Safety Informatics: Meeting the patient safety challenges posed by emerging health information technologies

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

# Introduction

Healthcare is becoming increasingly digital and connected (Wickramasinghe & Bodendorf, 2020). 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 while existing health information technologies become ubiquitous with increasing pace and interact with new and emerging technologies (Benbya et al., 2020).

In April 2020, we set up a national, expert collaboration to appraise the academic evidence for patient safety in health information systems. The collaborative intended to host a series of workshops that deliver publications to engage those directly involved in healthcare delivery and research, and to provide recommendations to address theoretical and practical gaps in the safety of informatics. The collaboration was led by the National Institute for Health Research Patient Safety Translational Research Centres from both Yorkshire and Humber, and Greater Manchester, UK (Johnson et al., 2020). The primary planned deliverable from the collaboration was a series of publications that begin to define the field of Safety Informatics as a platform for future directions in research.

In Section 1 of this paper, we define the Safety Informatics domain and highlight the need for research. Section 2 provides an overview of the workshop process during the development of this publication. In Section 3, we synthesise the output of the first workshop, which addressed the challenges and patient-safety implications of emerging health information technologies. The final section suggests recommendations for theoretically-informed frameworks to address these patient-safety implications.

# Section 1: Patient safety and Safety Informatics

\*Introduce patient safety to set the context

\*Discuss the relationship between patient safety and health information technology

\*\*Must distinguish between health information technology and health information systems.

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. For example, there continues to be rapid progress in the development and uptake of devices compatible with the Internet of Things: “*a network of devices all embedded with electronics, software, sensors, and connectivity to enable them to connect, interconnect, and exchange data*” (Wickramasinghe & Bodendorf, 2020). These networked devices, such as smart continuous glucose monitors (Facchinetti, 2016) and Parkinson’s disease monitoring watches (Bot et al., 2016), pose novel risks (Paxton & Branca, 2020). This is because when health information technologies interact, they form a health information system (HIS) (Onik et al., 2017), which has the potential to improve patient care but also to threaten patient safety in unintended and emergent ways (Heeks, 2006). 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 (e.g. IEC, 2006, 2009, 2011; see Chadwick et al., 2012 for discussion). Yaqoob et al. (2019) provide a lengthy report on the security and regulatory vulnerabilities associated with networked medical devices, while Benson and Grieve (2016) provide a thorough discussion of the principles of health interoperability.

Other challenges posed by an increasingly-complex HIS include: innovations that are not likely to be equally affordable nor available for all (Banerjee, 2019; Lupton, 2017; McAuley, 2014; Robinson et al., 2015); the transient relevance of algorithms and models (Hickey, Grant, Caiado, et al., 2013; Hickey, Grant, Murphy, et al., 2013; Jenkins et al., 2018); a continued lack of sufficient testing, despite early calls (Leveson, 1986); and societal challenges like an aging population (Pilotto et al., 2018), and legal and political jurisdiction (Wismar et al., 2011). Each of these challenges include some unknown implications for patient safety, which is why there is a need for rigorous study of the relationship between HISs and patient safety, i.e. a Safety Informatics.

## Safety Informatics

Karl Steinbuch is said to have coined the term *informatik* (Steinbuch, 1957) and it now functions as the German term for ‘computer science’ (Widrow et al., 2005). The anglicised term *informatics* has come to refer to interdisciplinary study of information and its environment*;* how it is represented, stored, searched and supplied (Gammack et al., 2011; Stock & Stock, 2013). Many subfields of informatics have been demarcated with medical informatics being one of the first (Kuhn et al., 2008). Biomedical (Shortliffe & Cimino, 2013), nursing (McCormick & Saba, 2015), clinical and clinical-research (Degoulet & Fieschi, 2012; Richesson & Andrews, 2019), public-health (Magnusson & Fu Jr., 2013), and bioinformatics (Baxevanis & Ouellette, 2020) are but a few of the further subfields recognised by the International Medical Informatics Association (IMIA, 2020), where they use principles from information science to address particular needs.

The International Medical Informatics Association (IMIA) working group on ‘Health Informatics for Patient Safety’ consider their role as “[promoting] *patient safety of health information systems and their associated medical devices. The focus…is 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. The framework defines three safety domains embedded in a socio-technical work system: safe HIT, safe use of HIT, and using HIT to improve safety. Safety Informatics address problems in all of these domains using principles from information science, i.e. the representation, storage, supply, search for and retrieval of relevant information (Stock & Stock, 2013).

# Section 2: Method

A workshop of 14 collaborators was convened who represent those who develop, evaluate and use health information technologies and their data for both research and practical purposes. Collaborators discussed the patient-safety implications of the challenges posed by a set of new and emerging health information technologies that were collated from a scoping review of the academic, commercial and grey literature relating to HISs. In subsequent meetings, the group collated and synthesised contributions to 1) describe characteristics of new and emerging health information technologies, 2) describe the challenges posed by the evolving HIS, 3) describe the patient-safety implications of the challenges posed, and 4) recommend approaches to address the patient-safety implications.

# Section 3: Workshop synthesis

## Characteristics of new and emerging HIT

We define 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 by collaborators. The technologies are characterised by…

## Challenges posed by new and emerging HIT

We propose six challenges posed by the kinds of HIT that are emerging. 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 non-physical influences because it requires more-abstract consideration of interactions and effects. Secondly, it is increasingly easier to collect data but it is not clear how they can be sensibly integrated and interpreted (Ranjan et al., 2018). 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.

