Safety Informatics: Meeting the patient safety challenges of health information technologies

*Likely word count for Viewpoint or Perspective article = 2,000 words*

# Introduction

Healthcare is becoming increasingly digital and connected (Wickramasinghe and Bodendorf, 2020). 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 adaptations like video consultation, which has accelerated community learning (Wherton *et al.*, 2020). Other technologies like electronic health records, decision-support tools and handheld medical devices have been developed and used for many years with reported benefits for patient care but also with concerns for patient safety (Sittig *et al.*, 2018). It is currently unclear what the implications are for patient safety as existing health information technologies become ubiquitous with increasing pace and interact with new and emerging technologies (Benbya *et al.*, 2020). The need for an improved understanding and praxis of patient safety is even more urgent given the accelerated development and adoption during the COVID-19 pandemic.

The Patient Safety Translational Research Centres were set up by the UK National Institute for Health Research to translate patient-safety knowledge into practice. In April 2020, a national, expert collaboration led by the Centres from both Yorkshire and Humber and Greater Manchester was set up to appraise the academic evidence for patient safety in health information systems. Our collaborative intends to host a series of workshops that deliver publications to engage those directly involved in the delivery and study of healthcare, and to provide recommendations to address theoretical and practical challenges for safety informatics. Our aim is to define the field of Safety Informatics from a UK perspective and establish a platform of safety informatics theory for future research and development.

In Section 1 of this paper, we outline the Safety Informatics domain at the intersection of safety science and health informatics and highlight the urgent need for theory development and research. Section 2 summarises the workshop process. In Section 3, we present the output from the workshop: challenges and patient-safety implications of emerging health information technologies and recommendations to address them.

# Section 1: Patient Safety and Safety Informatics

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*” (Vincent, 2010). It is sometimes conceptualised as a balance between risks of harm, resource use, and improving patient health (Cook and Rasmussen, 2005). Healthcare is a safety-critical industry (Sujan *et al.*, 2016) that must approach safety by concurrently avoiding, managing and embracing risk (Vincent and Amalberti, 2016). This sets healthcare apart from other safety-critical industries that predominantly focus on only one of these approaches.

While the patient-safety perspective on health information technology (HIT) is not novel (e.g. Gómez-González et al., 2020; Kostkova, 2015), the types of patient-safety challenges and our capacity to address them are constantly in flux. HIT is becoming increasingly networked (Wickramasinghe and Bodendorf, 2020), posing novel safety issues as technologies interact (Paxton and Branca, 2020). This is because when HITs interact, they form a health information system (HIS) (Onik, Fielt and Gable, 2017), the success or failure of which is partly due to emergent rather than planned change resulting from local improvisation (Heeks, 2006). Such a conception of HISs as complex adaptive systems (Johnson, 2019) is contrary to a normative idea of planned actions and outcomes, instead acknowledging the bounded understanding and control that actors actually have. It is for this reason that standards and regulations for medical devices now recognise the need for a systems perspective and consider system configurations and processes for device integration

Challenges posed by an increasingly-complex HIS include: innovations that are unlikely to be equally affordable and available for all (McAuley, 2014; Robinson *et al.*, 2015; Lupton, 2017; Banerjee, 2019); the transient relevance of algorithms and models (Jenkins *et al.*, 2018); a continued lack of sufficient testing, despite early calls (Leveson, 1986); and societal challenges like an aging population (Pilotto, Boi and Petermans, 2018); and legal and political jurisdiction (Wismar *et al.*, 2011). Each of these challenges are associated with known and unknown implications for patient safety, which need to be addressed for responsible provision of healthcare. There is a need for rigorous study of the relationship between HISs and patient safety, i.e. a Safety Informatics.

Although there is no official definition of 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*” (IMIA WG7, 2018). This scope is exemplified in Singh and Sittig's (2016) Health Information Technology Safety Measurement Framework, which defines three safety domains embedded in a socio-technical work system: safe HIT, safe use of HIT, and using HIT to improve safety. The aim of Safety Informatics is to address these domains using principles from information science, i.e. the representation, storage, supply, search for and retrieval of relevant information (Stock and Stock, 2013).

# Section 2: Method

A workshop of 14 health informatics researchers was convened who represent those who develop and evaluate HIT. Collaborators discussed the patient-safety implications of the challenges posed by a set of new and emerging HITs that were collated from a scoping review of the academic, commercial and grey literature relating to HITs and HISs. In subsequent meetings, the group collated and synthesised contributions to 1) describe characteristics of new and emerging HITs, 2) describe the challenges posed when HITs are brought together within HISs, 3) describe the patient-safety implications of these challenges, and 4) recommend approaches to address the patient-safety implications.

