AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE

March 2017

Literature review and environmental scan on approaches to the review and investigation of Health IT-related patient safety incidents

A/Prof Meredith Makeham, A/Prof Farah Magrabi, Mr Peter Hibbert and Dr Rae-Anne Hardie from the Australian Institute of Health Innovation at Macquarie University have prepared this report on behalf of the Australian Commission on Safety and Quality in Health Care

AUSTRALIAN INSTITUTE
OF HEALTH INNOVATION
Faculty of Medicine and Health Sciences

MACQUARIE
University

Published by the Australian Commission on Safety and Quality in Health Care
Level 5, 255 Elizabeth Street, Sydney NSW 2000

Phone: (02) 9126 3600
Fax: (02) 9126 3613

Email: mail@safetyandquality.gov.au
Website: www.safetyandquality.gov.au

ISBN: 978-1-925224-71-9

The Commission's preference is that you attribute this publication (and any material sourced from it) using the following citation:

> Makeham M, Magrabi F, Hibbert P, Hardie R. Literature review and environmental scan on approaches to the review and investigation of Health-IT related patient safety incidents. Sydney: ACSQHC; 2017

Disclaimer

The content of this document is published in good faith by the Australian Commission on Safety and Quality in Health Care (the Commission) for information purposes. The document is not intended to provide guidance on particular healthcare choices. You should contact your health care provider on particular healthcare choices.

This document includes the views or recommendations of its authors and third parties. Publication of this document by the Commission does not necessarily reflect the views of the Commission, or indicate a commitment to a particular course of action. The Commission does not accept any legal liability for any injury, loss or damage incurred by the use of, or reliance on, this document.

Preface

This preface has been written by the Australian Commission for Safety and Quality in Health Care to provide context and background to the main report that follows. The main report was written by experts from the Australian Institute of Health Innovation (AIHI) at Macquarie University.

Background and purpose

The Australian Commission for Safety and Quality in Health Care (the Commission) was established in 2006 by the Australian Government and state and territory governments to lead and coordinate national improvements in safety and quality in health care. The Commission has four strategic priorities that underpin its functions:

- Patient safety
- Partnering with patients, consumers and communities
- Quality, cost and value
- Supporting health professionals to provide safe and high-quality care.

At a program level, the Commission is also responsible for providing external clinical safety assurance to the national My Health Record system, which allows all Australians the ability to access and share their health information with their healthcare providers.

The literature on the clinical safety of health information technology (HIT) systems is rapidly evolving as these systems roll out across the Australian health system. The Commission requested the AIHI at Macquarie University to perform a literature review and environmental scan to identify appropriate methods for monitoring hazards affecting HIT systems and for investigating incidents resulting from the use of these systems.

The Commission acknowledges the support of the Australian Government Department of Health in the funding of this report.

Overview of findings and recommendations

The review findings are linked to four areas:

- Overview of HIT safety
- Methods for HIT system safety detection and investigation
- Classification of hazards and incidents
- Aggregation of hazards and incident data

Overview of health IT safety

The review finds that the requirements for HIT safety are similar to those that apply to existing patient safety systems. Among these requirements are that these systems should include the ability to detect hazards ahead of time, and should permit review of incidents after the event. They should also provide information about the prevalence of incident reporting and management systems, and allow the opportunity to classify and report on incidents to ensure a continuous open loop of feedback and improvement. Alongside the common themes with existing patient safety systems, the authors note that HIT safety also overlaps traditional IT service management principles. Any successful HIT safety system, therefore, needs to have in place a multidisciplinary team with appropriate skill sets from a clinical, health informatics and systems safety perspective.

Methods for health IT system safety detection and investigation

The authors reviewed methods for HIT system safety detection and incident investigation. Their findings indicate that existing detection methods (such as Failure Mode Effects Analysis, comprehensive system testing and hazard registers) are suitable in these systems. Similarly, existing incident investigation techniques (e.g. Root Cause Analysis, why-because and cause and effect analyses) were found to be suitable for HIT system incident investigations. The authors recommend a pragmatic approach in which more than one approach can be applied. They suggest the nature, context and severity of the incident should determine whether one or many of the approaches be used, and that people investigating incidents should retain the ability to use whichever approaches seem likely to yield insights or a channel through which to provide feedback.

Classification of hazards and incidents

The authors reviewed a number of existing classification systems that can be used to classify HIT incidents. Similar to their findings on the appropriate methods for detection and investigation, the authors found no single classification is suitable in all cases. Instead, they recommend that investigators use an appropriately skilled team of classifiers (with clinical, health informatics and technical expertise) taught a uniform methodology for applying any chosen classification system.

Aggregation of hazards and incident data

The authors reaffirmed the importance of fostering a workplace culture that avoids apportioning blame and instead promotes the reporting of HIT incidents and the provision of feedback to help improve these systems. Over time, the aggregation of regional and national-level HIT incident data will serve to strengthen the resilience of the Australian health sector to known HIT incidents. Ideally, this would be accompanied by a system that allows for safety alerts on known HIT risks to be shared across the sector to prevent issues occurring in the first instance.

Use and limitations of this review

The review outcomes provide objective evidence and guidance on potential methods for consideration by states and territories, private hospital operators and other organisations implementing and using HIT systems.

The review did not examine real-life HIT incidents in HIT systems in Australia. It does not take into account individual HIT system configurations at a national, regional and local level. The findings from the document therefore may be applicable to varying degrees within all HIT contexts in Australia.

Commission response to findings and recommendations

This document is an important contributor to the emerging national conversation on the use and safety of HIT systems. The Commission agrees with the overall message that promotes a pragmatic approach to hazard detection and incident investigation within HIT systems. As the nature and extent of HIT hazards are not yet fully understood and defined, the ability to adopt flexibly the most relevant methodologies and classification mechanisms is valuable.

The Commission will disseminate the findings and recommendations to state and territory governments, the private hospital sector, primary care providers and the medical software

industry. This will support organisations in these areas to refine their approaches to HIT safety, as they continue to implement digital clinical information systems.

Sharing this information will assist the health sector in developing its approach to HIT safety and incident investigation, and contribute to improved patient safety nationally.

AUSTRALIAN INSTITUTE
OF HEALTH INNOVATION
Faculty of Medicine and Health Sciences

MACQUARIE
University

Literature review and environmental scan on approaches to the review and investigation of Health IT-related patient safety incidents

Australian Institute of Health Innovation

Prepared for the Australian Commission on Safety and Quality in Health Care by:

A/Prof Meredith Makeham

A/Prof Farah Magrabi

Mr Peter Hibbert

Dr Rae-Anne Hardie

Australian Institute of Health Innovation

Macquarie University

Australian Institute of Health Innovation
Macquarie University NSW 2109 Australia
T: +61 (2) 9850 2400
aihi.mq.edu.au
CRICOS Provider No 00002J

MACQUARIE University

Table of Contents

Figures

Tables

Boxes

1. Executive summary

Health Information Technology (HIT) safety science is a rapidly developing discipline. There are numerous methods to proactively monitor and predict potential risks and hazards associated with HIT systems, as well as investigate near misses, patient safety incidents and system failures. Many of these methods have arisen from other technology-dependent fields, such as the aviation industry, while others are derived from clinical settings, reflecting the blend of factors that drive the development of HIT systems.

1.1. Purpose and scope

The purpose of this report is to provide a review of the recent literature and undertake an environmental scan to identify any new evidence or developments in methods used in HIT safety science for monitoring hazards and investigating incidents, and to consider current practices internationally that may inform the ongoing process of maintaining safety relating to HIT systems.

The aims of any Health Information Technology (HIT) safety system are to prevent harm that is associated with the HIT from occurring, as well as to allow the earlier detection of potential harm. In addition, should an incident occur, the ultimate aim is to prevent or minimise the chances of its recurrence as far as possible through the process of analysis and modifications to the system.

There are a number of important areas related to the subject of methodologies used in HIT investigations that were not within the scope of the literature review supporting this work, but that are important to be considered in conjunction with the presented findings. The ideal structure and methods underpinning a robust incident reporting and learning system, methods of engaging users and providing feedback and findings, as well as issues concerning the governance of incident investigation and the legal protection of reporters, are examples of related areas requiring further consideration.

1.2. Report structure

This report commences with an overview of the background literature relating to methodologies used in HIT hazard prediction and investigation. Following this are more in depth descriptions from the literature of the major methods found that are relevant to prospective hazard analysis and retrospective incident review (being Root Cause Analysis, the London Protocol, and Failure Mode and Effect Analysis). Then presented are findings from interviews with national and international experts regarding current safety processes for HIT systems. A discussion presents a proposed model to investigate and review HIT incidents, and the conclusion summarises the key findings of this report and discusses the limitations of the work. . The appendices include the interview questions used with international experts and a list of those interviewed.

1.3. Key findings

The key findings of this report are organised within four major themes.

1.3.1. General overview of HIT Safety

Key finding 1.1: The aim of HIT safety systems is to predict hazards and prevent patient safety incidents (PSIs) that are related to the HIT from occurring. They should improve the detection of PSIs and reduce their likelihood of going through to completion and reaching the patient. The ideal is to have a robust safety system that incorporates methods of prospective

hazard detection and retrospective incident review, and strengthens system resilience through improved detection and system defences.

Key finding 1.2: Users of HIT systems require access to incident reporting and learning systems that have the capacity to capture information about near misses, patient safety incidents and system failures, undertake investigations of incidents, classify and aggregate data at a regional and national level, and disseminate findings from lessons learnt.

