# Patient Safety Informatics: Meeting the Challenges of Emerging Digital Health

## 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 present a definition of Patient Safety Informatics that was informed by the workshop and existing literature, discuss the 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:** sociotechnical; systems; safety cases; health information systems; internet of things; health informatics

## 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.[2] 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 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 safety as existing digital health technologies become ubiquitous with increasing pace and interact in unforeseen ways.[5] There is thus 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. 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 develop 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 digital health technologies. The 14 participants in the inaugural workshop 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.

In this Viewpoint paper, we present a definition of Patient Safety Informatics that was informed by the workshop and existing literature, to discuss the challenges identified in the workshop, and to present recommendations to address the patient-safety concerns posed by them.

## The need for Patient Safety Informatics

### Patient safety and its relationship with digital health

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”.[6] It is sometimes conceptualised as a balance between risks of harm, resource use, and improving patient health.[7] Health care is a safety-critical industry[8] that must approach safety by concurrently avoiding, managing and embracing risk.[9] This sets health care apart from other safety-critical industries – like aviation and offshore oil production – that predominantly focus on only one of these approaches.[9]

While the patient-safety perspective on digital health technology is not novel,[10] the types of patient-safety challenges and our capacity to address them are constantly in flux. Policy, standards and regulations specific to digital health technology are being drafted worldwide[11] to keep pace with evolving health care, including the US Food and Drug Administration, and the UK’s National Health Service and the National Institute for Health and Care Excellence.[12–14] Digital health information technologies are becoming increasingly networked in line with the fourth industrial revolution, posing novel safety issues as technologies interact.[15] This is because when health information technologies interact, they form a health information system,[16] or what some have referred to as information infrastructures,[17] the success or failure of which is partly due to emergent rather than planned change resulting from local improvisation.[18] These health information systems are the inevitable structure of how digital health is evolving,[1,2] and will require a systemic perspective from developers, users and patient-safety researchers to mitigate emergent challenges to patient safety.

Markus[19] provides a framework to map the ways that digital health could evolve. Markus[19] 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. It is important to note that health information systems are complex adaptive systems[20] embedded within health care – itself a complex adaptive system. Whether technology is introduced via familiar or novel applications, it is likely to have unforeseeable consequences.

|  |  |  |
| --- | --- | --- |
| **Table 1.** Contingency table illustrating the risk categories associated with interactions of novel and existing technology and its application. Adapted from Markus19. | | |
|  | New technology | Existing technology |
| Novel application | *High risk* | *Moderate risk* |
| Familiar application | *Moderate risk* | *Low risk* |

Whether digital health evolves along Markus’s high, moderate or low risk paths, many challenges posed by increasingly-complex digital health are similar[21]: innovations are unlikely to be equally affordable and available for all[22]; algorithms and models are of transient relevance[23]; there has been a continued lack of sufficient testing, despite early calls[24]; societal challenges like an aging population[25]; and legal and political jurisdiction.[26] Each of these challenges are associated with known and unknown consequences for patient safety, which need to be addressed for responsible provision of health care. Hence, there is a need for rigorous study of the relationship between emerging digital health and patient safety – that is to say, a Patient Safety Informatics.

### Toward a definition of Patient Safety Informatics

We propose Patient Safety Informatics to be the study of patient-safety-related information in health care systems. This definition is based on a synthesis of the aforementioned literature of patient safety, existing literature on safety informatics, and our clinical, professional and academic experience (Figure 1).

Informatics is the interdisciplinary study of information and its environment.[27] Crucially, information flow is recognised as a key component of system safety and is a reflection of safety culture.[28] This understanding has led to the relatively new concept of Safety Informatics, defined as the scientific discipline studying safety information and its mechanisms, to address the lack of safety information in safety management.[29] For Wang and colleagues who proposed this definition, safety information refers to safety-related data that shows systems’ safety state and its changes.[30,31] Thus, our proposed definition of Patient Safety Informatics incorporates concern for the state and dynamics of patient-safety information.

Despite theoretical and practical progress in safety informatics, it has yet to be applied substantially to health care and patient safety. Bakken, Cimino and Hripcask explored how informatics can promote patient safety and provided recommendations like integrating informatics into health care curricula and the evaluation of digital health from health-economic, clinical and administrative perspectives.[32] While welcomed, these recommendations, and the challenges they purport to address, concern digital health technologies in isolation and their function in promoting patient safety, only. To address emerging digital health, Patient Safety Informatics must also consider the safety of health information systems and their safe use.[33]

The consideration of health care information systems is central to our proposed definition of Patient Safety Informatics, in line with the International Medical Informatics Association working group on ‘Health Informatics for Patient Safety’. The working group 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”.[34] 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 sociotechnical work system: safe health information technology, safe use of health information technology, and using health information technology to improve safety.[33]

## Challenges posed by emerging digital health

During the workshop, we highlighted 6 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.

