
Article:
Habli, Ibrahim orcid.org/0000-0003-2736-8238, White, Sean Paul, Sujan, Mark et al. (2 more authors) (2018) What is the Safety Case for Health IT? A Study of Assurance Practices in England. Safety science. pp. 324-335. ISSN: 0925-7535

https://doi.org/10.1016/j.ssci.2018.09.001

What is the Safety Case for Health IT?
A Study of Assurance Practices in England

Ibrahim Habli
(Corresponding Author)
Department of Computer Science
University of York
York, YO30 5GH, England
ibrahim.habli@york.ac.uk

Sean White
Clinical Safety/Solution Assurance
NHS Digital
Leeds, England
sean.white@nhs.net

Mark Sujan
Warwick Medical School
University of Warwick
Coventry, England
m-a.sujan@warwick.ac.uk

Stuart Harrison
Clinical Safety/Solution Assurance
NHS Digital
Exeter, England
stuartharrison@nhs.net

Marta Ugarte
Department of Medical Retina
Moorfields Eye Hospital NHS Foundation Trust London
London, England
marta.ugarte@moorfields.nhs.uk

Abstract

Objective Health IT (HIT) systems are increasingly becoming a core infrastructural technology in healthcare. However, failures of these systems, under certain conditions, can lead to patient harm and as such the safety case for HIT has to be explicitly made. This study focuses on safety assurance practices of HIT in England and investigates how clinicians and engineers currently analyse, control and justify HIT safety risks.

Methods Three workshops were organised, involving 34 clinical and engineering stakeholders, and centred on predefined risk-based questions. This was followed by a detailed review of the Clinical Safety Case Reports for 20 different national and local systems. The data generated was analysed thematically, considering the clinical, engineering and organisational factors, and was used to examine the often implicit safety argument for HIT.

Results Two areas of strength were identified: establishment of a systematic approach to risk management and close engagement by clinicians; and two areas for improvement: greater depth and clarity in hazard analysis practices and greater organisational support for assuring safety. Overall, the dynamic characteristics of healthcare combined with insufficient funding have made it challenging to generate and explain the safety evidence to the required level of detail and rigour.

Conclusion Improvements in the form of practical HIT-specific safety guidelines and tools are needed. The lack of publicly available examples of credible HIT safety cases is a major deficit. The availability of these examples can help clarify the significance of the HIT risk analysis evidence and identify the necessary expertise and organisational commitments.

Keywords: Health Information Technology; Patient Safety; Risk; Hazard; Safety Case.

1 INTRODUCTION

Health Information Technology (HIT) systems are increasingly categorised as safety critical since failures of these systems, under certain conditions, can lead to patient harm [1-4]. As a result, different national reviews have encouraged health systems and health services to consider, and where appropriate adapt, practices in other high-risk sectors, particularly aviation [10], which adopt systematic approaches to risk management [11-12]. This typically includes the implementation of a proactive safety management system, generation of a safety case and hazard log and institutionalisation of an open safety culture [13].

In England, the National Health Service (NHS) has been promoting and supporting such approaches for HIT safety assurance [14], through a dedicated Clinical Safety Team at NHS Digital. NHS Digital is a public body within the Department of Health that is responsible for providing data and IT systems for commissioners, analysts and clinicians in health and social care. Two safety standards, targeting HIT manufactures (SCCI0129 [15]) and health organisations (SCCI0160 [16]), have been issued by the Standardisation Committee for Care Information on behalf of NHS England. The NHS standards specify normative requirements, supported by informative guidance, for the implementation of a risk management process, including safety incident management, and demonstration of organisational commitments. These standards mandate the appointment of Clinical Safety Officers (CSOs), who, in their capacity as experienced clinicians, are expected to lead the HIT risk management activities.

While the NHS safety standards for HIT provide risk management requirements and guidelines, it is unclear how they should be approached and implemented in practice. Even in safety-critical industries, there is considerable debate about the practical

problems with common risk assessment principles, such as the definition of risk or decisions about acceptability of risk [59] [60] [61]. In healthcare, these practical problems are exacerbated by the different organisational and cultural contexts. Failure to appreciate and properly understand these differences can lead to unsatisfactory adoption and frustration, and even threaten patient safety [62] [63].

This paper aims to analyse the practice of HIT safety assurance practices in England, as scoped by the SCCI0160 and SCCI0160 standards. The paper focuses on how practitioners interpret and implement the risk management activities defined in the standards and describes the uncertainties and practical problems they encounter. By understanding these uncertainties and problems, clinicians, engineers and safety assessors can proactively act on potential human, organisational and technical failures and latent faults, particularly during the HIT design and deployment stages, before they transform into hazardous events or result in patient harm. The insights into the practice of HIT risk management will be helpful in determining recommendations for improving existing standards, guidance, and practical implementation.

This paper is organised as follows. In Section 2, we review the published literature on HIT and patient safety and highlight the importance of the socio-technical dimensions of assuring the safety of HIT. In Section 3, we introduce our research question and explain our research proposition, which is based on the risk-based safety argument on which the SCCI0160 and SCCI0160 standards are centred. In Section 4, we describe the qualitative research methods that we used to evaluate the extent to which our proposition is supported by evidence from current HIT risk management practices in England. In Section 5, we present our results in terms of overarching safety assurance themes and detailed findings that relate to the different stages in the HIT risk

management process. In Sections 6 and 7, we discuss the implications of our results and present our conclusions and areas for further work.

2 THE IMPACT OF HIT ON PATIENT SAFETY – A CONTROVERSIAL EVIDENCE BASE

The World Health Organization (WHO) reports that approximately 1 in 10 hospitalised patients experience harm [44]. At least 50% of these experiences are preventable. In the United States for example, adverse medical events are the third leading cause of death [46]. In low-income and middle-income countries, WHO estimates that around two-thirds of all adverse events happen in these regions [44]. Given the scale of this problem, ensuring patient safety is now both a national and global concern.

Vincent defines patient safety as the "*avoidance, prevention and amelioration of adverse outcomes or injuries stemming from the process of healthcare*" [43]. Technology, combined with improved patient engagement, has played a key role in improving and even redefining the boundary of patient safety to the extent that many types of harm that were seen as inevitable in the past, e.g. healthcare-associated infections, are now regarded as preventable [7].

One of these technologies is HIT, which has the potential to improve patient safety but also introduce new hazards [3]. For example, Electronic Prescribing can help eliminate transcription errors in a paper-based process but also increase risk by inducing unsafe shortcuts and alert fatigue [49] [50] [51]. HIT is a broad domain, and the existing literature on the impact of the different aspects of HIT on patient safety is both extensive and controversial [64] [70]. Despite the major investments worldwide in HIT and many reports about the positive impact the use of HIT such as Electronic Health Records and Computerised Physician Order Entry systems can have [12], there is still a lively debate

documented in several systematic reviews about the extent to which the available evidence supports the claims about the safety benefits of IT in healthcare ([5], [65], [66]).

The Institute of Medicine released a report looking specifically at the impact of HIT on patient safety [3]. The report concluded that the current state of safety and HIT was not acceptable. In addition, there is an increasing amount of evidence to suggest that the introduction of HIT can lead to unintended consequences, and create opportunities for failure, which can have significant adverse effects on patient safety ([67], [68], [68]).

Black and colleagues found in their systematic review of the impact of HIT on the quality and safety of care that many HIT interventions failed to live up to expectations, because they did not integrate well into existing clinical processes [5]. Such concerns about the consideration of the wider context of HIT implementation have given rise to socio-technical models, such as the one put forward by Sittig and Singh [8]. In their socio-technical model, Sittig and Singh identified eight dimensions, namely: (1) hardware and software computing infrastructure, (2) clinical content, (3) human-computer interface, (4) people, (5) workflow and communication, (6) internal organisational policies, procedures and culture, (7) external rules, regulations and pressures and (8) system measurement and monitoring [8]. These dimensions are consistent with recent approaches to studying patient safety such as the Systems Engineering Initiative for Patient Safety (SEIPS) model [45], in which technologies such as HIT are one of many interacting components. Further, the socio-technical nature of HIT failures are systematically classified by Magrabi et al [19], highlighting how HIT safety problems emerge from the interweaving between human (e.g. cognitive load), organisational (e.g. staffing levels) and technological factors (data loss). Further, the importance of these factors have recently been emphasised by a review of HIT adoption in England, which was led by Robert

Wachter and supported by the UK Department of Health and NHS England [54]. The review recommendations also called for improved education around HIT for clinicians and the need to strengthen the role of Chief Clinical Informatics Officers in hospitals.

In terms of public policy, in 2012, a review of national HIT safety initiatives concluded that such programs "*are at varying different stages of maturity, with England having the longest standing and most well developed safety programs, while Canada and the United States are at earlier stages*" [17]. Recently, a retrospective review of 850 HIT events reported to NHS Digital between 2005 and 2011 was performed [18], offering further evidence that HIT failures have been hazardous (68% of the events) and were associated with patient harm (3% of the events) including 3 deaths. This is consistent with reviews of HIT incidents in the US and Australia [19-20]. However, as acknowledged by the authors, the study considered a "*snapshot*" of the events, due to underreporting [21-22], to allow us to generalise the results and make a decision concerning the level of patient safety risk posed by HIT.