Key finding 1.3: As HIT safety overlaps the domains of patient safety and IT service management, detection, investigation and review need to be managed by a multidisciplinary team including clinicians and experts with skills in health informatics, IT systems, clinical safety and systems safety engineering. For detailed investigations informatics representation on the investigative team is essential.

1.3.2. Methodologies for HIT system safety detection and investigation

Key Finding 2.1: A variety of methods are used to explore errors across multiple domains in HIT safety. A combination of methods will be required to suit the specific aim relating to the investigation of system safety factors.

Key finding 2.2: Detection of potential hazards in complex HIT systems is best supported by using a range of data sources including automated approaches.

Key finding 2.3: For the prediction of hazards, the main methods described were Failure Mode Effects Analysis (FMEA), Failure Tree Analysis and the incorporation of system testing in simulated environments. This requires a high level of technical expertise within electronic health record (EHR) and clinical information system teams, working alongside clinician users.

Key finding 2.4: Hazard detection should be supported by a well-maintained hazard register. This can then be interrogated when incidents arise, and used to plan system safety improvements.

Key finding 2.5: Incident investigation by its nature requires methods that are retrospective. Many of the methods described for incident investigation are not mutually exclusive, and share many common features across data collection, analysis and interpretation, and the development of recommendations. Methods that were described by experts and in the literature include examples such as Root Cause Analysis, the London Protocol methodology, ‘why-because’ analyses, and ‘cause and effect’ analyses using fishbone diagrams. The choice of method will depend upon a number of factors relating to the severity of the incident and the availability of information, and methods are not mutually exclusive. Leading organisations commonly described using a combination of methods simultaneously.

Key finding 2.6: Sentinel events and incidents with a high potential for harm would ideally undergo in-depth investigations with methods that provide access to detailed information and incorporate consultation with a broad range of stakeholders. Root Cause Analysis and the London Protocol are both appropriately detailed methods for this, and should allow the establishment of a clear timeline of events and the opportunity for those involved in the investigation to be given feedback and consulted regarding the formulation of recommendations.

Key finding 2.7: The composition of an incident investigation team is a key factor in the success of conducting an investigation. An understanding of the technical aspects and complexity of the system, as well as understandings of the clinical context of an incident, are essential to include on an investigating team.

Key finding 2.8: The appropriate method of HIT incident investigation will depend upon the context of the incident, including the clinical setting (such as primary care or hospital), type of clinician or system user reporting or involved, and the existence of existing processes for incident investigation.

1.3.3. Classification of hazards and incidents

Key finding 3.1: Classification of hazards and incidents is important for numerous reasons. It allows the systematised reviews of issues required to generate feedback and recommendations regarding recurrent incidents. It allows an understanding of the nature and frequency of incidents and their contributing factors, which is important to direct resources appropriately in the development of mitigating strategies and solutions.

Key finding 3.2: A number of classification systems exist that are applicable to HIT incident classification. Described in the literature was the Magrabi *et al.* classification system, Sittig and Singh's Sociotechnical dimensions associated with IT incidents, and the WHO International Classification for Patient Safety.

Key finding 3.3: The classification of hazards and incidents is a specialised process, and teams responsible for this should include people with HIT technical expertise and clinicians familiar with the HIT system about which an incident is being categorised. These teams should be taught a standard method for the chosen classification system and care should be taken to maintain the integrity of the classification process, such as maintaining inter-coder reliability.

1.3.4. Aggregation of hazards and incident data: reporting and learning structures at the local, regional and national level

Key finding 4.1: Incident reporting systems are more successful when reporters are engaged and involved at a local level with a strong, non-punitive reporting culture, and participate in the generation of solutions and feedback of findings. This has been found in the literature on general patient safety incident reporting and learning, and is likely to be applicable to the HIT context.

Key finding 4.2: Regional (at the level of local health district or primary health network boundaries) and national level aggregation of incident data is fundamental to gaining a broad perspective of recurrent issues that may be occurring in several locations simultaneously, and gain a clearer understanding of the impact of a detected issue. It also allows greater power for searching collections of incidents and hazards for their use in trend analysis, and in detecting and resolving problems.

Key finding 4.3: In order to prevent incidents from happening, a register of identified potential hazards should be maintained and communicated with relevant stakeholders who can then ensure that mitigation strategies are in place, and that there is a high level of 'alert' for known potential risks.

Key finding 4.4: Dissemination of learning and feedback to reporters of incidents is an important principle in general patient safety incident analysis. As well as aiming to prevent the recurrence of incidents, it engages reporters and rewards their efforts to report problems.

1.4. Conclusion

Numerous methods exist that may be used in combination to investigate system safety and. There is no one method that will fit all of the requirements across the spectrum of proactive monitoring, retrospective analysis, aggregation of data, and development and dissemination of key findings. Each component of any safety system requires a tailored approach and should draw from a palette of multiple methods.

2. Introduction

Health Information Technology (HIT) safety science is a rapidly developing discipline, and there are numerous methods that exist both to proactively monitor and predict potential risks and hazards associated with HIT systems, and to investigate near misses, patient safety incidents and system failures. Many of these methods have arisen from other technology-dependent fields, such as the aviation industry (2), while others are derived from clinical settings, reflecting the blend of factors that drive the development of HIT systems.

The purpose of this report is to provide a review of the recent literature and undertake an environmental scan to identify any new evidence or developments in methods used in HIT safety science and to consider current practices internationally that may inform the ongoing process of maintaining safety relating to HIT systems.

The structure of this report commences with an Executive Summary, followed by an overview of the recent literature with respect to methodologies used in HIT investigation. After this are more in-depth descriptions from the literature of the major methods found that are relevant to prospective hazard analysis and retrospective incident review (being Root Cause Analysis, the London Protocol, and Failure Mode and Effect Analysis). The findings from interviews with national and international experts regarding current HIT safety processes in their various organisations are then described. A discussion section presents an overview of the literature and interview findings and presents a proposed model to investigate and review HIT incidents. The conclusion summarises the key findings of this report. The appendices include the interview questions used with international experts and a list of those interviewed.

3. Literature review of methods to investigate HIT incidents

3.1. Background

The investigation of Health Information Technology (HIT) incidents is an emerging specialty. The literature describing this subject should be considered as a special topic within more general patient safety literature on incidents occurring in the health sector more broadly.(3) Furthermore, this general patient safety literature in many respects is itself a subset of the literature describing general safety investigation methods across all settings, with many examples originating in other fields such as aviation and nuclear industries.(4) In any of these contexts, many of the methods described for incident investigation are not mutually exclusive, and share many common features across data collection, analysis and interpretation, and the development of recommendations.

The literature describing general safety investigation methods that might be applicable to all industries is very broad, with numerous examples of different methods of accident analysis and accident modelling approaches. Many of these provide useful theoretical frameworks to consider a systematic approach to the investigation of an incident of some kind. Examples include 'AcciMaps' (accident analysis methodology using a graphical representation) and Risk Management Frameworks (a more general modelling framework for describing accidents) (5); Causal Analysis Based on Systems Theory (CAST, a systems theoretic analysis technique that can aid in identifying causal factors) (6); and Why-Because Analyses (a technique for causally analysing behaviours of complex technical and sociotechnical systems).(7)

A recent review of general safety accident modelling approaches for complex sociotechnical systems provides an overview of many of these accident-modelling approaches, including more traditional as well as newer system-theoretic approaches. Examples of the latter include Cognitive Systems Engineering Approach (models behaviours of human-machine systems in the context of the environment in which the work takes place); Rasmussen's Sociotechnical Framework (takes into account environmental influences such as market competition and economic or political pressures); and STAMP (Systems-Theoretic Accident Model and Processes whereby accidents are related to inadequate control or enforcement of safety-related constraints on the design of the system).(8) The use of 'Safety Cases' is another general safety approach from other industries that has been suggested as a framework for investigating health safety incidents (9), although these have been criticised as using a "tick box" and compliance-driven approach which may be associated with poor safety management and standards.(10)

For mainstream patient safety incidents, there are a variety of methods depending on the type of investigation. For example, in the Victorian Health Incident Management System, there are three types of investigation (Figure 1). The severity of incidents is rated on a scale of one to four: Root Cause Analysis (RCA) is used for sentinel and level 1 incidents; the in-depth case review methodology is used for level 2 incidents; and local investigation and aggregate review is used for level 3 and level 4 incidents.

Similarly, there are multiple types of investigation for HIT incidents incorporating detailed methods such as RCA and the London Protocol.(11) The scope of the literature review included in this chapter is limited to the published and grey literature about investigations of HIT incidents; however, it is important to consider these within the context of the broader patient safety and general safety literature.