### 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, which lack the tangibility so foundational to trust in digital and robotic systems.[35] 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. 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.[36] In safety-critical industries like petrochemical processing and nuclear power, safety 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 digital health technologies. The process involves an exposition of risk to encourage proactive safety management.[8] The preparation of safety cases guides reflexivity that can be insightful when combined with a systems approach to conceptualising risk and safety.[37,38] Thus, patient safety might be facilitated by the use of dynamic, multi-view safety cases for digital health technology and for health care services.[39–41]

|  |  |  |  |
| --- | --- | --- | --- |
| **Table 2:** Summary of recommendations to address safety concerns posed by the challenges of emerging digital health. | | | |
|  | **Challenges** | **Consequences for patient safety** | **Recommendations** |
| 1 | Difficult to conceptualise threats to patient | Inadequate consideration of threats | Systems approach to conceptualising riskT; Safety |
|  | safety from non-physical innovations. | to patient safety. | casesP; Sociotechnical perspective |
|  |  |  |  |
| 2 | Unclear how to sensibly integrate and | Missed opportunities to use data; | Dynamic and causal modelling continuously |
|  | 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 health care dataP; Automated anomaly |
|  |  |  | detection |
| 3 | Reactive regulatory– and standards–based | Avoidable harm is experienced before | Gradual approval of medical devicesP; Systems |
|  | approaches to safety. | mitigations are put in place. | approach to conceptualising riskT |
|  |  |  |  |
| 4 | Difficult to build and maintain trust in health | Misinformation and disinformation | Sociotechnical perspectiveT; FactSheetsP |
|  | 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; |
|  | health information systems. | foreseen. | Systems approach to patient safetyT; Safety |
|  |  |  | casesP; Sociotechnical perspectiveT; Gradual |
|  |  |  | approval of medical devicesP |
| 6 | Solutionism inappropriately simplifies | Unfit interventions and assurances | Sociotechnical perspectiveT; Systems approach to |
|  | problems and predicaments. | might be suggested. | conceptualising riskT |
| P = practical application; T = Theory development. | | | |

### Challenge 2: Trust 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.[42,43] Unlike intermediary technologies that facilitate inter-personal interactions (eg telephone appointments and online booking systems), the use of technology like automated risk assessment algorithms and web–based treatment support can adversely alter the human interactions that are integral to quality and safety of care and of patients’ experiences. 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.[44]

An important consideration for trust is human confidence in the use of advanced forms of digital technology. Safety is sometimes assumed because of ignorance or lack of engagement with what patients perceive as inaccessibly complex technology and systems.[45] The public are becoming more informed about the adoption of technologies like artificial intelligence into health care and this is accompanied by a rise in wariness, especially if assurance as to the reliability and safety of these devices is not provided.[46] Furthermore, machine–learning tools are often complex and hence opaque to the user. Designing explainability into AI–based systems might affect accuracy and requires understanding of a range of non-technical issues, including medical, legal, ethical and societal considerations.[47]

In addition to design, the process by which a technology is implemented in health care systems affects confidence and adoption decisions. Often technology implementation is a top-down process in which health care professionals must find ways to make the technology work for them.[48] Lack of user-involvement in procurement and implementation can compromise health care professionals’ trust, along with shortcomings in perceived ease of use linked to issues with interoperability, accessibility and guidance.[49] In the worst cases, this can lead to technology abandonment[50] due to concerns over patient safety.[48]

We recommend a sociotechnical approach to the development and implementation of digital health that includes the perspectives of all stakeholders and components of the health care system at all stages of the system lifecycle. Technology is easier to embed if relationships between technical, social and organisational components are supported.[51] A sociotechnical approach facilitates transparency as a foundation for trust in technology and its implementation, in line with the Transparency for Trust initiative.[52] Sociotechnical models like the Systems Engineering Initiative for Patient Safety provide a framework for understanding clinical work-system relationships and safety outcomes,[53] and maps to the determinants of trusting relationships with technology.[46] Practically, developers and vendors of emerging digital health technologies should include supplier declarations of conformity to industry standards and distribute information co-developed with user communities to promote trust in proven digital health solutions.[54]

### Challenge 3: Integrating and interpreting data sources

*Inadequate integration of data sources can lead to misuse, abuse, and non-use of data.*