In order to harness the potential benefits that HIT can bring to the safety of care, it is important, therefore, to appreciate the clinical processes and the social and cultural context within which HIT is introduced. This applies equally to the generic risk management principles that have been adopted from other safety-critical industries [11] [12]. Sujan and colleagues undertook a consensus development exercise with healthcare stakeholders, and found that participants suggested that the concepts of safety and risk management were poorly understood in healthcare, and that there was a lack of transparency about how decisions about risk management were undertaken [55]. In order to improve the practice of HIT risk management, it will be helpful to understand how healthcare practitioners make sense of existing risk management principles, and

the problems that they experience in the application of the recommended HIT safety standards.

3 RESEARCH QUESTION AND PROPOSITION

The current literature shows that HIT can have both benefits for patient safety as well as introduce new risks. In order to reduce the adverse impact on patient safety resulting from the adoption of HIT, standards based on generic risk management principles used in safety-critical industries have been developed. What remains unclear is the extent to which these risk management principles fit with the healthcare domain, and how healthcare stakeholders make sense of them.

Given the importance of studying HIT safety as a socio-technical topic, as identified from the literature review in Section 2, our primary research question is as follows:

How do clinicians and engineers analyse and justify HIT safety risks, considering the socio-technical dimensions of safety assurance?

That is, this study concerns how the risk management requirements for HIT are implemented in practice. Further, the study focuses on how clinicians and engineers explain the rationale for, i.e. justify, key decisions in the risk management process, e.g. the reasoning for scoping the HIT system and its clinical settings in a particular way and the assumptions and basis for choosing particular risk control options and acceptability criteria. These decisions are often subjective and qualitative and therefore the underlying reasoning and assumptions have to be explicitly communicated. The need for justification of residual risks, as discussed in the next sections, is tightly linked with the requirement to provide a safety argument for HIT as part of the wider clinical safety case.

In seeking to answer the above question, our aim is to understand the strengths and weaknesses of current risk management practices for HIT in England, specifically as implemented using the two national safety standards SCCI0129 and SCCI0160. In this section, we explore the risk management process in these standards (Section 3.1) and discuss how they form the basis for our research proposition (Section 3.2).

3.1 SCCI0129 and SCCI0160 Risk Management Process

The SCCI0129 and SCCI0160 safety standards follow the risk management principles established for medical devices and are consistent with ISO14971 [26]. The overall risk management process is depicted Figure 1. The process commences with defining the HIT system and its clinical scope. This includes the intended system functionality, e.g. prescribing or patient identification, and the specific care setting within which the system is deployed. This is followed by identifying the safety hazards posed by HIT. In this context, a hazard is defined as "*a potential source of harm to a patient*" [15], e.g. the patient receives more than the intended drug dose. The risk of each hazard is then estimated. A risk is defined as the "*combination of the severity of harm to a patient and the likelihood of occurrence of that harm*" [15], e.g. the likelihood that the patient suffers a permanent life-changing incapacity as the result of the drug overdose. Each risk is then evaluated against predefined acceptability criteria, e.g. as defined in a risk matrix.

Next, options are identified and analysed for controlling the risks that are deemed unacceptable, e.g. through redundancy and supervision. In the rare case that a risk is deemed unacceptable (i.e. given predefined risk thresholds or matrices) and further control is not practicable, additional analyses are required to determine if the clinical benefits outweigh the residual clinical risk. Otherwise, the project has to be re-appraised. Following the implementation and verification of the risk control measures, the

organisation has to evaluate the outcome of all the risk management activities, i.e. whether residual risks can be accepted. The final three activities in the risk management emphasise the through-life nature of safety analysis and the importance of reviewing and updating the safety evidence during the deployment, use, monitoring and maintenance of the HIT system.

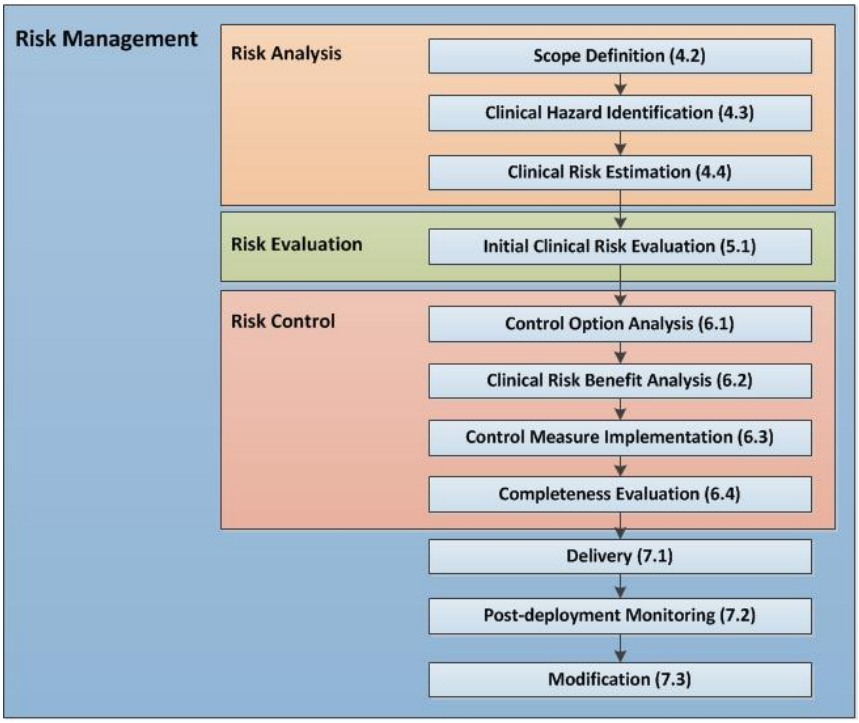

Figure 1: SCCI0129/SCCI0160 Risk Management Activities [15]

It is important to stress the significance of post-deployment monitoring [23] [24], particularly in assessing the effectiveness of the risk control measures, based on use data, and the on-going identification of any new safety conditions, e.g. hazards that were missed in the initial hazard analysis.

The above risk management activities produce two primary artefacts: Hazard Log (HL) and Clinical Safety Case Report (CSCR) [27-28]. The HL is a mechanism for recording the on-going identification, analysis and resolution of the HIT hazards and their

associated risks and controls. The HL essentially defines the evidence base generated from the risk management process, i.e. the data generated from risk analysis, evaluation and control as depicted in Figure 1. Since the evidence is rarely conclusive, it has to be explained and its sufficiency justified. This is performed using the CSCR, which documents an argument, based on the evidence, for why the system is considered to be safe for a given application in a given environment.

3.2 SCCI0129 and SCCI0160 Implicit Safety Argument

The aim of our study is to analyse the extent to which, by satisfying the risk management requirements of the SCCI0129 and SCCI0160 standards, organisations comply with a core, although currently implicit, risk-based argument that form the essence of the CSCR. This defines the theoretical proposition in this paper. We model this argument graphically in Figure 2, using the Goal Structuring Notation (GSN) [29]. GSN is a widely used notation for the representation of safety arguments in the safety-critical domain, capturing the individual elements of the safety argument, e.g. claims, strategies, context and evidence, and the relationships that exist between these elements.

Briefly, the chain of reasoning within the argument in Figure 2 is as follows: The top-level claim (*HIT Safety*) states that a HIT system is safe to use in a defined care setting. Both the description of the system and its setting, represented as *GSN Context*, should be generated from the Scope Definition activity in the risk management process in Figure 1. It is important to note that the scope of the argument is limited to HIT, which should contribute to a wider argument about the safety of the overall health services. This means that the scope of the HIT argument excludes certain types of risks, e.g. directly related to physical medical devices or drugs. The argument strategy (*Risk Strategy*) appeals to addressing the hazards and their associated risks as captured in the HL

(captured as *Context*). This is consistent with the risk-based and hazard-driven approach promoted in SCCI0129 and SCCI0160 standards. Given that it is often infeasible to eliminate all risks, the argument makes a subsequent supporting claim that any remaining risk, i.e. residual after implementing any control measures, are managed and accepted. The term '*accepted*' could be subject to different interpretations. The SCCI0129 and SCCI0160 standards give criteria for defining this term, namely that a residual risk is accepted if either it is within a predefined target (e.g. low/medium in a Clinical Risk Matrix) or the clinical benefits of the intended use outweigh the clinical risk (i.e. if further control is not practicable). This issue of risk-benefit analysis is a debatable and an ethically sensitive matter on which standards and legal systems have differed, i.e. similar to the discussion regarding the 'As Low As Reasonably Practicable' ALARP principle [48] [55]. In this particular case, the SCCI0129 and SCCI0160 standards are consistent with the medical devices safety standard ISO 14971 in allowing engineers and clinicians to determine, once all practicable control measures have been implemented, if a high risk can be accepted based on the clinical benefits that the technology can provide. For example, the technological safety risk posed during the transition period between an old and a new HIT, which might be high due to its impact on multiple services and patients, could be outweighed by the clinical benefits that result from the new system.