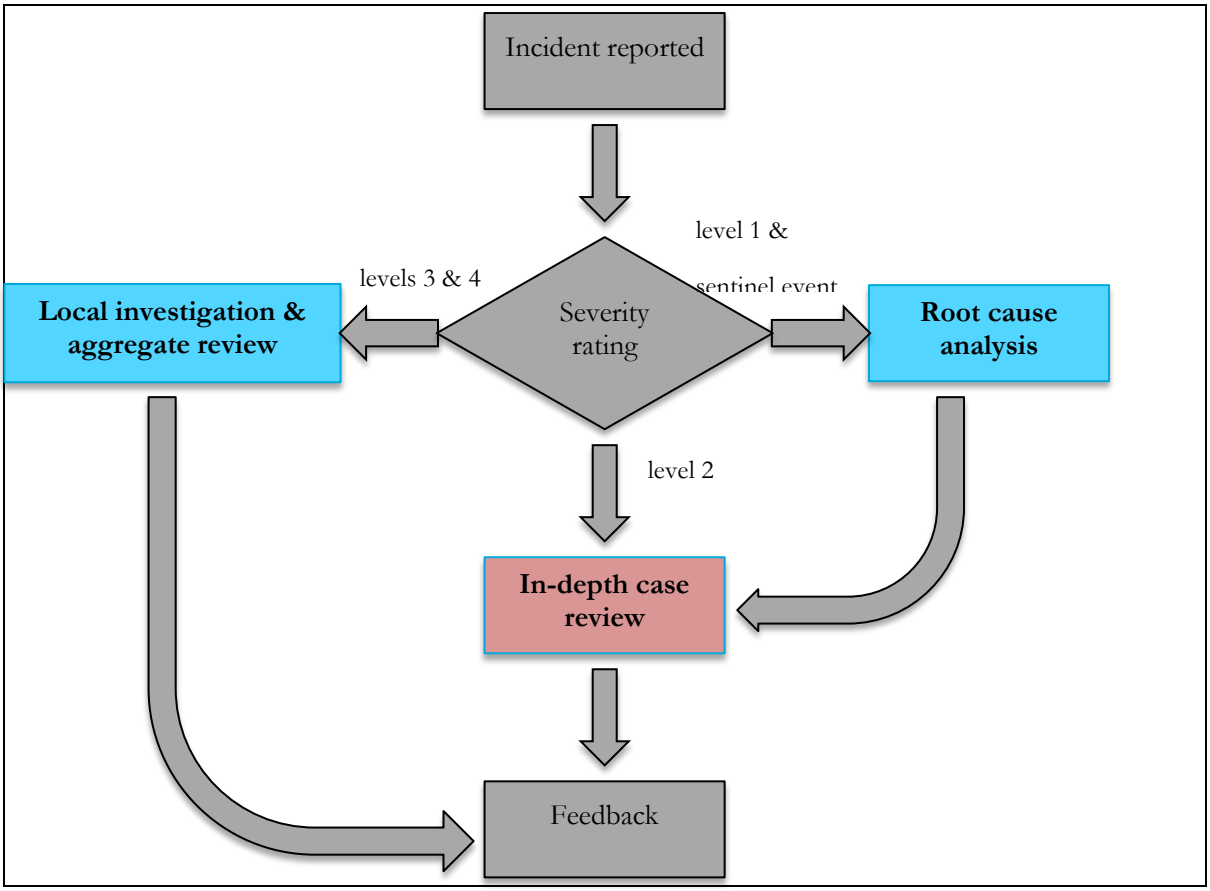


Figure 1. Methods depend on the types of investigation. There are three levels of investigation for clinical safety incidents in the Victorian Health Incident Management System.(12)

3.2. Literature review methods

The published and grey literature about current HIT methods of incident investigation was reviewed. Bibliographic databases including Scopus, PubMed and Science Citation Index Expanded from January 2004 to May 2016 were searched. Only English language case studies and analyses of HIT incidents were included. After titular and abstract review, papers were selected for full review. Grey literature was identified by searching the websites of international patient safety agencies and programs such as the US Agency for Healthcare Research and Quality. A narrative synthesis was used to integrate findings into descriptive summaries. Relevant frameworks for studying the safety of HIT were also examined.

3.3. Findings: Descriptive analysis of all investigations

Our search identified 21 investigations of HIT incidents (Appendix A: Summary of the 21 studies investigating HIT incidents). Most of these were aggregate reviews of incidents from a broad range of clinical settings in six countries including the USA, UK, the Netherlands, China, Hong Kong and Australia (86%, n=18). About half (n=10, 48%) involved a range of HIT systems, 33% (n=7) were focused on medication management systems and one related to radiology information systems. Of the 21 investigations, three were in-depth reviews from inpatient settings in the USA. Of these, two related to medications management systems including order entry and bar-coding (13,14) and the other involved an image viewer to track patients in an Emergency Department.(15)

Sixteen investigations examined patient outcomes (76%). In 15 of these, there were reports of patient harm and one case study related to a near-miss event (Appendix A: Summary of the 21 studies investigating HIT incidents). In the 13 investigations reporting the number of patient deaths, HIT incidents resulted in the death of 83 patients, with 66 of these coming from the sentinel events investigated by the US Joint Commission. In incidents reported to the US FDA and from across England's National Health Service (NHS), human factors issues were over-represented in the events involving patient harm.(16,17)

Two investigations reported the potential of HIT incidents to lead to large-scale adverse events, meaning that multiple individuals were affected.(18) In one, 23% of safety events (n=850) affected more than ten individuals across England.(17) In the second, 36% of system downtimes (n=116) in China were estimated to affect more than one hundred individuals.(19)

3.4. Detailed investigations

In-depth investigations seek to untangle the interaction of errors across multiple domains that cumulatively produce an adverse event. The two medications-related cases we reviewed used a series of techniques to examine a serious dosing error and a near miss.(13,15) Safety reviews were combined with semi-structured interviews and examination of HIT systems including usability inspection of the computer interface and reconstruction of the error in the system (Box 1). For example, Horsky *et al.* reconstructed 16 orders by two clinicians over two days where an elderly patient suffering from hypokalaemia (low potassium levels) became severely hyperkalaemic (high potassium levels).(13) Wrong, incomplete and missing information in the hospital order entry system resulted in the patient receiving multiple doses of potassium over a 42-hour period which caused the hyperkalaemia.

Box 1. Methods used to undertake detailed investigations.

1. Medical case history
2. Case & review notes by Significant Events Committee
3. Root-cause analyses
4. Quality assurance reports
5. Interviews with involved patients and clinicians
6. Computer log analysis
7. Usability inspection of computer interface

3.5. Aggregate reviews

Analyses of incidents are used to understand the nature of problems with IT that can pose risks to patient safety. Incidents are generally reviewed against existing classifications to identify common types of problems found with the design, build and use of HIT. The consequences of incidents, particularly their potential to lead to large-scale adverse events as well as effects on care delivery and patient safety are also considered.(18)

3.5.1. Information sources

Our examination of the 18 aggregate reviews revealed a range of information sources (Table 1). These reviews include dedicated programs for HIT safety in England's NHS and the US Department of Veterans Affairs. Another US review was a one-off analysis of a national sample of HIT incidents (called a Deep Dive™) by the ECRI Institute, a patient safety organisation based in the USA.(20) We also included the TechWatch study of HIT incidents in Australian general practice.(21) The majority of the reviews (78%, n=14) were about HIT incidents identified from existing sources of information about patient safety problems, including sentinel events associated with HIT, patient safety incident monitoring, equipment failure and hazards, adverse drug reactions, medico-legal investigations and the grey literature adverse drug reactions.

Table 1. Aggregate reviews drew on a range of information sources to examine incidents including dedicated HIT safety programs.

Study Source	Number of studies	% of studies
Dedicated HIT safety programs	2	11
National HIT service desk (17)	1	
Investigations of HIT safety issues (22)	1	
HIT incident reporting studies	2	11
ECRI Deep Dive (20)	1	
TechWatch study (21)	1	
Sentinel HIT events to The Joint Commission (23)	1	6
Patient safety incident reporting	5	28
National system (24)	1	
State-based systems (PA-PSRS, AIMS) (25, 26)	2	
Hospital-based systems	2	
Equipment failure & hazards reported to the FDA (16, 27)	2	11
Medications reporting	4	22
US Pharmacopeia, MEDMARX (28-30)	3	
Dutch central medication incidents registration (CMR) (31)	1	
Malpractice claims (32)	1	6
Online news articles and incident reports (19)	1	6
TOTAL	18	

3.5.2. Problems with IT

Classification systems have been developed to understand the underlying types of problems with HIT that pose risks to patients. An overview of the classifications used to examine HIT problems is given in Appendix B: Summary of classifications used to examine problems with HIT.

The Magrabi *et al.* classification system was used in 56% (n=10) of the investigations we reviewed and takes a bottom-up approach based on the natural categories of problems described in incident reports.(16,17,26,33) In this system, incidents are firstly subdivided as primarily relating to human factors or technical issues (Figure 2). For incidents primarily

involving human factors, the type of use error and contributing factors such as training, cognitive load and clinical workflow are then identified. For incidents falling into the technical space, the type of machine error and technical problems including a range of hardware and software issues are examined.