Advances in monitoring technologies means that a greater variety of data can be collected with greater ease and speed. 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.[55]

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.[56] Proposed solutions include standards for exchanging electronic health records,[57] distributed architectures to integrate electronic health records,[58] and 3rd-party infrastructure for linkage and querying of electronic health records, for example the CSIRO Health Data Integration tool.[59]

Other contributing solutions include dynamic modelling of the data,[23] which can provide a solution to the transient relevance of predictive models. Safety might also be facilitated by an improved understanding of the latent processes generating health care data. Methods that respect these latent processes are available to health informaticians.[60] Finally, progress in artificial intelligence (particularly anomaly detection) might help to mitigate unsafe decisions made from data errors.[61]

### 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 patients’ safety.*

The consequence of reactive regulations and standards is that avoidable harm might be experienced before mitigations are put in place. We recommend synchronisation of the development and evaluation of digital health technologies, similar to the Idea-Development-Exploration-Assessment-Long term study (IDEAL) framework and the US Food and Drug Administration’s Software Pre-Cert Pilot Program.{Formatting Citation} The IDEAL framework champions gradual approval of medical devices rather than the one-shot approval of CE marking,[62] which would allow “graded, responsible, but earlier patient access”.[63] Such frameworks simultaneously address concerns that the increased administrative burden of more-stringent regulations might delay products that are imperfect but practically useful.[64]

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.[37] Practically, this would be reflected in the guidance and requirements relating to risk assessments. It is hoped that these recommendations might help to manage increased sensitivity to safety during development. This is in line with the aforementioned Software Pre-Cert Pilot Program’s focus on the “digital health technology developer, not the product”.{Formatting Citation}

### 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 organizational forms, interdependence, and feedback effects.[65] 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.[48] 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.[66]

Health care systems are holarchical – nested systems-of-systems – as exemplified by the Heimdall framework of learning health systems[67] and Carayon et al.’s[68] 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.[69]

Our theoretical recommendations are to use systems–based definitions of risk and of resilience[37,70] to complement a systems approach to patient safety. As noted by Weicks,[66] resilience is an emerging ability of a system to respond to unexpected demands such that normal operations can continue. It moves away from a deterministic paradigm of safety research that assume merely-complicated and attributable sources of hazard.

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. Such complexity approaches will also be useful in addressing the question of how emerging challenges will interact with the other challenges.

### 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”.[71] Examples include diet apps that inappropriately simplify body composition as merely a function of calorie consumption,[72] and downplaying the unimproved quality of life of patients treated for neurological disorders because treatment did improve measurable variables of motor control.[73] Interventions might be unfit to address health and safety concerns if digital implementations are prioritised on ideological grounds. The driving techno-optimism might arise from differences of perceived risk or perceived capacity for control.[74]

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,[38] while the Systems Engineering Initiative for Patient Safety model provides a framework for understanding the structures, processes and outcomes in health care, more generally.[53] These approaches can help to sensitise developers and users of digital health to the relationships within health care systems that might facilitate unintended consequences.

## Conclusion

The intention of this paper was to begin the process of developing the theoretical and practical foundations of Patient Safety Informatics, answering calls for practical progress in safety science.[75] The intersection between the established and broad disciplines of digital technology, safety science and clinical practice give rise to applied research and practice in health informatics, patient safety and safety information systems.

We presented 6 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 an expert, interdisciplinary workshop focused on exploring the theoretical and practical foundations of Patient Safety Informatics. 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

JB, IH, OJ and NP conceptualised the workshop fundamental to this Viewpoint. CMI led project administration, data curation, investigation, visualisation, writing of the original draft and writing of edits. All authors contributed to the workshop and to reviewing, editing and the provision of resources for this Viewpoint.

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). 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.

We would like to acknowledge the contribution of other workshop attendees to informing the content of this paper: Dr Sarah Darley, Centre for Primary Care and Health Services Research, School of Health Sciences, University of Manchester; Ms Yan Jia, Department of Computer Science, University of York, Dr Aseem Mishra, Academic Clinical Fellow, University of Manchester; Mr Richard Dodd, University of Manchester.

We would like to acknowledge Robin Kok for his development of the JMIR citation style CSL for Mendeley, available under CC BY-NC 4.0 [76].

## Conflicts of interests

None declared.