Fourthly, although HITs are being developed to leverage HISs, 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 consequences of the HIT’s involvement within a HIS. Fifthly, 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 many medical treatments (Gardner & Warren, 2019).

Sixthly, the increased complexity and distal connectedness of HISs challenges notions of trust that have long been a part of patient care (Song & Zahedi, 2007; Thorne & Robinson, 1988). Trust in healthcare is a partly function of inter-personal behaviours (Calnan & Rowe, 2006) and the gatekeeping and competing incentives of actors in a HIS threaten this trust (Alaszewski, 2003; Mechanic & Schlesinger, 1996). Finally, there is the question of how these challenges will interact with the existing challenges alluded to Section 1.

## Patient-safety implications of HIT challenges

\*

# Section 4: Addressing challenges to patient-safety

In this section, we recommend theoretically-informed frameworks to address these patient-safety implications raised in Section 3.

## Safety cases

\*Suggestion: Ibrahim Habli (UoY) to lead on this section\*

\*Possible connection to decision field theory planning “individuals plan future choices on the fly through repeated forward-looking mental simulations”

The purpose of this subsection is to present the concept of a safety case (Denney et al., 2015; Despotou et al., 2012; Flood & Habli, 2011; Habli et al., 2019; Sujan et al., 2016, 2013, 2015).

## Interoperability

\*The purpose of this subsection is to present efforts made to improve the interoperability of health information technologies and health information technology systems. Special reference will be made to the HL7 FHIR standard created by HL7 International (Health Level Seven International, 2020), which is a standard for exchanging EHRs (Saripalle et al., 2019; see Houta et al., 2019 for application in epilepsy data), and an example of a distributed architecture to integrate EHRs (Roehrs et al., 2019, 2017), which makes use of blockchain approaches (Roehrs, 2019).

\*Middleware as “*an abstraction layer is necessary to abstract this heterogeneity in order to achieve a seamless integration with anything*” (Díaz et al., 2016)

\*The CSIRO Health Data Integration tool (Hansen et al., 2007)

## Standards

The purpose of this subsection is to present efforts to develop design standards for HIT (Kux & Majeed, 2017; Macrae, 2019; Masum et al., 2013), e.g. IEC 80001 standard (IEC, 2011), learning from Business Intelligence and sociotechnical theories (Moghimi et al., 2020), Clinical Decision Support Consortia (Wright et al., 2011), preceding scale-up with a scoping review of international, national, and relevant local guidelines (Furlong et al., 2019), Hippocratic Oath for Connected Medical Devices ; and using frameworks that sufficiently consider socio-technical systems and lifecycles of technology (Greenhalgh et al., 2017).

\*Studies in other domains suggest perceptions of risk diverge based on values (Regan, 2019), and call for discourse-based management of risk.

\*Also, bring in stuff on complex understanding of risk, and decisions under uncertainty.

Standards for HIT and HIS

## Dynamic and causal modelling

\*Suggestion: David Jenkins (UoM) to lead on this section\*

\*Possible citations: (Hickey, Grant, Caiado, et al., 2013; Huang et al., 2016; Sperrin et al., 2019, 2018; Su et al., 2018).

## Machine Learning for data quality

Despite the potential threats to patient safety, progress in artificial intelligence (particularly anomaly detection) might help to mitigate problems arising from data errors (an example of the HIS’s self-regulation (Comfort, 1994) ). 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. Such models are guides to operationalise data quality assessment protocols (Weiskopf et al., 2017, 2013), themselves informed by taxonomies of data quality dimensions (e.g. Feder, 2018; Weiskopf & Weng, 2013).

## Human Factors

\*Suggestion: Jon Benn (UoL) to lead on this section\*

# Conclusion

[Words < 150] The purposes of this section are to 1) summarise the intention of this first collaboration in the series, 2) succinctly summarise the characteristics of new and emerging health information technologies, 3) succinctly summarise the classes of patient-safety challenges and their safety implications, 4) succinctly summarise our suggested approaches to address the patient-safety challenges, 5) suggest the next steps required to facilitate these approaches, 6) foreshadow the subsequent collaboration in the series “*The implications of contemporary safety theory (Safety-I and Safety-II) for digital innovation in healthcare*”.

\*Space permitting, we might make the publication relevant to the COVID-19 pandemic by discussing patient-safety concerns arising from sudden atypical growth in remote monitoring, remote testing, remote imaging, robotic care, and personal preventive medicine.

\*Talk about “Our research highlights that such change is not merely about installing and using new technology. It involves introducing and sustaining major changes to a complex system with multiple interacting components” (Wherton et al., 2020)

The intention of this article was to begin the process of developing the theoretical and practical foundations of safety informatics, contributing to a unifying theory that is lacking in safety science (Swuste et al., 2020). At the time of writing, the SARS-CoV2 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). We anticipate that the pandemic has encouraged investment and production of remote health solutions at a pace far in excess of regulatory frameworks that were in place prior. In their 2020 Global Risk Report, the World Economic Forum note how health systems are often early adopters of technologies despite safety concerns (World Economic Forum, 2019). xIs the comment to be made about changes in regulations relating to COVIDx.

Perhaps the best defence against the challenges discussed in this article is to recognise and engage with health information systems as the complex dynamic systems that they are.

# References