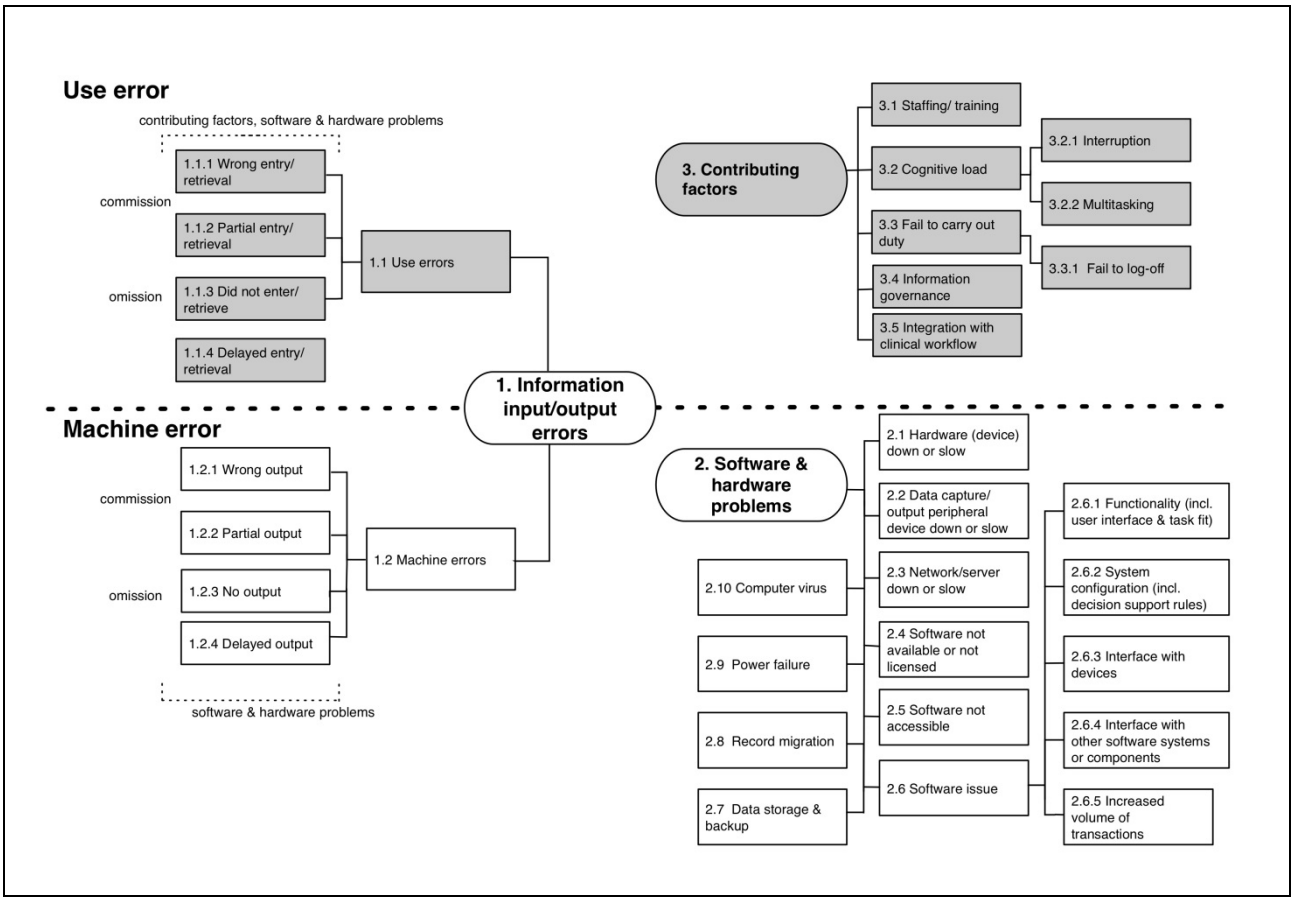


Figure 2. A classification of human and technical problems that contribute to HIT incidents.(17)

Another approach to classification of HIT problems is *Sittig and Singh's Sociotechnical Model* (34). This approach takes a top-down approach grouping problems into eight broad dimensions including hardware and software; clinical content, human-computer interaction; people; workflow and communication; organisational policies and procedures; external rules, regulations, and pressures; and system measurement and monitoring (Table 2).(22) Problems can also be grouped by the phases of HIT implementation.(35) An “initial” phase is characterised by immature technology where problems primarily relate to technical factors. The second phase is where use errors start to emerge whilst a final phase is where problems primarily relate to the lack of monitoring of safety concerns.

We found that some reviews were undertaken from a general patient safety perspective. For example, Stewart *et al.* used the *WHO International Classification for Patient Safety (ICPS)* to examine radiology incidents reported in a hospital.(36,37) The ICPS includes 10 high-level classes:

1. Incident Type
2. Patient Outcomes
3. Patient Characteristics

4. Incident Characteristics
5. Contributing Factors/Hazards
6. Organizational Outcomes
7. Detection
8. Mitigating Factors
9. Ameliorating Actions
10. Actions Taken to Reduce Risk

It aims to represent a continuous learning and improvement cycle emphasising identification of risk, prevention, detection, reduction of risk, incident recovery and system resilience. All of these occur throughout and at any point within the conceptual framework.

Table 2. Sociotechnical dimensions associated with HIT incidents.(38)

Sociotechnical dimension	Explanation
Hardware and software	Computing infrastructure used to support and operate clinical applications and devices
Clinical content	The text, numeric data and images that constitute the 'language' of clinical applications, including clinical decision support
Human–computer interface	All aspects of technology that users can see, touch or hear as they interact with it
People	Everyone who is involved with patient care and/or interacts in some way with healthcare delivery (including technology). This would include patients, clinicians and other healthcare personnel, IT developers and other IT personnel, informaticians
Workflow and communication	Processes to ensure that patient care is carried out effectively, efficiently and safely
Internal organisational features	Policies, procedures, the physical work environment and the organisational culture that govern how the system is configured, who uses it and where and how it is used
External rules and regulations	Federal or state rules (e.g. CMS's Physician Quality Reporting Initiative, HIPAA and Meaningful Use programme) and billing requirements that facilitate or constrain the other dimensions
Measurement and monitoring	Evaluating both intended and unintended consequences through a variety of prospective and retrospective, quantitative and qualitative methods
HIPAA, Health Insurance Portability and Accountability Act of 1996; IT, information technology.	

To enhance the detection of HIT problems the US Agency for Healthcare Research and Quality (AHRQ) has included categories for HIT in its new standard for reporting hazardous events called the "common format".(39) The AHRQ has also developed and tested a comprehensive software tool to support detection and management of hazards throughout the HIT life cycle.(40) The Health IT Hazard Manager facilitates the characterisation and communication of hazards along with their actual and potential adverse effects to support learning within healthcare organisations, across organisations using the same software and by vendors and policymakers.(41) It contains a proprietary classification system and was tested by seven organisations to examine 495 safety issues. The Hazard Manager and common formats were used in only one of the investigations examined. In this study, Castro *et al.* combined these tools with the Magrabi *et al.* classification and Sittig and Singh's

Sociotechnical Model to undertake an aggregate review of 120 sentinel events reported to the US Joint Commission.(23)

A third approach to review incidents was from an IT service management perspective. Lei *et al.* (19) used the *Synthesized IT Risk Model* to examine hardware, software and loss of network connectivity during computer system downtimes affecting health organizations in China (Appendix B: Summary of classifications used to examine problems with HIT).

3.5.3. Consequences of incidents

The majority of investigations reported the consequences of incidents assigned by reporters using local schemas. For example, investigations using the US Pharmacopeia, MEDMARX database used the National Coordinating Council for Medication Error Reporting and Prevention's (NCC MERP) Index for Categorizing Medication Errors (28-30). In Australia, studies of state and hospital-based incident monitoring systems used the Advanced Incident Management System (AIMS) event types and the Severity Assessment Code (SAC) (26). UK studies used the National Reporting and Learning System (NRLS) harm categories.(24) In the analysis of safety events from England's NHS, degree of harm was assessed using the UK national levels (low, moderate, severe, death) (42) in consultation with clinical experts. Other schemas include the 15 categories of sentinel event types.

Only three investigations sought to identify consequences using free text descriptions of incidents.(16,17,21) These were assigned using the AIMS event types into:

a) *Potential or actual harm to a patient*: an HIT problem led to a clinical error that reached the patient (36), an example being a patient had severe allergic reaction to prescribed medication.

b) *An arrested or interrupted sequence or a near miss*: an HIT problem led to a clinical error that was detected before reaching the patient (17,36), such as a prescription in a wrong name noticed and corrected while printing.

c) *An IT problem with a noticeable consequence but no patient harm*: a problem that affected care delivery but caused no harm to a patient, the delays in care delivery and necessary reworks were examined. An example is that computer network problems resulted in a delay in care delivery because additional phone calls were required to follow up missing test results.

d) *An IT problem with no noticeable consequence*: problems that did not directly affect the delivery of care. For example, an electronic backup copy of a patient record was corrupted, but this was detected and the copy was not needed.

e) *A hazardous event or circumstance*: problems that could potentially lead to an adverse event or a near miss such as prescribing software failing to display a patient's allergy status.

3.5.4. Large-scale effects

The study of safety events from England's NHS classified events as large-scale if they affected:

a) Ten or more HIT system users, patients or their records at one or more sites such as medical practices, hospitals or trusts

b) Multiple components or HIT systems such as all the computers at a site, one or more servers, or the whole computer network.

3.5.5. Clinical processes impacted

Some studies sought to examine clinical processes impacted by HIT incidents. In the TechWatch study, clinical processes were examined using categories from the Threats to Australian Patient Safety study (practice systems, investigations, medications, non-medication treatments and communication).(43) To analyse medication incidents, Cheung *et al.* (31) examined phases of the medication process in combination with the Magrabi *et al.* classification.(21) These included prescribing, transcription, entry of prescriptions into pharmacy system, compounding, dispensing, administration, patient monitoring, storage and logistics).

3.5.6. Delays and rework

Disruptions to clinical work were also examined. In one study, free-text incident descriptions were used to assess the direct consequences of incidents on clinical processes such as delay and rework.(26)

3.5.7. Clinical errors

The TechWatch study examined clinical errors arising from HIT problems based on their underlying mechanisms; a clinical error is an error (flawed plan or flawed execution of a plan) with actual or potential consequences for a patient.(44) Actual and potential clinical errors were categorised into:

a) *Errors that were unique to IT*: a clinical error caused by an HIT problem, for example, a prescribing error due to a drop-down menu, system downtimes.

b) *Errors that existed with paper records but were made more likely with IT*, for example, ordering medications for the wrong patient when interrupted.

c) *Errors that had always occurred but were more likely to cause harm with IT*, for example, a GP relies on the medication list in a discharge summary which does not match a specialist's notes but is more easily accessible in an electronic system.

d) *Errors that were no different with use of IT or paper records*, for example, a failure to use the latest protocol or guideline.

