improve Care Pathways. In: Scott P, de Keizer NF, Georgiou A, eds. *Applied Interdisciplinary Theory in Health Informatics: A Knowledge Base for Practitioners*. IOS Press; 2019:11-22. doi:10.3233/SHTI1263

20. Parvizi N, Woods K. Regulation of medicines and medical devices: Contrasts and similarities. *Clin Med J R Coll Physicians London*. 2014;14(1):6-12. doi:10.7861/clinmedicine.14-1-6

21. Lupton D. *Digital Health: Critical and Cross-Disciplinary Perspectives*. (Chamberlain K, Lyons A, eds.). Routledge; 2017. https://books.google.co.uk/books?hl=en&lr=&id=09srDwAAQBAJ&oi=fnd&pg=PT8&dq=Novel+challenges+of+new+and+emerging+digital+health+technologies&ots=5dgCyGehlJ&sig=OTsQkQj\_iHtz5W12G\_z5aSUt8F4&redir\_esc=y#v=onepage&q&f=false.

22. Robinson L, Cotten SR, Ono H, et al. Digital inequalities and why they matter. *Inf Commun Soc*. 2015;18(5):569-582. doi:10.1080/1369118X.2015.1012532

23. McAuley A. Digital health interventions: Widening access or widening inequalities? *Public Health*. 2014;128(12):1118-1120. doi:10.1016/j.puhe.2014.10.008

24. Banerjee A. Digital health interventions and inequalities: The case for a new paradigm. *BMJ Evidence-Based Med*. 2019;2:2-5. doi:10.1136/bmjebm-2019-111282

25. Jenkins DA, Sperrin M, Martin GP, Peek N. Dynamic models to predict health outcomes: current status and methodological challenges. *Diagnostic Progn Res*. 2018;2(1):1-9. doi:10.1186/s41512-018-0045-2

26. Leveson NG. Software Safety: Why, What, and How. *Comput Surv*. 1986;18(2).

27. Pilotto A, Boi R, Petermans J. Technology in geriatrics. *Age Ageing*. 2018;47(6):771-774. doi:10.1093/ageing/afy026

28. Wismar M, Palm W, Figueras J, Ernst K, van Ginneken E. *Cross-Border Health Care in the European Union: Mapping and Analysing Practices and Policies*. Copenhagen: WHO Europe; 2011. https://apps.who.int/iris/bitstream/handle/10665/327961/9789289002219-eng.pdf.

29. IMIA WG7. *WG7 - IMIA Working Group on Health Informatics for Patient Safety*.; 2018.

30. Singh H, Sittig DF. Measuring and improving patient safety through health information technology: The health IT safety framework. *BMJ Qual Saf*. 2016;25(4):226-232. doi:10.1136/bmjqs-2015-004486

31. Gammack J, Hobbs V, Pigott D. *The Book of Informatics*. Cengage Learning; 2011.

32. Westrum R. The study of information flow: A personal journey. *Saf Sci*. 2014;67:58-63. doi:10.1016/j.ssci.2014.01.009

33. Wang B, Wu C. Safety informatics as a new, promising and sustainable area of safety science in the information age. *J Clean Prod*. 2020;252:119852. doi:10.1016/j.jclepro.2019.119852

34. Wang B, Wu C. The outline of safety informatics. *J Intell*. 2018;37(2):88e96.

35. Huang L, Wu C, Wang B, Ouyang Q. A New Paradigm for Accident Investigation and Analysis in the Era of Big Data. *Process Saf Prog*. 2017;37(1):42-48. doi:10.1002/prs.11898

36. Underwood P, Waterson P. Systemic accident analysis: Examining the gap between research and practice. *Accid Anal Prev*. 2013;55:154-164. doi:10.1016/j.aap.2013.02.041

37. Bakken S, Cimino JJ, Hripcsak G. Promoting patient safety and enabling evidence-based practice through informatics. *Med Care*. 2004;42(2 Suppl):49-56. doi:10.1097/01.mlr.0000109125.00113.f4

38. Glikson E, Woolley AW. Human Trust in Artificial Intelligence: Review of Empirical Research. *Acad Manag Ann*. 2020. doi:10.5465/annals.2018.0057

39. Bishop P, Bloomfield R. A Methodology for Safety Case Development. *Saf Reliab*. 2000;20(1):34-42. doi:10.1080/09617353.2000.11690698

40. Haimes YY. On the Complex Definition of Risk: A Systems-Based Approach. *Risk Anal*. 2009;29(12). doi:10.1111/j.1539-6924.2009.01310.x

41. Ravitz AD, Sapirstein A, Pham JC, Doyle PA. Systems approach and systems engineering applied to health care: Improving patient safety and health care delivery. *Johns Hopkins APL Tech Dig (Applied Phys Lab*. 2013;31(4):354-365.