The aim of this argument is primarily to make the structure of the HIT safety argument explicit [12], highlighting that HIT safety assurance should be treated in the same way as other clinical interventions by considering the extent to which the technology can lead to, or mitigate, patient safety risks in a particular care setting.

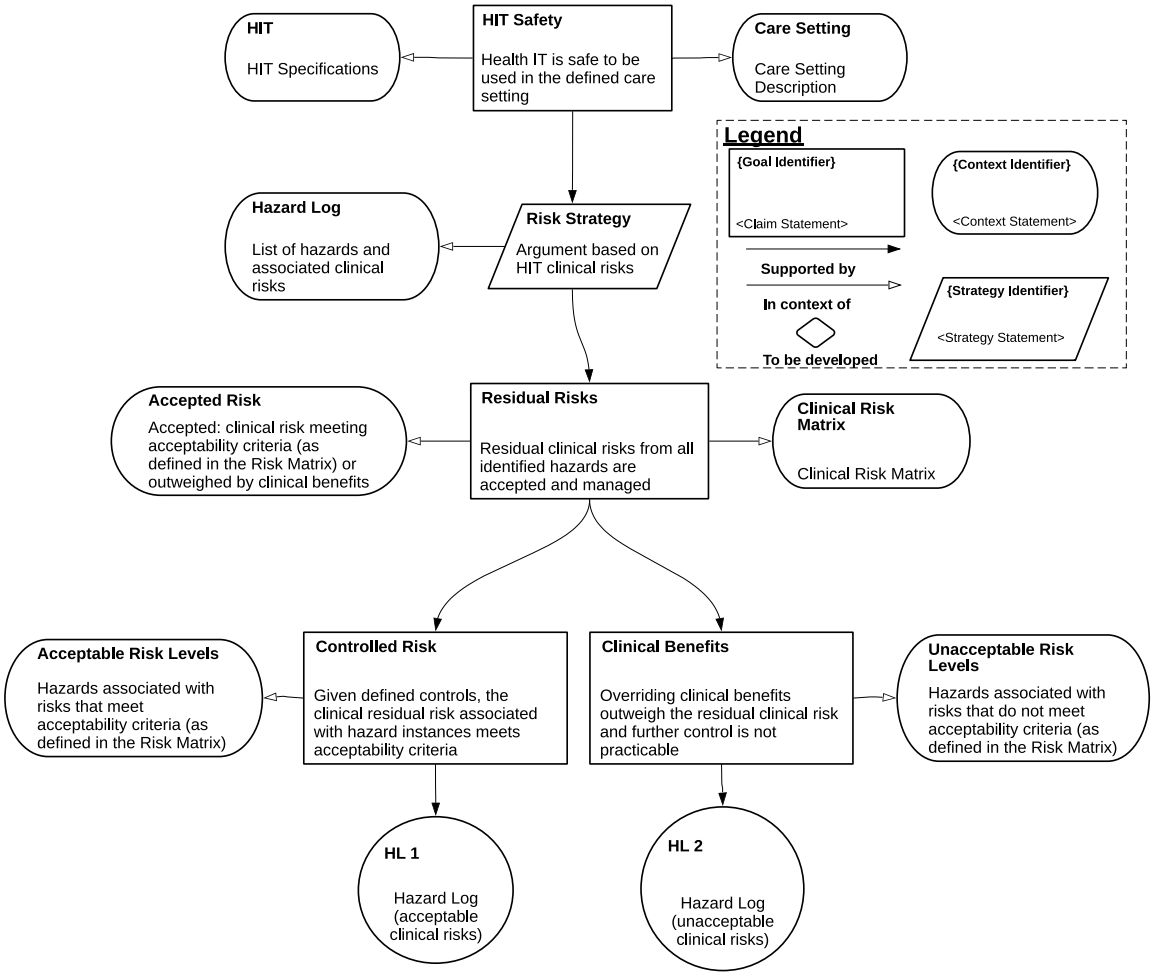

Figure 2: Risk-based Argument Structure

4 METHODS

In this paper, we are interested in understanding practice. As such, a qualitative research approach, in the form of a case study, is best suited [32]. We favoured breadth over depth, i.e. we were interested in eliciting the perspectives of a larger number of stakeholders as opposed to in-depth experiences of a few. Therefore, we opted against an ethnographic research design (e.g. studying the application of the HIT safety standards in one particular project).

This topic would benefit from active discussion among study participants with different backgrounds (i.e. engineering and clinical). To this end, a focus group approach was deemed to provide the best fit. The focus groups were complemented by document analysis of CSCRs that are produced as part of the HIT safety assessment process. Document analysis is complementary in that it focused on the evidence, as documented and explained in the reports submitted for formal review to the Clinical Safety Group at NHS Digital, and as such can particularly help identify safety documentation challenges.

Finally, in addition to reporting detailed and concrete findings, we are interested in identifying overarching safety assurance themes that cut across different types of HIT systems and healthcare settings. In order to achieve this, we used the Thematic Analysis methodology, based on the seminal work of Braun and Clarke [31], for supporting the systematic identification, analysis and reporting of patterns in qualitative data.

Our study had the ethics approval from Physical Sciences Ethics Committee at the University of York. Our data collection and analysis methods are explained in more detail in the next two sections.

4.1 Data Collection

Three separate one-day workshops were organised by the Clinical Safety Team at NHS Digital in February and March 2016, involving different participants at each workshop (Figure 3). The participants, 34 in total, were purposefully selected and invited by the Clinical Safety Team at NHS Digital due to their expertise in the development, deployment and/or assessment of HIT and their understanding of both the engineering and clinical perspectives of the technology. As illustrated in Figure 3, they represented the three main parties involved in HIT risk management: NHS Digital (authority), health

organisations (users) and HIT manufacturers (developers). The participants covered key roles primarily clinical safety officers, software engineers and safety assessors.

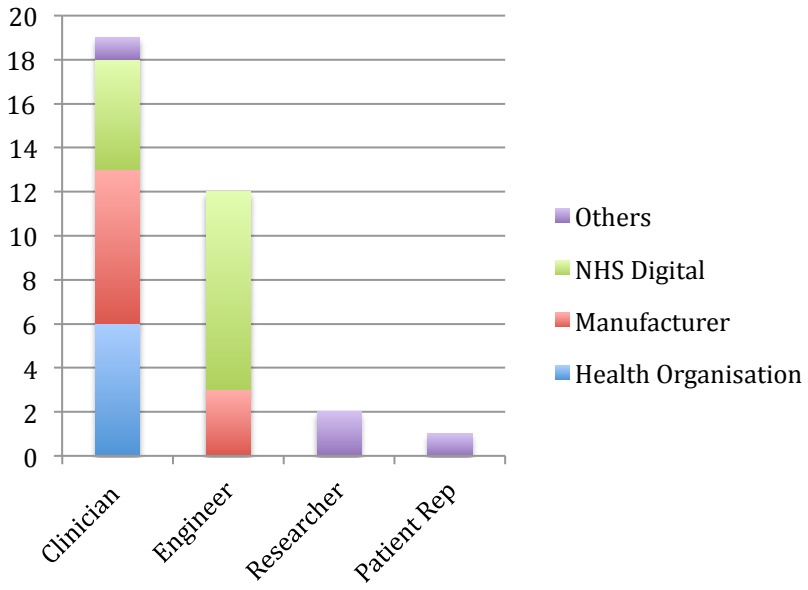

Figure 3: Workshop Participants

The workshops covered the core risk management activities in the SCCI0129 and SCCI0160 safety standards:

- Scope Definition: do we understand the HIT system, both its design and use, within the intended health and/or social care setting?
- Hazard identification: what are the potential sources of harm?
- Risk Estimation: what are the likelihood and severity of the harm associated with the identified hazards?
- Risk Control: if risks are not acceptable (i.e. given predefined risk thresholds or matrices), how are these controlled, e.g. through elimination and mitigation?
- Risk Acceptability: how are decisions made, and by whom, concerning risk acceptability?

Each of these topics at each workshop was allocated 20 minutes and was discussed in groups of 5 participants [30]. Each round started and focused on one of the questions shown in Table 1, which correspond to our overall research question and safety argument and are derived from the Risk Management process in Figure 1. However, it is important to note that in order to manage the time allocated for each workshop (5 hours) we had to cluster the different topics under no more than 5 rounds. This meant that we included Risk Evaluation under the Risk Estimation Round (under two different questions). Further, given the importance of risk acceptance decisions, we created a separate round for this complex issue that required significant input particularly from the clinical participants.