3.6. Safety frameworks

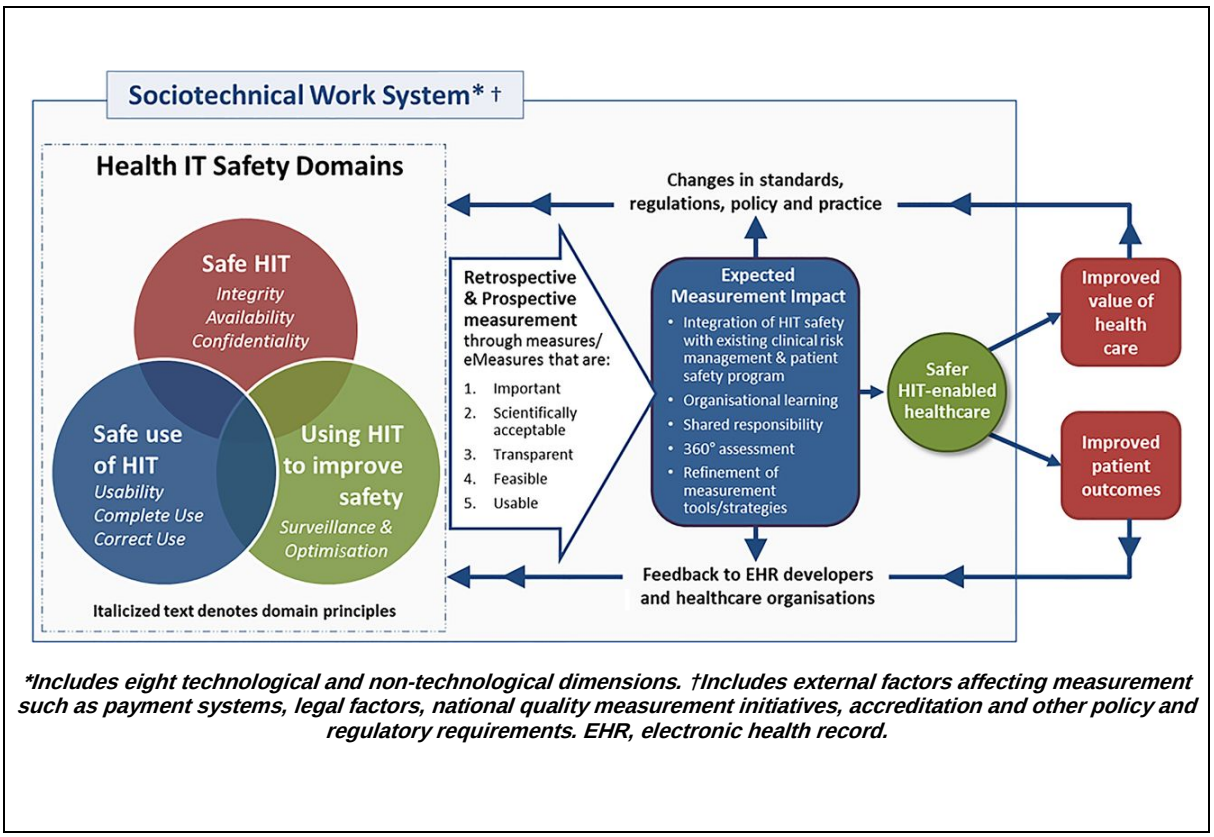
There are many frameworks for the safety of HIT. We examined two of these which are particularly relevant to the investigation and review of HIT incidents.

3.6.1. The Health IT Safety (HITS) Measurement Framework

The Health IT Safety (HITS) Measurement Framework provides a conceptual foundation for HIT-related patient safety measurement, monitoring, and improvement.(45) The HITS framework, summarised in Figure 3, follows both Continuous Quality Improvement and sociotechnical approaches and calls for new measures and measurement activities to address safety concerns in three related domains: 1) concerns that are unique and specific to technology such as addressing unsafe HIT related to unavailable or malfunctioning hardware or software; 2) concerns created by the failure to use HIT appropriately or by misuse of HIT, for example reducing nuisance alerts in the electronic health record (EHR), and 3) the use of HIT to monitor risks, health care processes and outcomes and identify

potential safety concerns before they can harm patients, an example being using EHR-based algorithms to identify patients at risk for medication errors or care delays.

The framework proposes to integrate both retrospective and prospective measurement of HIT safety with an organization's existing clinical risk management and safety programs. It aims to facilitate organisational learning, comprehensive 360-degree assessment of HIT safety that includes vendor involvement, refinement of measurement tools and strategies, and shared responsibility to identify problems and implement solutions. Additions to the model below have been considered in other literature, such as the three-phase development process from The SAFER Guides: 1) Address safety concerns unique to EHR technology (data availability, integrity and confidentiality), 2) Optimise the safe use of EHRs (through complete/correct EHR use and EHR system usability), and 3) Use EHRs to monitor and improve patient safety (safety surveillance, optimisation and reporting.(46) A long-term framework goal is to enable rigorous measurement that helps achieve the safety benefits of HIT in real-world clinical settings.



**Includes eight technological and non-technological dimensions. †Includes external factors affecting measurement such as payment systems, legal factors, national quality measurement initiatives, accreditation and other policy and regulatory requirements. EHR, electronic health record.*

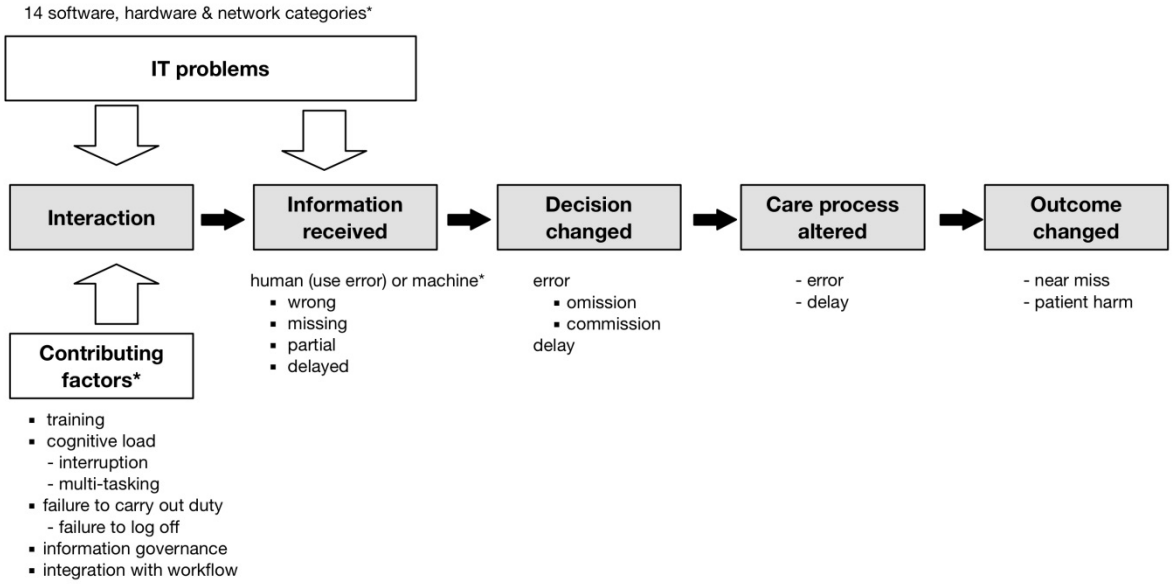
Figure 3. Health Information Technology Safety Measurement Framework (HITS Framework).

3.6.2. The Information value chain

Another framework is the information value chain which connects the use of a technology to the final outcome. It can be used to examine the effects of HIT problems on care delivery and patient outcomes (Figure 4).(47) The chain is initiated when a user interacts with an HIT system. A subset of these interactions will yield new information; only some will lead to changed decisions, and only some decisions will see changes in the care process. Similarly, only a subset of process changes may have an impact on patient outcome. Using this framework the effects of HIT problems on user interaction, errors and delays in information received as well as sociotechnical contextual variables that influenced user interaction (contributing factors) can be unpacked. The resulting effects on decision-making, care processes and patient outcomes can also be considered.

HIT problems, user interaction, errors in information received, decision-making, care processes, outcomes and sociotechnical contextual variables (contributing factors) can be categorised using the Magrabi *et al.* classification (17). The schema can be used to trace errors in information received arising from the use of software (use errors) as well as machine errors, which cover problems in the design of software and hardware. Four types of errors in information (information errors) can be considered: wrong, missing, partial and delayed.(47)

Errors and delays in decision-making can be similarly identified including *omission errors,* such as when an intended action was not executed, and *commission errors,* such as when an action was wrong. Observable impact on care process and outcomes can be examined using a standard approach, (16, 17, 26, 36) as discussed in 3.6.1.



**The Magrabi et al. classification can be used to categorise HIT problems, errors in information received and contributing factors (17).*

Figure 4. The information value chain connects use of a technology to final outcome (highlighted in grey).(47) It can be used to examine the effects of HIT problems on user interaction, information received as well as effects on decision-making, care process and patient outcomes.