## Abbreviations

CSIRO: Commonwealth Scientific and Industrial Research Organisation

IDEAL: Idea-Development-Exploration-Assessment-Long term study

NASSS: Non-adoption, Abandonment, and Challenges to the Scale-Up, Spread, and Sustainability

NIHR: National Institute for Health Research

# 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. Elsevier; 2020;18:100129.
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.
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;
4. Sittig DF, Wright A, Coiera E, Magrabi F, Ratwant R, Bates DW, et al. Current challenges in health information technology–related patient safety. Health Informatics J. 2018;(2):1–9.
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. Vincent C. Patient Safety. 2nd ed. Oxford: Wiley-Blackwell; 2010.
7. 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. PMID: 15805459
8. 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. Elsevier Ltd; 2016;84:181–189.
9. Vincent C, Amalberti R. Approaches to Safety: One Size Does Not Fit All. Safer Healthc Strateg Real World. Springer; 2016. p. 27–38.
10. Kostkova P. Grand challenges in digital health. Front Public Heal. 2015;3(134):1–5.
11. International Comparative Legal Guide. Digital Health Laws and Regulations 2020 [Internet]. Tanenbaum W, editor. Global Legal Group; 2020.
12. NHS. The NHS Patient Safety Strategy: Safer culture, safer systems, safer patients [Internet]. NHS England and NHS Improvment; 2019.
13. NICE. Evidence standards framework for digital health technologies: User guide [Internet]. National Institute for Health and Care Excellence; 2019.
14. US Food and Drug Administration. Digital Health Innovation Action Plan [Internet]. 2017.
15. Wickramasinghe N, Bodendorf F, editors. Delivering Superior Health and Wellness Management with IoT and Analytics [Internet]. Springer; 2020.
16. 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, editors. Pacific Asia Conf Inf Syst. 2017. p. 1–14.
17. Aanestad M, Grisot M, Hanseth O, Vassilakopoulou P. Information Infrastructures within European Health Care: Working with the Installed Base. Springer; 2017.
18. Heeks R. Health information systems: Failure, success and improvisation. Int J Med Inform. 2006;75(2):125–137.
19. Markus ML. Technochange management: Using IT to drive organizational change. J Inf Technol. 2004;19(1):4–20.
20. Johnson OA. General System Theory and the Use of Process Mining to Improve Care Pathways. In: Scott P, de Keizer NF, Georgiou A, editors. Appl Interdiscip Theory Heal Informatics A Knowl Base Pract. IOS Press; 2019. p. 11–22.
21. 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. PMID: 24532735
22. Banerjee A. Digital health interventions and inequalities: The case for a new paradigm. BMJ Evidence-Based Med. 2019;2:2–5.
23. Jenkins DA, Sperrin M, Martin GP, Peek N. Dynamic models to predict health outcomes: current status and methodological challenges. Diagnostic Progn Res. Diagnostic and Prognostic Research; 2018;2(1):1–9.
24. Leveson NG. Software Safety: Why, What, and How. Comput Surv. 1986;18(2).
25. Pilotto A, Boi R, Petermans J. Technology in geriatrics. Age Ageing. 2018;47(6):771–774.
26. 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 [Internet]. Copenhagen: WHO Europe; 2011.
27. Gammack J, Hobbs V, Pigott D. The Book of Informatics. Cengage Learning; 2011.
28. Westrum R. The study of information flow: A personal journey. Saf Sci. Elsevier Ltd; 2014;67:58–63.
29. Wang B, Wu C. Safety informatics as a new, promising and sustainable area of safety science in the information age. J Clean Prod. Elsevier Ltd; 2020;252:119852.
30. Wang B, Wu C. The outline of safety informatics. J Intell. 2018;37(2):88e96.
31. 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.
32. Bakken S, Cimino JJ, Hripcsak G. Promoting patient safety and enabling evidence-based practice through informatics. Med Care. 2004;42(2 Suppl):49–56.
33. 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. PMID: 26369894
34. IMIA WG7. WG7 - IMIA Working Group on Health Informatics for Patient Safety. 2018.
35. Glikson E, Woolley AW. Human Trust in Artificial Intelligence: Review of Empirical Research. Acad Manag Ann. 2020;
36. Bishop P, Bloomfield R. A Methodology for Safety Case Development. Saf Reliab. 2000;20(1):34–42.
37. Haimes YY. On the Complex Definition of Risk: A Systems-Based Approach. Risk Anal. 2009;29(12).
38. 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.
39. 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. Elsevier; 2015;140:200–207.
40. 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. Elsevier; 2018;110:324–335.