At the end of each round, members moved to new groups. Each group had a stable host who moderated the discussion. The role of the moderator was to ensure that the participants focused on the round question and encourage active engagement by all participants and record observations. Overall discussion sessions were scheduled to share insights with the larger group.

Table 1: Discussion Questions

Round 1: Scope Definition
How is the HIT scope defined so that it is clear, correct and comprehensive?
Round 2: Hazard Identification
How is Hazard Identification performed so that the hazards identified are specific, relevant, clearly documented and “complete”?
Round 3: Risk Estimation
How is the risk classification framework calibrated so that it is appropriate to the system and environment? How are decisions concerning severity and likelihood made, scoped and justified?
Round 4: Risk Control
How are risk controls identified, ranked, verified and monitored?
Round 5: Risk Acceptability
How are safety risk acceptance decisions made and justified? Who is responsible for making and approving these decisions?

The workshops were followed by detailed reviews of the CSCRs for 20 HIT systems, covering primary and secondly care, following the same questions listed in Table 1. The CSCRs were selected by the Clinical Safety Team at NHS Digital as a representative sample of the CSCRs that they had reviewed in the last 5 years. The CSCR reviews were used to corroborate and augment the data collected at the workshops. The review team comprised 5 safety experts from the Clinical Safety Team at NHS Digital. The document analysis is treated as a secondary source of data. Each CSCR was reviewed by one member of the team, with experience and competency in both safety and HIT.

The CSCRs considered diverse functions, including:

- Electronic prescribing
- Electronic health records
- Patient demographics
- Booking and referral
- Care planning
- Maternity care management
- Emergency care management
- Bed management
- Health data middleware

The CSCRs were submitted by health organisations (for specific deployments), manufacturers (for type approval) and NHS Digital (for the national infrastructure).

The workshop participants and moderators and the CSCR reviewers recorded their observations and comments in written summary notes, against the questions in Table 1, and were asked to note the organisational, clinical, human, technological and technical factors relevant for each of the risk management topics.

4.2 Data Analysis

The written summary notes were imported into NVivo11 for analysis. The text was coded following an iterative process and analysed using *Thematic Analysis* [31-32], determining and interpreting repeated patterns of meaning in the data set. The coding was *theory-driven*, based on how the SCCI0129 and SCCI0160 safety standards expect the clinicians and engineers to justify HIT risks, i.e. following the implicit risk-based argument in Figure 2.

The initial codes corresponded to the inputs to, and outputs from, the risk management activities. These inputs and outputs represent *hypothetical* weaknesses [25], combined with organisational factors [8], which have the potential to undermine the implicit risk-based argument (Figure 2). This was used to ensure the coding of specific weaknesses and strengths in intermediate stages (e.g. poor understanding of clinical context) and not just in the outcome (e.g. inappropriate classification of risks). The final phase involved combining the different codes into overarching themes using a thematic map.

5 RESULTS

Four themes that cut across the different HIT risk management activities were identified, representing two areas of strength: establishment of a systematic approach to risk management and close engagement by clinicians; and two areas for improvement: the need for greater depth and clarity in risk management practices and more organisational support for assuring safety.

These themes are summarised in Table 2. The data indicates that the assurance framework established through the SCCI0129 and SCCI0160 standards has provided a principled approach to risk management, building on best practice in system safety. In

particular, these standards are based on, and informed by, principles of system safety management in safety-critical industries, most notably the UK Defence Standard 00:56 [58]. The role of the clinicians, particularly the CSOs, has been recognised by the different organisations. Most of the safety analyses are clinically-led, with representation from multidisciplinary teams. However, concerns exist about the rigour, detail and clarity of the HIT safety evidence. The identified HIT hazards, and their associated risks and controls, are rarely specific to the system and the clinical environment, or justified in sufficient detail, to enable the stakeholders to evaluate and, where necessary, challenge the safety beliefs about the system. Further, organisational support for safety is fundamental, particularly with regard to making sufficient resources available for implementing the HIT risk management process. Unfortunately, these resources are seldom provided. Where they exist, such resources are typically used to confirm, rather than assess, the acceptability of the risk posed by the system. Risk analysis is also commonly performed late in the lifecycle. This often weakens the credibility of the evidence and its ability to influence the deployment of the system.

Table 3 provides a detailed summary of the specific safety assurance factors that were identified by our data analysis, which trace to one or more of the themes in Table 2. These factors are categorised as either technical or social and they are described against the particular HIT risk management activity to which they relate. Table 3 also lists specific recommendations that were made by the workshop participants. In the rest of this section, these factors and recommendations are examined in more detail and are illustrated through examples provided by the workshop participants.

Table 2: Summary of Themes, Representing Areas of Strength and Improvement

	Theme	Examples
Strengths	**Risk-based**: current approach provides a systematic process and a common language for identifying and analysing the risks of hazardous HIT failures, combined with the requirements for organisational commitment.	– Wide-scale use of HLs and CSCRs; – CSCRs cover HIT-related hazards, risk estimation, available controls and acceptance statements.
	Clinical engagement: there has been a recognition of the significant role of clinicians, particularly CSOs, during HIT risk management and approval.	– CSOs taking a leading role within health organisations, manufacturers and NHS DIGITAL; – CSO advice is now regarded as necessary for HIT approval.
Improvements	**Depth of evidence**: safety evidence tends to be generic and requires more explicit clinical and engineering justification in the context of the deploying health organisations.	– Risk estimation lacking empirical data, relevant to the clinical environment; – Insufficient clarity about the effectiveness of risk controls.
	Organisational support: level of organisational funding and commitment does not seem to be proportionate to the safety criticality of HIT, particularly within health organisations.	– Risk analysis performed as a late activity, purely for compliance reasons, as a tick-box exercise; – Lack of clarity about responsibilities and authorities.

Table 3: Summary of Safety Assurance Factors

Topic	Summary of Findings	Recommendations (Made By Participants)
Scope Definition	T1[1]: Great variation in the level of detail and clarity for specifying the HIT system and its clinical environment; T2: No consensus on key terms: 'clinical scope', 'intended use' and 'operational environment'; S1[2]: Good engagement by clinicians though often depends on availability rather than expertise; S2: Authorship bias: clinicians (contextual) vs engineers (technical); T3: Insufficient consideration of variation in practice in clinical environment and impact of local HIT configurations; T4: Lack of detailed information on integration and interfaces with external systems.	R1: Modelling notations needed for integrating clinical and engineering perspectives; R2: Clear definitions to be included in the standards; R3: More coverage required for different configurations and clinical settings; R4: More emphasis on interoperability requirements.
Hazard Identification	T5: Confusion about the terms hazard, risk, harm and quality issues; T6: Difficulty of positioning hazardous failures of HIT within care processes; T7: Hazards too detailed to reflect potential harm to patients; T8: Hazards very generic and poorly linked to clinical environment; S3: Hazards identified by manufactures lacking validation for their relevance by deploying health organisations; S4: Lack of early engagement in, and funding for, hazard identification; S5: Perception of hazard identification as a tick box exercise.	R5: Publish anonymised Hazard Logs for HIT and known hazards of care within the NHS; R6: Develop practical guidance on hazard identification workshops and techniques; R7: Develop guidance on the necessary clinical and engineering expertise needed for hazard identification.
Risk Estimation	T9: Two main risk matrices used: NHS NPSA and NHS Digital, with medium region leading to most confusion; T10: Too much customisation leading to complication in risk communication, rating and comparison; T11: Insufficient historical data to generate empirical estimate of severity and likelihood; T12: Risk parameters estimated qualitatively and subjectively, e.g. expert judgement; S6: Expert judgement not provided with clear justification; S7: Hazards biased based on clinical representation (of different specialities); T13: Risk overestimation as a result of confusing likelihood of hazard and likelihood of resulting patient harm; S8: Risk classification sometimes performed retrospectively; T14: Insufficient consideration of demographics and patient variation.	R8: Implementation of a consensus risk estimation framework is needed to ensure consistency and promote learning; R9: Stressing the importance of customising standard risk matrices to suit local environments; R10: Greater explanation and justification needed for severity and likelihood parameters.
Risk Control	T15: System re-design most desirable (removing source of hazard or carefully implementing alerts); S9: Training and appealing to clinical expertise most common; S10: Training generally regarded as a weak (and too generic) risk control; T16: Choice of control depends on phase: redesign during development and workarounds after deployment; S11: Alert fatigue regarded as a source of concern; S12: Concerns about lack of documentation, traceability and assessment of changes in risk controls; T17: Lack of explicit evidence and feedback about the effectiveness and suitability of risk controls.	R11: Importance of diversity and balance in risk control types; R12: Appealing to vigilance by clinicians should depend on detectability; R13: Training to be specific, justified and on-going; R14: Proactive monitoring of, and feedback on, workarounds and design changes.
Risk Acceptance	T18: Lack of documented clinical justification and technical explanation for risk acceptance; T19: Rare use of the 'As Low As Reasonably Practicable' (ALARP) principle; S13: No clearly established accountability and responsibilities of the stakeholders involved in risk acceptance decisions (senior management and CSOs); S14: Clear emphasis on professional registration and judgement of clinicians.	R15: Define more clearly the roles, responsibilities, authority and resources within both manufacturers and health organisations; R16: Greater emphasis on interpretation and justification of acceptance decisions.