3.7. Chapter summary

Our review found that the available literature is small. While HIT may have been previously identified amongst other safety problems, the first analysis specifically focused on HIT risks was published in 2010. We found that existing repositories of patient safety problems are a rich source of incidents for aggregate reviews. While aggregate reviews covered a range of health settings, the detailed investigations of HIT-related adverse events examined here were limited to hospital settings. Incidents involving consumer HIT were not specifically covered in any of the studies we reviewed.

The Magrabi *et al.* classification is the only schema that has been validated for national-scale systems and general practice. Most recently, it was used in a systematic review of the literature including 34 studies (2004-2015); no new categories were required to code the HIT problems, information errors and contributing factors, further validating the classification.(48) Regardless of the specific approach, aggregate reviews allow problems with HIT to be

collated and classified, providing an objective basis for comparing patterns over time and between settings, and for the development and prioritisation of preventive and corrective strategies.(44) In summary:

- Detailed investigations use a variety of different methods to untangle the interaction of errors across multiple domains that cumulatively lead to an adverse event. Investigations of HIT-related adverse events use computer logs and usability inspections in addition to other methods that are traditionally used in patient safety.
- Aggregate reviews are used to understand the nature of problems with HIT that can pose risks to patient safety. Incidents are generally reviewed against existing classifications to identify common types of problems found with the design, build and use of HIT. Exemplar classifications are the AHRQ Hazard Manager Ontology, the Magrabi *et al.* classification and Sittig and Singh's sociotechnical model.
- Severity assessment is generally based on local schemas. The scale and scope of HIT incidents including their potential to lead to large-scale adverse events also needs to be considered.
- Existing patient safety initiatives are a rich source of information about HIT risks; for example, sentinel events, patient safety incident monitoring, databases of equipment failure and hazards, adverse drug reactions and medico-legal investigations.

4. Root cause analysis

Root Cause Analysis (RCA) is a systematic process that attempts to answer three questions about something that has gone wrong (an incident):

- What happened?
- Why did it happen?
- How can we prevent it happening again?

RCA uses small teams, comprising of a diverse set of individuals, who are independent of the incident. In health care, they are often commissioned under jurisdictional policies or legislations using tools such as Severity Assessment Codes, which attempt to describe and rank severity and frequency of incidents.

There is a broad consensus that RCA represents a toolbox of approaches rather than a single method. More than 40 RCA techniques are described, including brainstorming, cause-effect charts, “five whys” diagrams and fault trees.(49-51) However, regardless of these variations, RCAs are organised in sequential steps (Figure 5) designed to answer the three questions above.

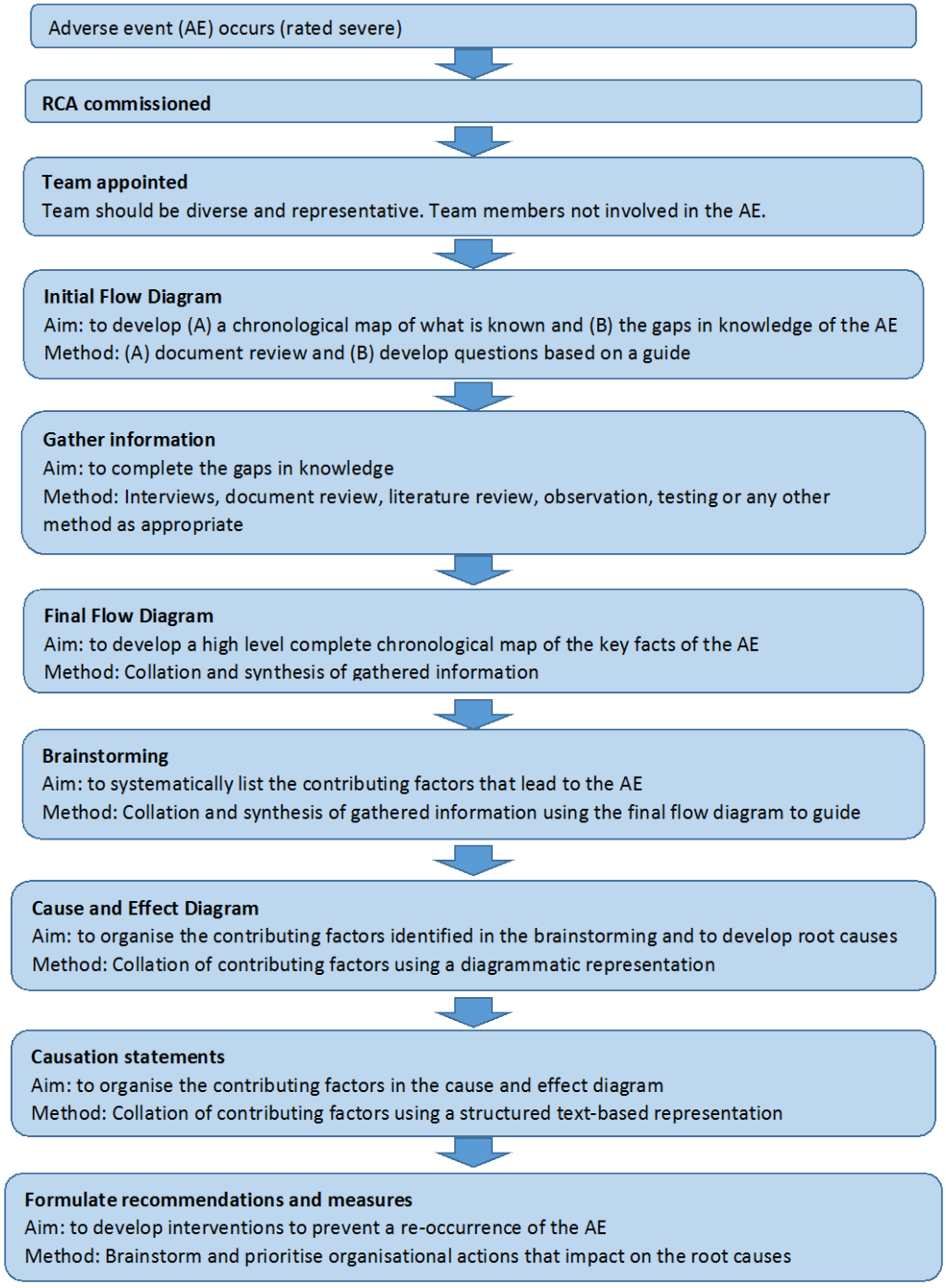


Figure 5. Sequential steps of Root Cause Analysis (RCA).(50,52,53)

In the literature scan that was undertaken, there were no papers that specifically described RCA as applied to e-health. However, there are many lessons from health that can be applied to the e-health sector, both in terms of challenges with, and potential ways to strengthen the method. These are outlined below using the RCA steps as a way of structuring this information with general findings discussed first. A summary of the key challenges as described by Nicolini *et al.* is also presented in Box 2.(50)

Box 2. The challenges of conducting Root Cause Analysis (RCA).(50)

Forming the investigation team and gathering evidence Determining team constitution and terms of reference Securing participation of clinical and non-clinical representatives Scheduling team meetings
Obtaining statements and good quality of information Conducting the analysis and identifying root causes Organizing the multidisciplinary meeting Ensuring equal and fair participation of participants
Applying tools and analytical approaches Avoid analytical myopia and discounting 'deep' root causes factors
Formulating and implementing service improvements Avoid giving undue attention to the report Managing the change process Competing with other change agendas and initiatives

4.1. General findings

The main general issues found with RCA were organisational expectations and culture, time to complete, standardisation, and lack of aggregation of data.

4.1.1. Organisational expectations and culture and time to complete

Hospitals may focus on "who" did "what", rather than on "why" the error occurred – this facilitates a culture of blame wherein the health care provider is formally or informally punished rather than identifying the impact of the system-based causal factors on performance.(54) The investigation's inputs and outputs may be heavily affected by professional, disciplinary and departmental politics and are thus far from independent.(49,55)

In most jurisdictions, there are mandatory time constraints for completing the RCA. Whilst these may be necessary, they may also limit the quality of recommendations by the RCA team and the ability to design and implement robust system improvements.(56,57) In some jurisdictions, there is a stronger organisational expectation with meeting the timeframe rather than on conducting a robust analysis.(52,57-59)

RCAs are a significant investment and organisations should expect a certain return on investment (ROI), just as other activities are expected to achieve.(60) It should be possible to measure the effectiveness of RCA against performance on an organisation's enterprise

risk management (ERM) strategy at the corporate level. Indeed, RCAs should be considered to reduce any significant performance gaps.(60)

Use of metrics to measure the effectiveness and sustainability of the RCA process has been advocated by two papers.(53,60) The metrics in Box 3 are examples from these papers.

Box 3. Root Cause Analysis metrics examples

Percentage of RCAs conducted based on reactive triggers, versus RCAs targeting chronic issues (from OA and FMEA types of analyses).

Percentage of reactive RCAs commenced within one week or less of the incident occurrence (ensuring that proper data collection takes place before the evidence is no longer available).

Percentage of trained/qualified RCA facilitators actively conducting RCA investigations.

Number of RCAs performed per year per facilitator.

Percent of contributing factors written to meet the Five Rules of Causation.

Percent of RCA reviews with at least one stronger or intermediate strength action.

Percent of actions that are classified as stronger or intermediate strength.

Percent of actions that are implemented on time.

Percent of actions completed.

Audits or other checks that independently verify that hazard mitigation has been sustained over time.

Staff and patient satisfaction with the RCA2 review process (survey).

Percent of RCA results presented to the board.

Percentage of RCA recommendations that were applied across the organisation.

Percentage of RCA recommendations that were made in previous RCAs.