41. Flood M, Habli I. Multi-view safety cases. IET Conf Publ. 2011;2011(578 CP):1–6.
42. Thorne SE, Robinson CA. Reciprocal trust in health care relationships. J Adv Nurs. 1988;13(6):782–789.
43. Song J, Zahedi FM. Trust in health infomediaries. Decis Support Syst. 2007;43(2):390–407.
44. Wardle C, Derakhshan H. Information Disorder: Toward an interdisciplinary framework for research and policy making. Rep to Counc Eur. 2017;108.
45. Classen D. Medication Safety: Moving from illusion to reality. JAMA. 2003;289(9):1154–1156.
46. Siau K, Wang W. Building trust in artificial intelligence, machine learning, and robotics. Cut Bus Technol J. 2018;31(2):47–53.
47. Amann J, Blasimme A, Vayena E, Frey D, Madai VI. Explainability for artificial intelligence in healthcare: a multidisciplinary perspective. BMC Med Inform Decis Mak. BioMed Central; 2020;20(1):1–9.
48. McCrorie C, Benn J, Johnson OA, Scantlebury A. Staff expectations for the implementation of an electronic patient record system: A qualitative study Corresponding author. BMC Med Inform Decis Mak. BMC Medical Informatics and Decision Making; 2019;19(222):1–14.
49. Adjekum A, Blasimme A, Vayena E. Elements of Trust in Digital Health Systems: Scoping Review. JMIR. 2018;20(12):e11254.
50. Morland C, Pettersen IJ. Translating technological change-new technology and practices in a hospital. Int J Product Perform. 2018;67(6):1000–1015.
51. Cresswell K, Sheikh A. Organizational issues in the implementation and adoption of health information technology innovations: An interpretative review. Int J Med Inform. Elsevier Ireland Ltd; 2013;82(5):e73–e86. PMID: 23146626
52. 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). PMID: 31045497
53. 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. Elsevier Ltd; 2020;84(December 2019):103033. PMID: 31987516
54. Arnold M, Piorkowski D, Reimer D, Richards J, Tsay J, Varshney KR, et al. FactSheets: Increasing trust in AI services through supplier’s declarations of conformity. IBM J Res Dev. 2019;63(4–5).
55. Baker K, Dunwoodie E, Jones RG, Newsham A, Johnson OA, Price CP, et al. Process mining routinely collected electronic health records to define real-life clinical pathways during chemotherapy. Int J Med Inform. Elsevier Ireland Ltd; 2017;103:32–41. PMID: 28550999
56. 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. Elsevier; 2016;67:99–117.
57. Saripalle R, Runyan C, Russell M. Using HL7 FHIR to achieve interoperability in patient health record. J Biomed Inform. Elsevier; 2019;94(103188).
58. 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.
59. Hansen DP, Pang C, Maeder A. HDI: Integrating health data and tools. Soft Comput. 2007;11(4):361–367.
60. 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.
61. Macrae C. Governing the safety of artificial intelligence in healthcare. BMJ Qual Saf. 2019;28:495–498.
62. 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.
63. Hirst A, Philippou Y, Blazeby J, Campbell B, Campbell M, Feinberg 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. PMID: 29697448
64. Oelze I, Neeser K, Müller E. PP31 Medical Device Regulation : What Is New? Int J Technol Assess Health Care. 2019;35(S1):42–43.
65. Begun JW, Zimmerman B, Dooley K. Health Care Organizations as Complex Adaptive Systems. In: Mick SM, Wyttenbach M, editors. Adv Heal Care Organ Theory. San Francisco, CA: Jossey-Bass; 2003. p. 253–288.
66. Weick KE. Sensemaking in organizations. SAGE; 1995.
67. Mclachlan S, Potts HWW, Kudakwashe D, Buchanan D, Lean S, Johnson OA, et al. The Heimdall framework for supporting characterisation of learning health systems. J Innov Heal Inf. 2018;25(2).
68. 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. PMID: 25831959
69. Greenhalgh T, Wherton J, Papoutsi 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;19(11). PMID: 29092808
70. Haimes YY. On the Definition of Resilience in Systems. Risk Anal. 2009;29(4):498–501.
71. Morozov E. To Save Everything, Click Here: The Folly of Technological Solutionism. New York: PublicAffairs; 2013.
72. Maturo A. Fatism, self-monitoring and the pursuit of healthiness in the time of technological solutionism. Ital Sociol Rev. 2014;4(2):157–171.
73. 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. Springer Netherlands; 2019;22(3):363–374.
74. 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.
75. Rae A, Provan D, Aboelssaad H, Alexander R. A manifesto for Reality-based Safety Science. Saf Sci. 2020;126(June).
76. Kok R. Corrected JMIR citation style for Mendeley desktop [Internet]. 2014.