[1] 'T' indicates a 'Technical' factor.
[2] 'S' indicates a 'Social' factor.

5.1 HIT Scope Definition

The *Scope Definition* covers the HIT functionality and clinical setting. The workshop participants indicated that it is often the hardest part of the process. The majority of the CSCRs reviewed lacked a detailed description of the HIT systems and their clinical context. This is attributed to factors that relate to the terminology used in the safety standards, the complex nature of HIT systems and the variable nature of the clinical settings.

Firstly, the terminology itself is problematic. Engineers and clinicians have different interpretations of the terms ‘clinical scope’, ‘intended use’ and ‘operational environment’. The current standards define some of these terms but not to the extent necessary to resolve the different interpretations.

Secondly, while the engagement between clinical and engineering teams is improving, there are some concerns as to whether the *right* people with the necessary skills and experience, including front-line clinical, are involved in the HIT risk management process as opposed to merely those who are *keen* to engage.

Thirdly, there is a general agreement that the system and its intended use are not described to the depth and clarity necessary to complete the subsequent safety analysis activities. Authorship bias of the document is a key factor. Clinicians tend to focus on high-level usage whereas engineers consider the more technical design. Unified notations, bridging the gaps between the clinical and engineering perspectives, appear to be needed.

Finally, current practices do not seem to cope with the high degree of variability in the clinical environment and with the bespoke system configurations. One senior clinical participant expressed this as an inherent characteristic of healthcare: "*if you ask 24 clinicians about e-prescribing you'll get 24 different answers*". This is often exacerbated by the emergent behaviours resulting from the complex interconnectivity and interoperability between the various HIT systems, including interfaces with external social care and national systems.

5.2 Hazard Identification

The workshop participants highlighted that the notion of *hazard* is not familiar within healthcare settings. It is seen as an engineering rather than clinical concept. The term *risk* is more recognisable by clinicians, as expressed by one participant: "*the NHS has always worked in the 'risks': don't know what a hazard is*". The overwhelming majority of hazards are care hazards, which predate the deployment of HIT and to which the technology now contributes, e.g. patient misidentification. Positioning the specific hazardous failures of HIT within the care process is seen as a difficult task.

Firstly, deciding on the level of granularity for hazard identification is problematic. On the one hand, many of the identified HIT hazards are too detailed and correspond to technical failures (i.e. 'network unavailability'). As such, they do not reflect the potential harm to patients. On the other hand, other hazards are defined generically, with little information about the context, to make them relevant to the clinical environment (e.g. 'wrong prescription'). In part, this can be complicated by a poorly-defined scope, as illustrated by one participant: "*an important distinction needed to be made between hazards caused by system and hazards caused by clinical activity. Can the system lead to patient harm or was the patient harm already there but the system perpetuates it?*" It

was noted that many of the events flagged by engineers as hazards were treated as quality issues by clinicians, i.e. events that commonly occur and from which recovery is expected, e.g. 'delay in providing care'.

Secondly, where do hazards come from? A common scenario has been to take the HL generated by the manufacturers and instantiate it to fit within the specific clinical context of the health organisations. The perception here is that the manufacturers are more competent and have the resources to produce the HL to the required quality. The potential consequence, however, is that health organisations adopt the HL without the adaptation necessary to cater for the specific local clinical requirements. This is, in part, due to lack of early engagement as highlighted by one participant: "*Poor quality is due to many reasons including doing the work last minute, 'as something that needs to be done', a tick box exercise. It is usually left to the clinician assigned rather than done in plenty of time with a multidisciplinary team. The hazards are generic, often lifted from other documents*". Some highlighted the lack of resources as the primary contributor: "*a continuing message is that there is no funding and resources provided to the NHS to deal with these issues*".

Finally, to ensure consistency and promote learning, some participants (particularly safety assessors) emphasised the need to "*publish anonymised hazard logs for HIT and known hazards of care within the NHS*", combined with "*practical guidance on Hazard Identification workshops and techniques*". That is, for HIT functions that tend to be common in many clinical settings, e.g. as part of electronic prescribing or patient administration systems, there is a need for the HIT safety community to collectively identify and make available common hazards that are associated with the use of these

functions, supported by guidance on how to analyse the risk of these hazards based on the specific characteristics of the HIT system and its clinical settings.

5.3 Clinical Risk Estimation

Two risk classification matrices are mainly adopted, namely the ones provided by the National Patient Safety Agency [34] and NHS Digital [35-36]. Views vary about the suitability of these matrices, ranging from treating them as the "*least understood*" to highlighting problems with specific parts, e.g. "*medium region is hard to deal with; too wide*". Many participants highlighted the importance of adaptation: "*never one size fits all*" and "*key is understand one's own matrix*". However, too much adaptation can make it difficult to communicate and compare risks between organisations, particularly in the event of incidents, e.g. inconsistent risk ratings of the same hazardous condition between the manufacturer, health organisation and NHS Digital. Participants recognised the "*potential for implementing a consensus' framework*" to aid risk communication, help ensure consistency and promote learning at the national level.

When using the risk matrices, it was observed that there is insufficient historical or experimental data to generate an empirical estimate of the severity and likelihood parameters. One participant attributed this to "*data for old systems not found or generalisable*". Each deployment of the technology is seen as novel, intended to cater for the local clinical requirements. As expressed by one participant, there is "*no denominator for likelihood in most cases*". As such, subjectivity is seen as inevitable; the risk parameters are estimated qualitatively based predominantly on expert judgment. For some analysts, the lack of precision is not regarded as a problem: "*main reason should be to compare the relative importance of the different risks rather than to be precise*".

However, as indicated in the earlier discussion, for this to be effective in communicating the level of risk posed by HIT, common or consistent risk matrices are necessary.

At a more detailed level, some recurring misconceptions were highlighted. Firstly, it was observed that many risks were overestimated as a result of confusing the likelihood of the hazard and that of the associated patient harm. According to the SCCI0129 and SCCI0160 standards, the likelihood parameter of a clinical risk is associated with the occurrence of harm. For example, the likelihood of a late e-prescription might be medium but the likelihood of any resulting patient harm might be very low due to the availability of a backup paper-based system. Secondly, the consideration of exposure and population size is often unclear in the risk estimates. Current risk estimates do not cater for differences in demographics and patient variables. For example, a large population with high-risk co-morbidities is a significant factor that could influence the severity of HIT hazards, i.e. delays in data communication between primary and secondary care organisations can lead to severe complications that might be easier to control in smaller communities. As such, patient demographics and social contexts have to be explicitly specified in the HIT Scope Definition. Thirdly, concerns were raised about instances where risk classification was performed retrospectively, as expressed by one participant: "*often start with idea of risk rating then look at severity and likelihood as validation*". This can be attributed to treating risk analysis as an afterthought: "*back documentation exercise rather than at current phase in lifecycle*". Finally, the need "*for greater explanation and justification in risk assessment*", i.e. expert justification, was highlighted both in the workshop and reviews. It was acknowledged that expert judgement is important but should be combined with a clear justification in order to address potential

bias "*based on clinical representation*", especially in cases where front-line clinical users from different disciplines with different risk profiles are under-represented.

5.4 Clinical Risk Controls

When risks are deemed unacceptable (i.e. given predefined risk thresholds or matrices), the consideration of further risk reduction is necessary. This ranges from system controls, e.g. re-design and testing, to organisational measures, e.g. process change and training. System redesign is recognised as the most desirable. Training, and appealing to clinical expertise, is highlighted as the most common.

Firstly, diversity and balance in the types of risk controls are seen as necessary. Redesigns are more likely to be feasible early in the development phase as highlighted by one participant: "*design is a stronger control as you are getting the error out*". Redesign takes different forms from removing the source of the hazards to implementing alerts, although alert fatigue was acknowledged as a source of concern. After deployment, workarounds are common. As expressed by one participant, "*users used the system beyond their intended use or had workarounds, which again increased risk and not something that could be controlled and tested for prior to implementation*". It is acknowledged that many workarounds are deployed for the right reasons, i.e. to mitigate new risks that are not explicitly considered in the CSCR.

However, the problem lies in the lack of traceability, monitoring and assessment of workarounds: "*often the answer is 'refer to business process' without stating what the business processes are*". That is, the opportunity to learn from, and improve based on, these workarounds is often lost.

Secondly, although training is seen as a weak risk control, it is heavily relied upon. The effectiveness of training is "*variable*". Claims about training have to be specific: "*the user is trained to do x and y*". The content of the training has to be justified. On-going training is required and should be "*widened to all users and not just select users for testing or acceptance*" as articulated by one participant.