42. Denney E, Pai G, Habli I. Dynamic Safety Cases for Through-Life Safety Assurance. *Proc - Int Conf Softw Eng*. 2015;2(2):587-590. doi:10.1109/ICSE.2015.199

43. Flood M, Habli I. Multi-view safety cases. *IET Conf Publ*. 2011;2011(578 CP):1-6. doi:10.1049/cp.2011.0260

44. Habli I, White S, Sujan MA, Harrison S, Ugarte M. What is the safety case for health IT? A study of assurance practices in England. *Saf Sci*. 2018;110:324-335. doi:10.1016/j.ssci.2018.09.001

45. Despotou G, White S, Kelly T, Ryan M. Introducing safety cases for health IT. *2012 4th Int Work Softw Eng Heal Care, SEHC 2012 - Proc*. 2012:44-50. doi:10.1109/SEHC.2012.6227010

46. Sujan MA, Spurgeon P, Cooke M, Weale A, Debenham P, Cross S. The development of safety cases for healthcare services: Practical experiences, opportunities and challenges. *Reliab Eng Syst Saf*. 2015;140:200-207. doi:10.1016/j.ress.2015.03.033

47. Ranjan R, Rana O, Nepal S, et al. Integrating the Internet of Things and Data Science. *IEEE Cloud Comput*. 2018;5(3):12-26. doi:Doi 10.1109/Mcc.2018.032591612

48. Díaz M, Martín C, Rubio B. State-of-the-art, challenges, and open issues in the integration of Internet of things and cloud computing. *J Netw Comput Appl*. 2016;67:99-117. doi:10.1016/j.jnca.2016.01.010

49. Saripalle R, Runyan C, Russell M. Using HL7 FHIR to achieve interoperability in patient health record. *J Biomed Inform*. 2019;94(103188). doi:10.1016/j.jbi.2019.103188

50. Houta S, Ameler T, Surges R. Use of HL7 FHIR to structure data in epilepsy self-management applications. *2019 Int Conf Wirel Mob Comput Netw Commun*. 2019:111-115.

51. Roehrs A. OmniPHR: A blockchain based interoperable architecture for personal health records. 2019. http://www.repositorio.jesuita.org.br/bitstream/handle/UNISINOS/8867/Alex Roehrs\_.pdf?sequence=1&isAllowed=y.

52. Roehrs A, André C, Righi R. OmniPHR : A distributed architecture model to integrate personal health records. *J Biomed Inform*. 2017;71:70-81. doi:10.1016/j.jbi.2017.05.012

53. Roehrs A, Andr C, Righi R, Jos S, Wichman MH. Toward a Model for Personal Health Record Interoperability. *IEEE J Biomed Heal Informatics*. 2019;23(2):867-873.

54. Hansen DP, Pang C, Maeder A. HDI: Integrating health data and tools. *Soft Comput*. 2007;11(4):361-367. doi:10.1007/s00500-006-0090-6

55. Sperrin M, Jenkins D, Martin GP, Peek N. Explicit causal reasoning is needed to prevent prognostic models being victims of their own success. *J Am Med Informatics Assoc*. 2019;26(12):1675-1676. doi:10.1093/jamia/ocz197

56. Beam AL, Kohane IS. Big Data and Machine Learning in Health Care. *JAMA*. 2018;319(13):1317-1318. doi:10.1001/jama.2017.18391

57. Macrae C. Governing the safety of artificial intelligence in healthcare. *BMJ Qual Saf*. 2019;28:495-498. doi:10.1136/bmjqs-2019-009484

58. Challen R, Denny J, Pitt M, Gompels L, Edwards T, Tsaneva-Atanasova K. Artificial intelligence, bias and clinical safety. *BMJ Qual Saf*. 2019;28(3):231-237. doi:10.1136/bmjqs-2018-008370

59. Sako Z, Adibi S, Wickramasinghe N. Addressing Data Accuracy and Information Integrity in mHealth Solutions Using Machine Learning Algorithms. In: ; 2020:345-359. doi:10.1007/978-3-030-17347-0\_16

60. Sedrakyan A, Campbell B, Merino JG, Kuntz R, Hirst A, McCulloch P. IDEAL-D: a rational framework for evaluating and achieve this goal. *BMJ*. 2016;353(i2372):1-7. doi:10.1136/bmj.i2372

61. The European Parliment and The Council of the European Union. Council Directive 93/68/EEC of 22 July 1993. *Off J Eur Union*. 1993;68.