Percentage of root causes identified in previously completed RCAs.

Number and percentage of repeat RCAs conducted.

4.1.2. Standardisation

The issues identified around standardisation were:

- The RCA process is neither standardised nor reliable between organisations, which leads to personal agendas and inconsistent identification of systematic errors.(54)
- A standardised nomenclature does not exist to allow analysis of recurring errors across an organisation.(54)
- Although multiple tools exist to help raise the quality of RCAs and facilitate aggregation, these are underused.(58)
- These points collectively mean that the quality of RCAs is highly variable.(57)

4.1.3. Lack of aggregation of data

RCAs typically are conducted independently and each root cause of the incident is addressed with its own unique corrective action plan, which may prove inadequate or have unintended adverse consequences. There often is also no attempt to aggregate the root causes and identify trends that could be addressed through culture change or performance improvement methods.(54,58)

Individual RCA reports can be reviewed to systematically analyse trends, drawing out common issues and recurrent causal factors from across incidents.(49,50,58,60) This enables prioritisation and resources to be directed to the areas of greatest need. One way to achieve this is to form cross-departmental standing groups around patterns of (causes of) incidents (that is, communication problems between shifts, falls and infection control), which would support local learning activities and system-level interventions.(49,50) Applying RCA proactively, on unacceptable risks, near misses, and chronic failures that do not rise to the level of identified triggers, is advocated.(60)

A related activity would be for organisations to design and create a knowledge-management infrastructure that would store successful RCA logic. They should make this RCA database readily available to those in the organisation who may be in a position to make similar decisions in the future.(60)

Related to this, but pitched at a different level, a national oversight body to ensure best practices for conducting investigations, instigate high-level discussions and negotiations, and track results to ensure that clinicians and health care organisations learn from errors and incidents, is advocated.(58) Part of their role could be placing more emphasis on understanding variations in the implementation of RCA and developing a greater evidence base for the best way to conduct them.(58,60) Applying RCA in a uniform and standardised manner that requires appropriate breadth and depth of analysis (and developing tools to facilitate this) should be an end goal for an oversight body.

4.2. Commissioning the RCA

The motivating factors for initiating an RCA are often to satisfy external regulatory requirements.(52,60) This means that incidents that have caused the most harm are prioritised for analysis, even though more valuable insights may be derived from close calls.(52) Given that RCAs are retrospective, they are commissioned only after a defined incident has occurred. Therefore, an RCA is used as a reactive tool responding to bad outcomes after the fact (60); it may take away resources from proactive management of known problems.(54,58)

An RCA should be undertaken on those incidents that can demonstrate ROIs correlated to Key Performance Indicators (KPIs). These may include on unacceptable risks, near misses, and chronic failures that do not rise to the level of triggers on tools such as Severity Assessment Codes.(60) Tools such as Failure Modes and Effects Analysis (FMEA) and Opportunity Analysis (OA) may be able to assist:

- The key risks in FMEA (severity × probability x detectability) can be used as a prioritisation tool. Often, a “Pareto Split” will apply, where 20% of potential incidents will reflect 80% of the total risk. This 20% of the incidents is referred to as “the significant few” and these can be candidates for RCA.(60)
- Opportunity analysis (OA) is an historical data tool that attempts to uncover the hidden value of chronic failures. This tool typically defines what a “failure” is in a given system and then seeks to identify what failures have occurred in that system that has met that failure definition. The tools attempts to take into account how often small failures occur and extrapolate their seemingly small cost/occurrence to large annual costs when looking at the organisation’s big picture.(60)

4.3. Forming a team

The main problems identified with forming a team include recruiting participants, lack of team knowledge, cognitive biases, interpersonal problems, and lack of management support. Other issues include keeping the team focused, organising the first meeting (52) and funding of team members’ time.(61)

4.3.1. Recruiting participants

Ensuring participation of the most appropriate individuals is a consistent finding. People who are senior in the clinical area where the incident occurred may be difficult to recruit and bring together. This often can delay proceedings and create frustration among the rest of the RCA team, especially if there are timelines to maintain.(49,50,57)

4.3.2. Lack of team knowledge

As RCA teams are often made up of healthcare providers, they may not have the expertise to develop effective interventions as they are generally not trained in the principles of safety engineering.(49,50,56,59,62,63) Roles such as human factors engineering, medical device manufacturing and organisational psychology/sociology are often not represented. Thus, there is a risk of coming to premature conclusions regarding the root cause when the first “obvious” cause is found (61) and interventions may be superficial, an example is informing or re-educating staff with little chance of permanently reducing the risk of a recurrent incident.(52,56,57) Formulating good recommendations can be learnt, but this takes time.(52)

4.3.3. Cognitive biases

Hindsight bias, biased perspectives, and pre-existing agendas can all influence team members’ actions and outcomes(52,61) RCA team members may come to the RCA with preconceived ideas and they may, unintentionally or otherwise, align the outcomes with “prior opinions and powerful audiences”.(63,64)

4.3.4. Interpersonal problems

Difficulty with teams including uncooperative colleagues, hierarchical tensions, and inter-professional differences can all influence RCA actions and outcomes.(49,50,52,58,59,61) A

lack of strong leadership within the team can also mean that personal agendas and biases influence findings and recommendations.(61)

4.3.5. Lack of management support

RCA teams may not feel empowered to effect change beyond their local unit or hospital, so they may, for example, elect to train local staff to use a workaround strategy rather than notify the device manufacturer about the need for a redesign.(61,65)

The RCA teams should:

- Have an experienced and effective leader who is aware of potential for cognitive biases and personal agendas and who can manage the diversity of personalities.(49,50,66)
- Comprise members of RCA teams who complete training before participating in an RCA.(49,50,59,63)
- Be multidisciplinary, including a balance between medical and nursing staff.(63)
- Include frontline staff with intimate knowledge of the incident, and personnel with knowledge of the systems and processes that might have played a role in the incident.(66)
- Integrate knowledge from system safety engineering fields.(61)
- Have explicit support from institutional or units leadership.(66)

Additionally, RCA investigators should be encouraged to perceive themselves, and be trained as, agents and facilitators of organisational development instead of professional investigators or inspectors. Progress would stem not from conducting bigger and better RCAs, but rather from repositioning RCA investigations as opportunities to trigger local and organisational learning.(49,50)

4.4. Gather information

Gathering information generally involves undertaking interviews, reviewing documents including medical records and observing. Logistical issues such as arranging interviews(52) and delays in collecting information and convening the group (49,50) are noted, while more important risks are listed below.

4.4.1. Not seeking outside knowledge

RCA team members may get so involved in the analysis of a particular incident that they fail to recognise the value of looking outside the system for similar occurrences. This includes reviewing the incident system or relevant literature.(67)

4.4.2. Failing to investigate to a sufficient degree

Many RCAs do not dig deeply enough to uncover entrenched system-based causes of incidents or latent failures. To learn about latent failures, staff members must ask probing questions about how the organisation was managing information, the environment, human resources, equipment and technology, and associated human factors at the time of the incident.(67)

The RCA team is more inclined to focus on individual shortcomings and may be less inclined to uncover the underlying system causes of these actions. Organisational culture, team

composition and team leadership may facilitate this focus. This situation often leads to inaccurate assumptions.(61,67)

4.4.3. Information quality

Medical records typically contain little specific information relating to incidents. As such, RCA teams are often required to “trawl” and synthesize additional information sources, such as computer systems, staff rotas, equipment identification, and other routinely-collected hospital episode data.(49,50)

Interviews may be more susceptible to recall bias compared to direct observations of workflow and processes.(61) Staff members may recite what they thought was the right answer and not necessarily what was the daily practice.(61)

The team may rely too much on the written content of policies and procedures to illustrate what normally happens when care is provided. There may be an assumption that what is in the policies is reflective of what really happens day-to-day.(67) This means the team may find no systems issues as the policies may be well written and broadly applicable.

4.4.4. Hierarchies

From the perspective of people being interviewed for RCAs, although the mantra of RCA is “systems-based”, many healthcare workers perceive the approach as an agent of the organisation and view it with suspicion and fear disciplinary consequences.(49,50) Within the team, despite efforts towards integrated and inter-professional working, professional and hierarchical differences may influence the direction, dynamic, and outcomes of RCA meetings. This can manifest in reluctance of people to speak up and for opinions to be suppressed and not be given due weight or consideration.(49)

4.4.5. Emotions

As RCA deal with potentially traumatic and stressful incidents, emotions can heavily affect the process. Not all team leaders are good at addressing these issues, which can result in discussions failing to progress.(49)

4.4.6. Strategies to improve data gathering

Using guides for asking questions and to the direct the information-gathering processes is recommended. The most commonly used, and probably the most comprehensive, tool in health care is that developed by the U.S. Department of Veterans Affairs. (53) This tool structures questions into communication, training, fatigue/scheduling, environment/equipment, rules/policies/procedures and barriers categories. Two other examples are the “six Ps pneumonic” (68), and Grissenger, which can be used as guides for use during interviews.(67)

Storytelling, video-reflection, and other approaches should be considered and used alongside the traditional engineering-based RCA tools.(49)

Two papers reviewed the use of simulation to supplement RCAs.(69,70) Incidents were selected from medico-legal claims or incidents – in both cases, these were related to surgery. Simulations were developed from the underlying medical records and staff were recruited to participate. The simulations were run several times and then analysed. In both studies, additional root causes compared to the traditional RCA were identified and these were felt to be more amenable to effective systems changes.