Finally, closely linked with training is the role of clinicians as risk controls. Some participants emphasised the need for clinicians, as highly qualified professionals, to retain "*awareness*", "*responsibility*" and "*accountability*". However, many expressed concerns about over-relying on clinicians to compensate for poor system design. Appealing to vigilance by clinicians should depend on *detectability*, i.e. given the workload and time constraints, is it reasonable for a clinician to notice and recover from the hazardous HIT failure? One clinical participant expressed this as follows: "*it's easy in case of obviously wrong results or lack of system availability but harder in cases where the results are wrong but plausible".* Extracting evidence about the effectiveness of the risk controls, based on actual data, continues to be a challenge.

5.5 Clinical Risk Acceptance

The HIT safety evidence generated from the risk management activities is rarely conclusive. Risk decisions require interpretation and justification by those responsible for making them. However, there is a concern that such justification and the detailed clinical and technical explanation are rarely documented.

In the majority of the cases, the criteria against which the decisions are made tend to appeal to the risk classification matrix, e.g. lack of any risks rated as high. The principle that the risks should be As Low As Reasonably Practicable (ALARP) is mentioned [37]. However, the use of this principle, particularly in cases where it is believed that the

clinical benefits outweigh the residual clinical risk, remain rare and tend to be qualitative, i.e. no statistical basis for comparing costs and clinical benefits.

Further, there is no consensus on the parties responsible for making and approving the risk acceptance decisions. Senior managers are highlighted as ultimately accountable. However, given that they are remotely involved in the HIT safety analysis, the basis on which senior management approves the systems is unclear. As expressed by one participant: "*it is signed-off by top management though it is not clear what process and who has ultimately signed-off*". The size, cost and criticality of the system are key factors. Small-scale systems are typically approved by senior clinicians and rarely by the CEO. Clear responsibilities are also difficult to identify, given "*the culture within the NHS with changes all the time*", e.g. changes due to organisational restructuring by merging different hospital services or units.

More commonly, senior management approval relies on the advice given by the CSOs from the health organisation and the manufacture. One participant highlighted that "*CSOs have a key role in translating evidence and advising top management*". This was clearly the case in most of the CSCRs reviewed. The professional registration of the CSOs reinforces competency and accountability. This is particularly important where there are cost and safety tradeoffs, as indicated by one participant: "*the important thing was to ensure that clinical justification overrides any other justification such as financial*".

6 DISCUSSION

Our original proposition was that by satisfying the risk management requirements of the SCCI0129 and SCCI0160 safety standards, clinicians and engineers complied with the implicit risk-based argument depicted in Figure 2. Our analysis of the data collected from the workshops and CSCR reviews indicates that the degree of *detail* and *clarity* in the

HIT safety evidence is often insufficient to determine the extent to which this risk-based argument is supported. The problem lies in the way in which the risk management activities are implemented rather than in the argument itself. As highlighted through the recommendations in Table 3, Clinicians, engineers and assessors need practical means by which they determine if the evidence is rigorous, detailed and clear, given the risk posed by the system. This is a key area for improvement.

In Figure 4, we revisit the risk-based argument and annotate the different elements with specific recommendations, which were extracted from the data collected (as summarised in Table 3). For example, defining the HIT system and its environment clearly and concisely, taking into consideration variability in clinical practice, is fundamental and is highlighted in the 'Scope Definition' results presented in Table 3. The HIT safety evidence generated from risk analysis can easily be undermined due to a poor understanding of the systems and their care settings. Further, as indicated in Table 3 and illustrated in the annotated argument in Figure 4, the rationale for deciding on the likelihood and severity parameters for each risk should be more explicitly communicated.

It is important to note that the risk-based argument should not be seen as a static artefact [38-39]. Continuously updating the CSCRs, based on feedback from end-users, is essential, particularly given the common use of workarounds. Otherwise, gaps between the documented evidence and the actual safety of the HIT system might lead to "*a culture of 'paper safety' at the expense of real safety"* [40].

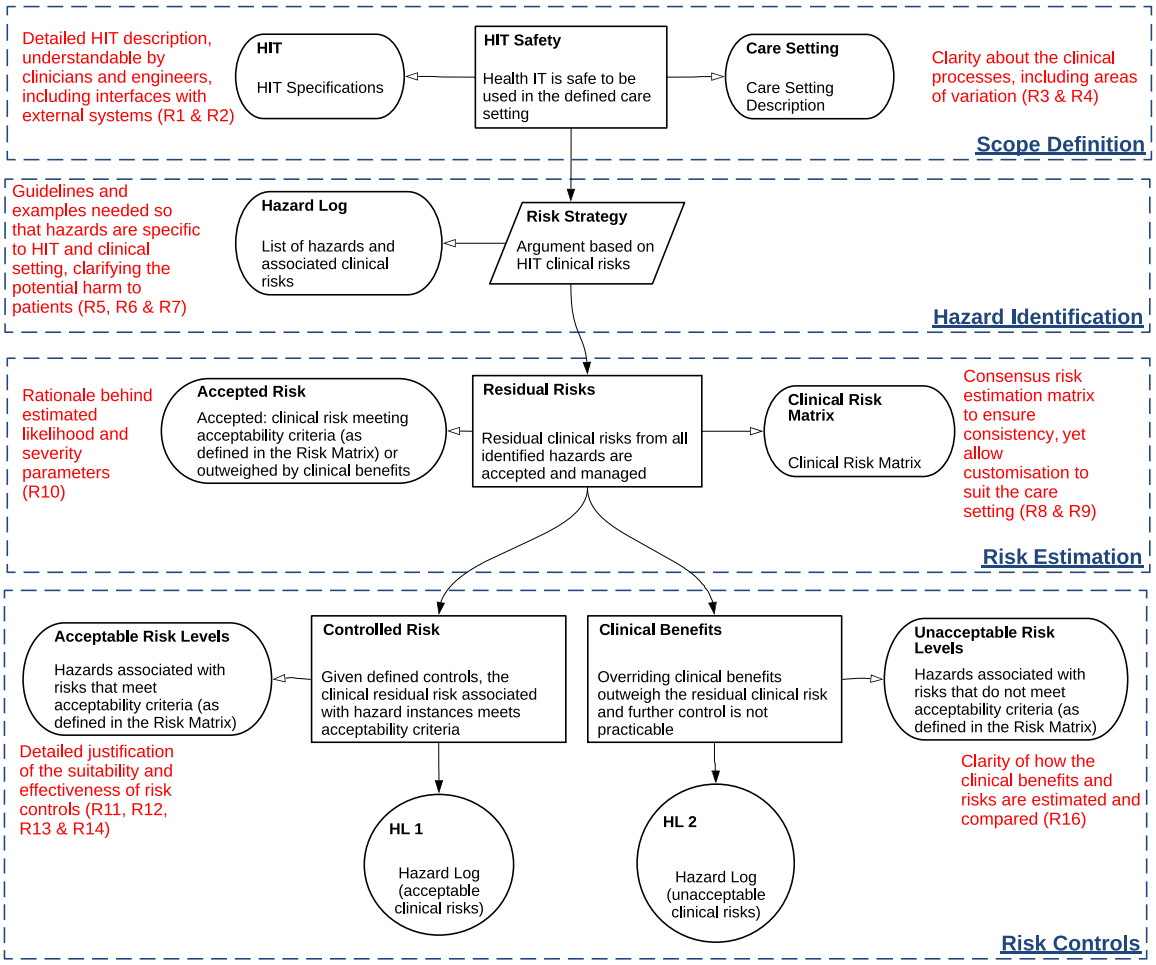

Figure 4: Risk-based Argument Pattern, Annotated with Areas for Improvement

Health organisations face challenges in terms of securing the necessary resources, particularly when addressing the HIT risk management requirements for the first time. As such, the risk-based argument cannot be seen in isolation of an organisational argument. In Figure 5, we sketch an example fragment of such an organisational argument, with four claims that have to be developed, and substantiated with evidence, concerning the level and the quality of support provided by the organisation. Such evidence, concerning the availability of resources, including a dedicated CSO, the competency of those performing the risk analysis and the safety culture within the organisation, could then be scrutinised to assess as to whether the organisational

support is proportionate to the scale, complexity and safety risk associated with the HIT system. This is an important issue that was highlighted in the recommendations in Table 3 (see R15). Weaknesses in this organisational argument could undermine confidence in the primary risk-based argument, e.g. a poor safety culture would undermine the credibility of the safety evidence captured in the Hazard Log.