62. Hirst A, Philippou Y, Blazeby J, et al. No Surgical Innovation Without Evaluation: Evolution and Further Development of the IDEAL Framework and Recommendations. *Ann Surg*. 2019;269(2):211-220. doi:10.1097/SLA.0000000000002794

63. Oelze I, Neeser K, Müller E. PP31 Medical Device Regulation : What Is New? *Int J Technol Assess Health Care*. 2019;35(S1):42-43. doi:10.1017/S0266462319001958

64. Plsek PE, Greenhalgh T. The challenge of complexity in health care. *BMJ*. 2001;323(7313):625-628. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC1121189/pdf/625.pdf%0Ahttp://www.ncbi.nlm.nih.gov/pubmed/11557716.

65. Thorne SE, Robinson CA. Reciprocal trust in health care relationships. *J Adv Nurs*. 1988;13(6):782-789. doi:10.1111/j.1365-2648.1988.tb00570.x

66. Song J, Zahedi FM. Trust in health infomediaries. *Decis Support Syst*. 2007;43(2):390-407. doi:10.1016/j.dss.2006.11.011

67. Calnan M, Rowe R. Researching trust relations in health care: Conceptual and methodological challenges – an introduction. *J Health Organ Manag*. 2006;20(5):349-358. doi:10.1108/14777260610701759

68. Mechanic D, Schlesinger M. The impact of managed care on patients’ trust in medical care and their physicians. *JAMA*. 1996;275(21):1693-1697. doi:10.1001/jama.1996.03530450083048

69. Alaszewski A. Risk, trust and health. *Heal Risk Soc*. 2003;5(3):235-239. doi:10.1080/13698570310001606941

70. Wardle C, Derakhshan H. 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-researc/168076277c.

71. Classen D. Medication Safety: Moving from illusion to reality. *JAMA*. 2003;289(9):1154-1156.

72. Tomassoni AJ, Simone K. Herbal medicines for children: an illusion of safety? *Curr Opin Pediatr*. 2001;13:162-169.

73. Thedell T. The Theater of Safety. *Prof Saf*. 2013;58(10):28.

74. Siau K, Wang W. Building trust in artificial intelligence, machine learning, and robotics. *Cut Bus Technol J*. 2018;31(2):47-53.

75. Kim H, Lee TH. Strategic CSR Communication: A Moderating Role of Transparency in Trust Building. *Int J Strateg Commun*. 2018;12(2):107-124. doi:10.1080/1553118X.2018.1425692

76. Wykes T, Schueller S. Why reviewing apps is not enough: Transparency for trust (T4T) principles of responsible health app marketplaces. *J Med Internet Res*. 2019;21(5). doi:10.2196/12390

77. Holden RJ, Carayon P, Gurses AP, et al. SEIPS 2.0: A human factors framework for studying and improving the work of healthcare professionals and patients. *Ergonomics*. 2014;56(11):1-30. doi:10.1080/00140139.2013.838643.SEIPS

78. Carayon P, Wooldridge A, Hoonakker P, Hundt AS, Kelly MM. SEIPS 3.0: Human-centered design of the patient journey for patient safety. *Appl Ergon*. 2020;84(December 2019):103033. doi:10.1016/j.apergo.2019.103033

79. Arnold M, Piorkowski D, Reimer D, et al. FactSheets: Increasing trust in AI services through supplier’s declarations of conformity. *IBM J Res Dev*. 2019;63(4-5). doi:10.1147/JRD.2019.2942288

80. Begun JW, Zimmerman B, Dooley K. Health Care Organizations as Complex Adaptive Systems. In: Mick SM, Wyttenbach M, eds. *Advances in Health Care Organization Theory*. 1st ed. San Francisco, CA: Jossey-Bass; 2003:253-288.

81. Mclachlan S, Potts HWW, Kudakwashe D, et al. The Heimdall framework for supporting characterisation of learning health systems. *J Innov Heal Inf*. 2018;25(2). doi:http://dx.doi.org/10.14236/jhi.v25i2.996

82. Carayon P, Hancock P, Leveson NG, Noy I, Sznelwar L, van Hootegem G. Advancing a sociotechnical systems approach to workplace safety-developing the conceptual framework. *Ergonomics*. 2015;58(4):548-564. doi:10.1080/00140139.2015.1015623

83. Haimes YY. On the Definition of Resilience in Systems. *Risk Anal*. 2009;29(4):498-501. doi:10.1111/j.1539-6924.2009.01216.x

84. Hilborn RC. Sea gulls, butterflies, and grasshoppers: A brief history of the butterfly effect in nonlinear dynamics. *Am J Phys*. 2004;72(4):425-427. doi:10.1119/1.1636492