We defined emerging technology as innovation, novel application of an existing technology, or novel uptake or use of an existing technology by an organisation or user. Table x1x shows some of the example HITs considered. The technologies are characterised by personalisation, decentralisation, a systems orientation, and a move toward a user-led/patient-centred experience.

# Section 3: Results

The workshop produced seven challenges that new and emerging HIT posed, each with implications for patient safety. Table xC.I.R.x summarises the challenges and our theoretical and practical recommendations to address the safety concerns. Each is only briefly presented below with references for further reading.

## Difficulty conceptualising threats to patient safety

Firstly, much of the innovation is not physical, instead leveraging existing hardware in novel ways. This manifests as software, systems architecture and communication protocols. 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.

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 in acceptably safety within a particular context (Bishop and Bloomfield, 2000). 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 NHS, 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 (Sujan *et al.*, 2016). The preparation of safety cases guides reflexivity that can be insightful when combined with a systems approach to conceptualising risk and safety (Haimes, 2009a; Ravitz *et al.*, 2013). Thus, patient safety might be facilitated by the use of dynamic (Denney, Pai and Habli, 2015), multi-view (Flood and Habli, 2011) safety cases for HIT (Despotou *et al.*, 2012; Habli *et al.*, 2018) and for healthcare services (Sujan *et al.*, 2015).

## Unclear how to integrate and interpret data streams

Secondly, more data of a greater variety can be collected with greater ease and speed but it is not clear how they can be sensibly integrated and interpreted (Ranjan *et al.*, 2018). 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 HITs] *… to achieve a seamless integration*” (Díaz, Martín and Rubio, 2016). Proposed solutions include standards for exchanging electronic health records (Saripalle et al., 2019; see Houta et al., 2019 for application in epilepsy data), distributed architectures to integrate electronic health records (Roehrs, André and Righi, 2017; Roehrs, 2019; Roehrs *et al.*, 2019), and 3rd-party infrastructure for linkage and querying of electronic health records, e.g. the CSIRO Health Data Integration tool (Hansen, Pang and Maeder, 2007).

Other contributing solutions include dynamic modelling of the data (Jenkins *et al.*, 2018), 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 interest (Sperrin *et al.*, 2019), which might clarify ‘Big healthcare data’ (Beam and Kohane, 2018). Finally, progress in artificial intelligence (particularly anomaly detection) might help to mitigate problems arising from data errors (Challen *et al.*, 2019; Macrae, 2019). For example, to minimise inappropriate decisions due to poor data quality, Sako et al. (2020) provides a conceptual framework for automated assessment of data quality and information integrity. These methods are examples of how HIT can be used to improve patient safety as well as help with safe use of HIT.

## Reactive regulations and standards

Thirdly, 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 implication is that avoidable harm might be experienced before mitigations are put in place. We recommend synchronisation of the development and evaluation of HIT, similar to the IDEAL framework (Sedrakyan *et al.*, 2016). The IDEAL framework champions gradual approval of medical devices rather than the one-shot approval of CE marking (The European Parliment and The Council of the European Union, 1993), which would allow “*graded, responsible, but earlier patient access*” (Sedrakyan *et al.*, 2016; Hirst *et al.*, 2019). Such frameworks simultaneously address concerns that the increased administrative burden of more-stringent regulations might delay products that are imperfect but practically useful (Oelze, Neeser and Müller, 2019).

We also recommend that regulators and developers of standards adopt a systems approach to conceptualising risk (Haimes, 2009a) to appropriately reflect the complex adaptive nature of healthcare (Plsek and Greenhalgh, 2001). It is hoped that these recommendations might help to manage increased sensitivity to safety during development.

## Trust in opaque and complex systems

Fourthly, trust has long been a part of patient care (Thorne and Robinson, 1988; Song and Zahedi, 2007) but it is threatened by the way that digitisation and complexification of HISs can hinder the proximity and intimacy of care. Trust in healthcare is partly a function of inter-personal behaviours (Calnan and Rowe, 2006) with the gatekeeping and competing incentives of actors in a HIS potentially jeopardising this trust (Mechanic and Schlesinger, 1996; Alaszewski, 2003). Without trust in expert and reliable sources, patients’ safety is under threat from misinformation and disinformation from sources more intimate and familiar (Wardle, 2017).

We suggest that a socio-technical perspective will help all stakeholders in healthcare to acknowledge the systemic nature of HISs and their place within healthcare systems.\*\*Jon Benn\*\*

…

A socio-technical perspective has the potential to address all three domains of HIT patient safety as proposed by Singh and Sittig (2016) - safe HIT, safe use of HIT, and using HIT to improve safety – which is perhaps unsurprising given that it is explicitly a socio-technical model.