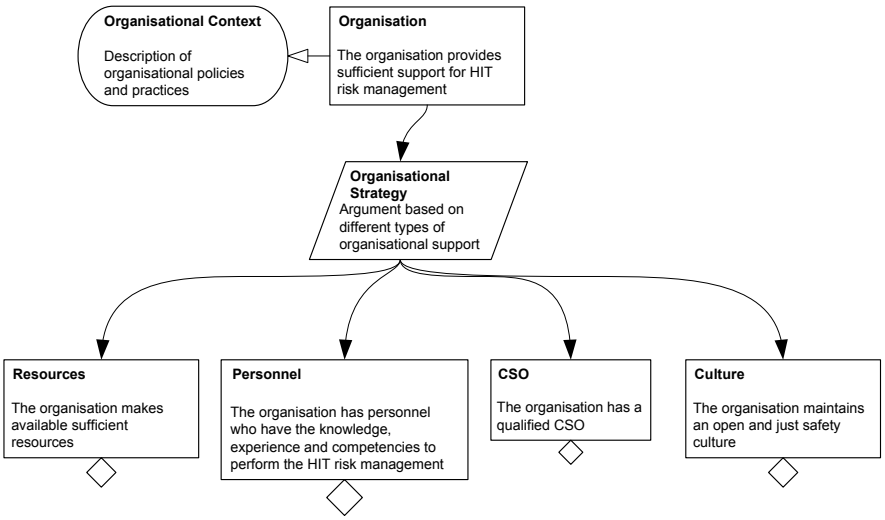

Figure 5: Organisational Argument

Further, the lack of publically available examples of HLs and CSCRs for HIT represents a significant deficit in the literature. Many of the HIT safety concepts, e.g. hazards and risk controls, could remain abstract unless they are related to, and illustrated using, specific health and social care settings and HIT functionality. As such, more practical HIT-specific safety guidelines and detailed examples are needed, and evaluated in different care settings [41], in order to clarify the significance of the HIT risk management and identify the necessary organisational commitments.

From the HIT safety literature's perspective, this study provides further evidence concerning the importance of treating HIT safety assurance as a socio-technical process, involving both clinical and engineering stakeholders [6] [8]. Although the data

highlights concerns about the lack of sufficient funding and safety culture, it also highlights conceptual challenges regarding the implementation of systems and safety engineering techniques in healthcare settings [9]. This was exemplified in the difficulty of modelling the HIT system given the variable nature of clinical settings; a significant issue that has been highlighted in the patient safety literature [45] [7]. The current literature on Resilience Engineering [39] and Safety 2.0 [56] [57] emphasise the need to redefine the notion of variability. This is in order to help distinguish between, on the one hand, unsafe violations and, on the other hand, desirable performance adjustments that are necessary to ensure the ability of the system to maintain safety, given changing demands and disturbances. The Systems Engineering Initiative for Patient Safety (SEIPS 2.0) [45] also now more explicitly considers variability through the concepts of configuration and adaptation.

Another key conceptual challenge relates to the difficulty of resolving the different interpretations of the notion of hazards and risk classification schemes for HIT and how they relate to hazards and risks at the health service level. That is, it is important to explore and evaluate more explicitly the relationship between a HIT safety case and the overall safety case for a hospital, of which the HIT safety issues are one of many important, and sometimes competing, factors.

Finally, in making the case for HIT, the decision-making process would benefit from the rigour that Health Technology Assessment (HTA) [52] could bring, i.e. similar to the application of HTA to other healthcare interventions, e.g. for medical procedures and drugs, in which different types of clinical, social, economic, and organisational risks and benefits are compared and analysed [53]. That is, HTA and safety risk management can be seen as complementary. On the one hand, HTA is used to inform policy decisions by

searching for *actual* evidence of effectiveness and complementing this with an economic evaluation, i.e. ensuring that funds are allocated in the best possible way. On the other hand, safety risk management is used to identify *potential* hazards and risks and analyse means of managing the uncertainty with the HIT design and use. As such, HTA can inform HIT safety decisions, because it can provide concrete evidence of effectiveness, and the rigorous evaluation designs (e.g. Randomised Controlled Trials) can provide useful insights for the risk management process.

7 CONCLUSIONS

Knowledge in patient safety tends to move in three phases [42]: '*superficial simplicity*' (e.g. emulation of safety practices in aviation), followed by '*confusing complexity*' (e.g. unique healthcare characteristics and assumptions emerge and challenge the effectiveness of the new approaches) and ultimately '*profound simplicity*' (e.g. open safety culture is seen as a foundational aspect). Current HIT safety practices in England are in the second phase. Adopting a systematic approach to risk management, building on best practice in system safety, has been beneficial. Much of the benefit has been realised due to the close engagement by the clinicians. However, despite such progress, more work remains in order to mature current safety assurance practices and improve organisational support. Significant effort is still needed to develop and evaluate practical techniques and tools, in different health and social care settings, that help clinicians and engineers generate and explain the HIT safety evidence to the required level of rigour, detail and clarity.

ACKNOWLEDGMENTS

This work was supported, in part, through a grant by the UK Royal Academy of Engineering (ISS1516\8\8).

REFERENCES

[1] Ash, J.S., Berg, M. and Coiera, E., 2004. Some unintended consequences of information technology in health care: the nature of patient care information system-related errors. Journal of the American Medical Informatics Association, 11(2), pp.104-112.

[2] Koppel, R., Metlay, J.P., Cohen, A., Abaluck, B., Localio, A.R., Kimmel, S.E. and Strom, B.L., 2005. Role of computerized physician order entry systems in facilitating medication errors. JAMA, 293(10), pp.1197-1203.

[3] Committee on Patient Safety and Health Information Technology. HIT and Patient Safety: Building Safer Systems for Better Care. National Academies Press, 2011.

[4] Agboola, S.O., Bates, D.W. and Kvedar, J.C., 2016. Digital Health and Patient Safety. JAMA, 315(16), pp.1697-1698.

[5] Black, A.D., Car, J., Pagliari, C., Anandan, C., Cresswell, K., Bokun, T., McKinstry, B., Procter, R., Majeed, A. and Sheikh, A., 2011. The impact of eHealth on the quality and safety of health care: a systematic overview. *PLoS Med*, *8*(1), p.e1000387.

[6] Meeks, D.W., Takian, A., Sittig, D.F., Singh, H. and Barber, N., 2014. Exploring the sociotechnical intersection of patient safety and electronic health record implementation. Journal of the American Medical Informatics Association, 21(e1), pp.e28-e34.

[7] Vincent, C. and Amalberti, R., 2015. Safety in healthcare is a moving target. BMJ Quality & Safety, pp.bmjqs-2015.

[8] Sittig, D.F. and Singh, H., 2010. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. Quality and Safety in Health Care, 19(Suppl 3), pp.i68-i74.

[9] Wears, R.L., Cook, R.I. and Perry, S.J., 2006. Automation, interaction, complexity, and failure: A case study. Reliability Engineering & System Safety, 91(12), pp.1494-1501.

[10] Stolzer, A.J., Halford, M.C.D. and Goglia, M.J.J., 2015. Safety management systems in aviation. Ashgate Publishing, Ltd.

[11] Kapur, N., Parand, A., Soukup, T., Reader, T. and Sevdalis, N., 2016. Aviation and healthcare: a comparative review with implications for patient safety. JRSM open, 7(1), p.2054270415616548.

[12] Sujan, M.A., Habli, I., Kelly, T.P., Pozzi, S. and Johnson, C.W., 2016. Should healthcare providers do safety cases? Lessons from a cross-industry review of safety case practices. Safety Science, 84, pp.181-189.

[13] Dekker, S., 2012. Just culture: Balancing safety and accountability. Ashgate Publishing, Ltd.

[14] Department of Health, 2012. Health and Social Care Act 2012. The Stationery Office.

[15] NHS Digital. SCCI0129, Clinical Risk Management: its Application in the Manufacture of HIT Systems – Specification. Standardisation Committee for Care Information. 2016.

[16] NHS Digital. SCCI0160, Clinical Risk Management: its Application in the Deployment and Use of HIT Systems. Standardisation Committee for Care Information. 2016.

[17] Kushniruk, A.W., Bates, D.W., Bainbridge, M., Househ, M.S. and Borycki, E.M., 2013. National efforts to improve health information system safety in Canada, the United

States of America and England. International journal of medical informatics, 82(5), pp.e149-e160.

[18] Magrabi, F., Baker, M., Sinha, I., Ong, M.S., Harrison, S., Kidd, M.R., Runciman, W.B. and Coiera, E., 2015. Clinical safety of England's national programme for IT: A retrospective analysis of all reported safety events 2005 to 2011. International Journal of Medical Informatics, 84(3), pp.198-206.

[19] Magrabi, F., Ong, M.S., Runciman, W. and Coiera, E., 2010. An analysis of computer-related patient safety incidents to inform the development of a classification. Journal of the American Medical Informatics Association, 17(6), pp.663-670.

[20] Magrabi, F., Ong, M.S., Runciman, W. and Coiera, E., 2012. Using FDA reports to inform a classification for health information technology safety problems. Journal of the American Medical Informatics Association, 19(1), pp.45-53.

[21] Donaldson, L., 2002. An organisation with a memory. Clinical Medicine, 2(5), pp.452-457.

[22] Sujan, M., 2015. An organisation without a memory: A qualitative study of hospital staff perceptions on reporting and organisational learning for patient safety. Reliability engineering & system safety, 144, pp.45-52.