85. Morozov E. *To Save Everything, Click Here: The Folly of Technological Solutionism*. New York: PublicAffairs; 2013.

86. Maturo A. Fatism, self-monitoring and the pursuit of healthiness in the time of technological solutionism. *Ital Sociol Rev*. 2014;4(2):157-171. doi:10.13136/isr.v4i2.80

87. Gardner J, Warren N. Learning from deep brain stimulation: the fallacy of techno-solutionism and the need for ‘regimes of care.’ *Med Heal Care Philos*. 2019;22(3):363-374. doi:10.1007/s11019-018-9858-6

88. Harris P, Middleton W. The illusion of control and optimism about health: On being less at risk but no more in control than others. *Br J Soc Psychol*. 1994;33:369-386.

89. Gann B. Transforming lives: Combating digital health inequality. *IFLA J*. 2019;45(3):187-198. doi:10.1177/0340035219845013

90. Rae A, Provan D, Aboelssaad H, Alexander R. A manifesto for Reality-based Safety Science. *Saf Sci*. 2020;126(June). doi:10.1016/j.ssci.2020.104654

91. Swuste P, Groeneweg J, van Gulijk C, Zwaard W, Lemkowitz S, Oostendorp Y. The future of safety science. *Saf Sci*. 2020;125(September 2019):104593. doi:10.1016/j.ssci.2019.104593

92. Johnson OA, Benn J, Habli I, Peek N, McCrorie C, McInerney CD. Theoretical and practical foundations of Safety Informatics: Workshop programme proposal. https://github.com/ciaranmci/TheoryDevWrkshop1. Published 2020. Accessed May 14, 2020.

\*\* Tables and figures must be submitted separately\*\*

\*\* FYI, tables have to be presented in this simplified format but the Lancet editing team will improve aesthetics \*\*

|  |  |  |
| --- | --- | --- |
|  | *New technology* | *Existing technology* |
| *Novel application* | High risk | Moderate risk |
| *Familiar application* | Moderate risk | Low risk |
| ***Table 1:* Contingency table illustrating the risk categories associated with interactions of novel and existing technology and its application. Adapted from Markus**6**.** | | |

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | **Challenges** | **Consequences for patient safety** | **Recommendations** | **Safe**  **HIT** | **Safe**  **use of**  **HIT** | **HIT to**  **improve**  **safety** |
| 1 | Difficult to conceptualise threats to patient | Inadequate consideration of threats | Systems approach to conceptualising riskT; Safety | x | x | - |
|  | safety from non-physical innovations. | to patient safety. | casesP; Socio-technical perspective |  |  |  |
| 2 | Unclear how to sensibly integrate and | Missed opportunities to use data; | Dynamic and causal modelling continuously | x | x | x |
|  | interpret new and voluminous data streams. | Inappropriate use of data; Biased use | surveilled for performanceP; Middleware for |  |  |  |
|  |  | of data. | interoperabilityP; Standards for linkage and |  |  |  |
|  |  |  | exchange of healthcare dataP; Automated anomaly |  |  |  |
|  |  |  | detection |  |  |  |
| 3 | Reactive regulatory- and standards-based | Avoidable harm is experienced before | Gradual approval of medical devicesP; Systems | x | - | - |
|  | approaches to safety. | mitigations are put in place. | approach to conceptualising riskT |  |  |  |
| 4 | Difficult to build and maintain trust in health | Misinformation and disinformation | Socio-technical perspectiveT; FactSheetsP | x | x | x |
|  | information systems that are obscure and | threaten patient safety. |  |  |  |  |
|  | complex. |  |  |  |  |  |
| 5 | Emergent patient-safety consequences in | Hazards cannot be completely | Systems approach to conceptualising riskT; | x | x | - |
|  | health information systems. | foreseen. | Systems approach to patient safetyT; Safety |  |  |  |
|  |  |  | casesP; Socio-technical perspectiveT; Gradual |  |  |  |
|  |  |  | approval of medical devicesP |  |  |  |
| 6 | Solutionism inappropriately simplifies | Unfit interventions and assurances | Socio-technical perspectiveT; Systems approach to | X | - | - |
|  | problems and predicaments. | might be suggested. | conceptualising riskT |  |  |  |
| Recommendations are tagged as theory development (T) and practical application (P) in line with the foundational aim of the workshop series. The rightmost columns are the domains of safety for Health Information Technology (HIT), as per Singh and Sittig’s Health Information Technology Safety Measurement Framework.30 | | | | | | | |
| ***Table 2:* Summary of recommendations to address safety concerns posed by the challenges of emerging digital health.** | | | | | | | |