## Emergent patient-safety implications

Fifthly, although HITs are being developed to leverage HISs, e.g. the internet of things (Wickramasinghe and Bodendorf, 2020), safety considerations are often focused on the HIT in isolation. This reductionist approach leads to a myopic view of the HIT’s effects that does not consider the emergent, patient-safety implications of the HIT’s involvement within a HIS. Healthcare systems are complex with a diversity of organizational forms, interdependence, and feedback effects (Begun, Zimmerman and Dooley, 2003). They are also holarchical, like a systems of systems, as exemplified by the Heimdall framework of learning health systems (Mclachlan *et al.*, 2018) and Carayon *et al.*'s (2015) model of workplace safety. We recommend a systems and holarchical conceptualisation of healthcare processes and patient-safety implications to complement the complex, holarchical structure of healthcare.

To this end, Haimes (2009a) 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 (Haimes, 2009b). 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 (Hilborn, 2004). Such complexity approaches will also be useful in addressing the question of how these new and emerging challenges will interact with the existing challenges alluded to in Section 1.

## Solutionism

Sixthly, and 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”* (Morozov, 2013). Examples include diet apps that inappropriately simplify body composition as merely a function of calorie consumption (Maturo, 2014), and the legal and ethical consequences of treatments like deep brain stimulation (Gardner and Warren, 2019). The implications for patient safety are that HIT interventions might be unfit for the true hazards that they present because of distraction by techno-optimism or technology push.

In addition to earlier recommendations of adopting socio-technical perspective and a systems approach to conceptualising risk, solutionism can be addressed by adopting a systems approach to patient safety. Ravit*z et al*. (2013) describe such an approach with a case study on medication infusion pumps and the Systems Engineering Initiative for Patient Safety model, SEIPS, provides a framework for understanding the structures, processes and outcomes in healthcare, more generally (Holden *et al.*, 2014). These approaches can help to sensitise developers and users of HIT to the relationships within healthcare systems that might facilitate unintended consequences.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Table xC.I.R.v1x** Summary of recommendations to address safety concerns posed by the challenges of new and emerging health information technology. Recommendations are tagged as theoretical, T, and practical, P, in line with the foundational aim of the workshop series. | | | | | | |
|  | **Challenges** | **Implications for patient safety** | **Recommendations** | **Safe**  **HIT** | **Safe use of HIT** | **HIT to improve safety** |
| 1 | Difficult to conceptualise threats to patient safety from non-physical innovations. | Inadequate consideration of threats to patient safety. | Systems approach to conceptualising riskT; Safety casesP; Socio-technical perspectiveT | x | x | - |
| 2 | Unclear how to sensibly integrate and interpret new and voluminous data streams. | Missed opportunities to use data; Inappropriate use of data; Biased use of data. | Dynamic and causal modelling continuously surveilled for performanceP; Middleware for interoperabilityP; Standards for linkage and exchange of healthcare dataP; Automated anomaly detectionP | x | x | x |
| 3 | Reactive regulatory- and standards-based approaches to safety. | Avoidable harm is experienced before mitigations are put in place. | Gradual approval of medical devicesP; Systems approach to conceptualising riskT | x | - | - |
| 4 | Difficult to build and maintain trust in health information systems that are obscure and complex. | Misinformation and disinformation threaten patient safety. | Socio-technical perspectiveT; | x | x | x |
| 5 | Emergent patient-safety consequences in health information systems. | Hazards cannot be completely foreseen. | Systems approach to conceptualising riskT; Systems approach to patient safetyT; Safety casesP; Socio-technical perspectiveT; Gradual approval of medical devicesP | x | x | - |
| 6 | Solutionism inappropriately simplifies problems and predicaments. | Unfit interventions and assurances are suggested. | Socio-technical perspectiveT; Systems approach to conceptualising riskT | x | - | - |

# Conclusion

The intention of this article was to begin the process of developing the theoretical and practical foundations of safety informatics, answering calls for practical progress in safety science (Rae *et al.*, 2020) and a unifying theory (Swuste *et al.*, 2020). We presented six challenges posed by new and emerging HITs, described the implications for patient safety, and recommended theoretical and practical mitigations. These challenges, implications and recommendations were gathered at a workshop of health informatics researchers focused on exploring the theoretical and practical foundations of safety informatics. Subsequent workshops in our series will address the implications of contemporary safety theory for digital innovation, sociotechnical evaluation of digital technology, and digital technology designed to improve patient safety (Johnson *et al.*, 2020). This article contributes foci for these future discussions as we establish a platform of safety informatics theory for future research and development.

# References