[23] Ross, A. and Anderson, J.E., 2015. Mobilizing resilience by monitoring the right things for the right people at the right time, in Wears, R.L., Hollnagel, E. and Braithwaite, J. eds., Resilient Health Care, Volume 2: The Resilience of Everyday Clinical Work. Ashgate Publishing, Ltd.

[24] Vincent, Charles, Susan Burnett, and Jane Carthey, 2014. Safety measurement and monitoring in healthcare: a framework to guide clinical teams and healthcare organisations in maintaining safety. BMJ Quality & Safety 23.8: 670-677.

[25] Rae, A., Alexander, R. and McDermid, J., 2014. Fixing the cracks in the crystal ball: A maturity model for quantitative risk assessment. Reliability Engineering & System Safety, 125, pp.67-81.

[26] International Organization for Standardization, 2000. ISO 14971: medical devices-application of risk management to medical devices. ISO.

[27] Kelly, T.P., 1999. Arguing safety: a systematic approach to managing safety cases. University of York.

[28] The Health Foundation, 2012. Using safety cases in industry and healthcare. The Health Foundation.

[29] GSN community standard, Version 1, Available: http://www.goalstructuringnotation.info/documents/GSN_Standard.pdf [Accessed 14 June 2016].

[30] Brown, J., Isaacs, D. 2015. The world café: shaping our futures through conversations that matter. Berrett-Koehler Publishers.

[31] Braun, V. and Clarke, V., 2006. Using thematic analysis in psychology. Qualitative research in psychology, 3(2), pp.77-101.

[32] Yin, R.K., 2013. Case study research: design and methods. Sage publications.

[33] Rae, A.J., McDermid, J.A., Alexander, R.D. and Nicholson, M., 2014. Probative blindness: how safety activity can fail to update beliefs about safety. In System Safety and Cyber Security. IET, pp.1-6.

[34] National Patient Safety Agency. 2008. A risk matrix for risk managers. NPSA.

[35] NHS Digital. SCCI0129, Clinical Risk Management: its Application in the Manufacture of HIT Systems – Implementation Guidance. Standardisation Committee for Care Information. 2016.

[36] NHS Digital. SCCI0160, Clinical Risk Management: its Application in the Deployment and Use of HIT Systems – Implementation Guidance. Standardisation Committee for Care Information. 2016.

[37] Health and Safety Executive. 2001. Reducing risk: protecting people. HSE.

[38] Denney, E., Pai, G. and Habli, I., 2015, May. Dynamic safety cases for through-life safety assurance. 37th International Conference on Software Engineering-Volume 2 (pp. 587-590). IEEE Press.

[39] Hollnagel, E., Braithwaite, J. and Wears, R.L. eds. 2013. Resilient health care. Ashgate Publishing, Ltd.

[40] Haddon-Cave, C., 2009. The Nimrod Review: an independent review into the broader issues surrounding the loss of the RAF Nimrod MR2 aircraft XV230 in Afghanistan in 2006, report. The Stationery Office.

[41] Ammenwerth, E., 2015. Evidence-based Health Informatics: How Do We Know What We Know? Methods Inf Med, 54(4), pp.298-307.

[42] Gandhi, T.K., Berwick, D.M. and Shojania, K.G., 2016. Patient Safety at the Crossroads. JAMA, 315(17), pp.1829-1830.

[43] Vincent C., 2010 Patient Safety, 2nd edn. Oxford: Wiley Blackwell.

[44] Patient Safety: Making health care safer. Geneva: World Health Organization; 2017.

[45] Holden, R.J., Carayon, P., Gurses, A.P., Hoonakker, P., Hundt, A.S., Ozok, A.A. and Rivera-Rodriguez, A.J., 2013. SEIPS 2.0: a human factors framework for studying and improving the work of healthcare professionals and patients. *Ergonomics*, 56(11), pp.1669-1686.

[46] Makary, M.A. and Daniel, M., 2016. Medical error-the third leading cause of death in the US. BMJ: *British Medical Journal* (Online), 353.

[47] Dekker, S.W. and Leveson, N.G., 2014. The systems approach to medicine: controversy and misconceptions. BMJ Qual Saf, pp.bmjqs-2014.

[48] Health and Safety Executive. Reducing Risks, Protecting People. HSE, 2001.

[49] Bates, D.W., Leape, L.L., Cullen, D.J., Laird, N., Petersen, L.A., Teich, J.M., Burdick, E., Hickey, M., Kleefield, S., Shea, B. and Vander Vliet, M., 1998. Effect of computerized physician order entry and a team intervention on prevention of serious medication errors. Jama, 280(15), pp.1311-1316.

[50] Kaushal, R., Shojania, K.G. and Bates, D.W., 2003. Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. Archives of internal medicine, 163(12), pp.1409-1416.

[51] Avery, A.J., Rodgers, S., Cantrill, J.A., Armstrong, S., Cresswell, K., Eden, M., Elliott, R.A., Howard, R., Kendrick, D., Morris, C.J. and Prescott, R.J., 2012. A pharmacist-led information technology intervention for medication errors (PINCER): a multicentre, cluster randomised, controlled trial and cost-effectiveness analysis. The Lancet, 379(9823), pp.1310-1319.

[52] Drummond, M.F., Sculpher, M.J., Claxton, K., Stoddart, G.L. and Torrance, G.W., 2015. Methods for the economic evaluation of health care programmes. Oxford university press.

[53] Bassi, J. and Lau, F., 2013. Measuring value for money: a scoping review on economic evaluation of health information systems. Journal of the American Medical Informatics Association, 20(4), pp.792-801.

[54] Wachter, R M. Making IT work: harnessing the power of health information technology to improve care in England. London, UK: Department of Health, 2016.

[55] Sujan, M.A., Habli, I., Kelly, T.P., Gühnemann, A., Pozzi, S. and Johnson, C.W., 2017. How can health care organisations make and justify decisions about risk reduction? Lessons from a cross-industry review and a health care stakeholder consensus development process. Reliability Engineering & System Safety, 161, pp.1-11.

[56] Hollnagel, E., 2014. Safety-I and safety–II: the past and future of safety management. Ashgate Publishing, Ltd.

[57] Sujan, M.A., Huang, H. and Braithwaite, J., 2017. Learning from incidents in health care: Critique from a Safety-II perspective. Safety Science, 99, pp.115-121.

[58] UK Ministry of Defence, 2007. Standard 00-56 on Safety management requirements for defence systems. Ministry of Defence, Directorate of Standardisation, Kentigern House, 65.

[59] Althaus, C.E., 2005. A disciplinary perspective on the epistemological status of risk. Risk Analysis, 25(3), pp.567-588.

[60] Aven, T. and Renn, O., 2009. On risk defined as an event where the outcome is uncertain. Journal of risk research, 12(1), pp.1-11.

[61] Aven, T., 2012. *Foundations of risk analysis*. John Wiley & Sons.

[62] Sutcliffe, K.M., Paine, L. and Pronovost, P.J., 2016. Re-examining high reliability: actively organising for safety. BMJ Qual Saf, pp.bmjqs-2015.

[63] Clay-Williams, R. and Colligan, L., 2015. Back to basics: checklists in aviation and healthcare. BMJ Qual Saf, 24(7), pp.428-431.

[64] Sujan, M., 2018, Managing the patient safety risks of bottom-up health information technology innovations : recommendations for healthcare providers. Journal of Innovation in Health Informatics, 25 (1).

[65] Brenner, S.K., Kaushal, R., Grinspan, Z., Joyce, C., Kim, I., Allard, R.J., Delgado, D. and Abramson, E.L., 2015. Effects of health information technology on patient outcomes: a systematic review. Journal of the American Medical Informatics Association, 23(5), pp.1016-1036.

[66] Ranji, S.R., Rennke, S. and Wachter, R.M., 2014. Computerised provider order entry combined with clinical decision support systems to improve medication safety: a narrative review. BMJ Qual Saf, 23(9), pp.773-780.

[67] Ash, J.S., Sittig, D.F., Dykstra, R.H., Guappone, K., Carpenter, J.D. and Seshadri, V., 2007. Categorizing the unintended sociotechnical consequences of computerized provider order entry. International journal of medical informatics, 76, pp.S21-S27.

[68] Mozaffar, H., Cresswell, K.M., Williams, R., Bates, D.W. and Sheikh, A., 2017. Exploring the roots of unintended safety threats associated with the introduction of hospital ePrescribing systems and candidate avoidance and/or mitigation strategies: a qualitative study. BMJ Qual Saf, pp.bmjqs-2016.

[69] Thimbleby, H., Lewis, A. and Williams, J., 2015. Making healthcare safer by understanding, designing and buying better IT. Clinical Medicine, 15(3), pp.258-262.

[70] Singh, H. and Sittig, D.F., 2016. Measuring and improving patient safety through health information technology: The Health IT Safety Framework. BMJ Qual Saf, 25(4), pp.226-232.