4.5. Flow diagramming

Many RCAs do not include a sequence of incidents, a flow chart, or a narrative that adequately describes what happened.(67) Flow diagramming should be an integral and mandatory feature of RCA reports.

4.6. Cause and effect / Causation statements

It is recognised that from a technical perspective, developing causes is amongst the most challenging of the RCA steps.(52) Because a RCA investigation is often not standardised and therefore “uncontrolled”, there may be no relationship between the determined root causes and the incident.(52)

It has been noted that despite this step being a critical one for RCAs, some investigations are not including it.(49,50) RCA investigators tend to focus more on the sequence of incidents (“when”) rather that understanding “why”(49)

Common issues include:

- The identified causes are often too nonspecific to develop actionable correction plans.(54)
- Focusing on a single root cause.(58)
- Analyses may end when the most convenient root cause is found or one that fits the investigator’s biases rather than the correct root cause.(52)
- The accuracy of the cause is dependent on the quality of the information gathered, which is often flawed.(63)

These issues all fit under the umbrella of failing to consider human error and human factors. The investigation of an incident sometimes ends when a human error or violation is identified as the cause. However, identification of pre-existing performance-shaping factors (such as task complexity, workflow, time availability or urgency, process design, experience, training, fatigue, and stress), or other environmental conditions, system weaknesses, or equipment design flaws that allowed the error or violation to occur, is a process that must be undertaken.(67)

Systems that standardise terminologies and processes can link together seemingly disparate causes into coherent and logical chains.(54) The Human Factors Analysis and Classification System (HFACS) is one such example.(54)

Boyd (71) and Pham (56) advocate systems to determine which causes require actions to be taken. Boyd (71) aims to broaden the causation from the details of an incident so that interventions generalise to other incidents of this type. They eliminate causal factors that have only a small degree of influence, or that are not the kinds of causes it would be usual to mention.(71)

Boyd also advocates a method taken from biology examining the causes of traits using four questions (71):

- Mechanism (How does it work?)
- Function (What is it for?)
- Development (How did it develop?)
- Evolution (How did it evolve?)

Pham, using the Commercial Aviation Safety Team (CAST) method, attempts to rank these possible mitigating actions by rating each as more or less effective a priori and according to their likelihood of implementation (see “Develop recommendations” section below).(56)

4.7. Develop recommendations

Formulating corrective actions is more difficult than finding problems (52,58), and numerous issues are cited:

- Recommendations may be aimed at the wrong level of the health care system.(58)
- RCA teams are not obliged to use evidence to justify their recommendations.(63)
- Each intervention is not clearly linked to one or more causative factors.(67)
- Systematic methods for generating risk control recommendations are not used widely.(62)
- Recommendations that are considered to be weak interventions (such as developing new rules and educating staff) are among the most common risk-reduction strategies that occur in RCAs.(57,61,62,67) These are less likely to introduce effective changes into the system.
- RCA teams may not look broadly enough at the risks they uncover to determine whether these same risks are present in other parts of the organisation or among other processes of care. For example, a mix-up between look-alike products in one area of the hospital could happen in another area of the hospital. Yet an intervention might target only a single unit, service, or department, or the RCA team might not address other products that looked similar to the ones that caused confusion.(67) On the other hand, RCA teams can attempt to learn too much about distant system issues from a single incident.(67)
- RCA teams may be unaware of the resources needed to implement final action items.(56)
- Organisations attempt to implement too many interventions.(56)
- Recommendations are made only against the single most important root cause, ignoring lesser possible causes.(66)
- Deriving general principles from the investigation of a situated activity and re-articulating these principles as recommendations is a difficult task.(72)
- The need to produce an action plan of recommendations also means that safety problems are routinely discussed in terms of available solutions.(72) In this way, problems that do not have feasible, short-term solutions are rarely addressed in action plans. This is particularly pertinent for factors related to long-term resource constraints.(49)
- Reports are often circulated to the participants for repeated comment and feedback, with the aim of “getting everybody on board”. The effort of maintaining consensus amongst participants, may mean that few contain any contentious or highly consequential findings or recommendations.(49)
- Producing a “nice” report at times becomes the main goal of the investigation and displaces the original objective of producing learning and change.(49)

- Using the investigations as a resource for action instead of their trigger; in other words, an RCA process supports changes that departments had tried to promote previously without success. Instead of a process of “evidence-based change”, this is “change-based evidence”, whereby “evidence” about “root causes” was used to support existing agendas.(49,55)

A number of authors emphasise teams should attempt to create recommendations or interventions that are known to be “strong” or more reliable.(56,58,61,62) There are some tools that categorise interventions by their reliability or strength that are quite useful for teams to discuss and consider.(53,61) Card uses a two-dimensional framework to assess interventions against effectiveness and sustainability as shown in Figure 6.(62)

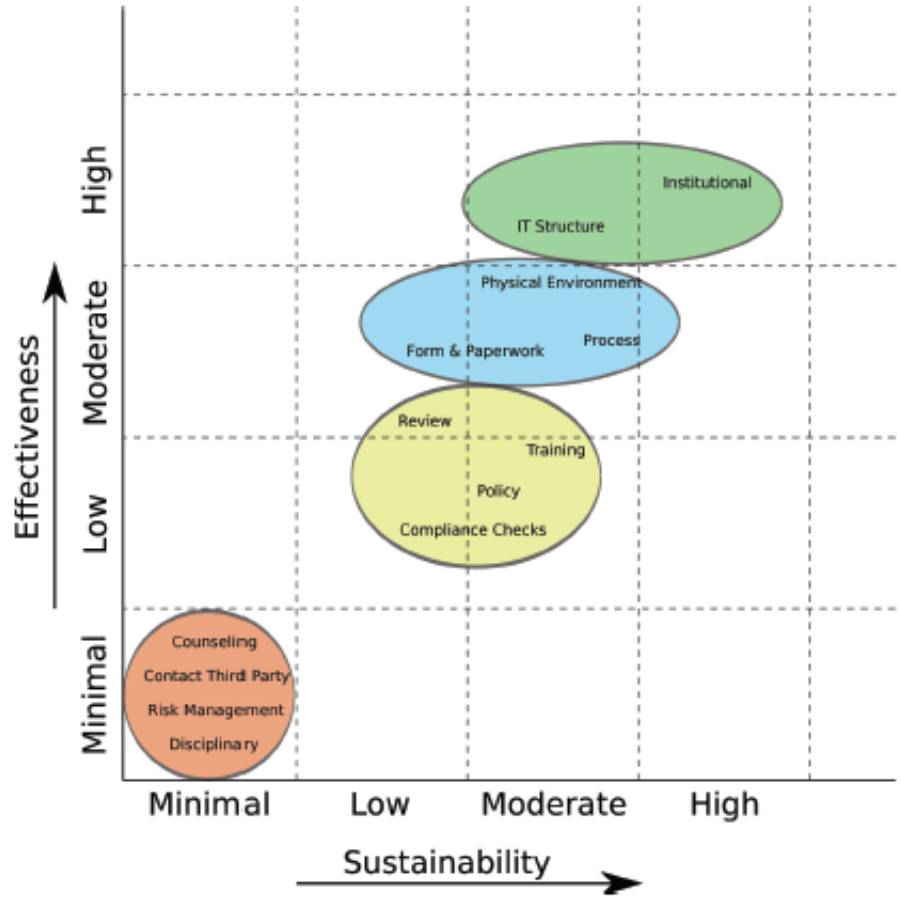


Figure 6. Effectiveness and sustainability of interventions.(62)

Pham uses a risk-prioritisation and reduction process similar to the model used in aviation by the CAST.(56) It divides the tasks of risk identification and risk mitigation into distinct but related expert teams. Two new steps are added to the process:

(a) Prioritising the factors that contributed to harm in the incident

(b) Evaluating the probability that these factors will cause harm in the future.

As a result, CAST attempts to develop interventions that address the root causes and contributing factors most responsible for causing patient harm. For the most important root causes and contributing factors, the CAST method attempts to design interventions that

reduce the probability that future patients will be harmed and that have a high probability of being implemented as intended given the available resources(56)

The investigating team uses a seven-point Likert scale to rate the importance of each identified problem and contributing factor in causing the incident (power 1, P1) and the importance of each problem and contributing factor in future incidents (this measure is called applicability, A). The output of the first step is a prioritised list of problems and contributing factors regarding the causality of the incident.(56)

The investigation team then recommends interventions and rates how well each intervention will mitigate the problem or contributing factor (power 2, P2). The intervention team assigns a score to the belief that the intervention will be implemented as intended (this measure is called confidence, C). Scores on power 2 are based on the strength of the intervention (probability) to reduce harm. Interventions that result in system redesign (such as changing a product design) have higher power 2 scores than interventions that encourage vigilance or re-education (Table 2).(56)

In some cases, it may be useful to complement these objective measures by gaining insight from clinicians and other staff who work in the area affected. The collective beliefs of frontline staff (perceptions of risk) correlate closely with actual risk and may serve as a valid measurement of the extent to which interventions actually reduced risks.

Simple questions include:

1. Are you aware of this sentinel event, its causes, and consequences?

2. In your opinion, how much risk does _____ (harm of interest) pose for patients on this unit? (Use seven-point Likert scale.)

3. Do you believe the interventions will reduce risks to future patients? If not, why?

4. Do you feel that the interventions have been effectively implemented? If not, why?

5. Do you think the degree of risk has changed within the past (time since intervention)?

6. If you think it has changed, how much greater or how much less do you think the risk is now than it was? (Measure on the seven-point Likert scale.) What do you think has caused this change?

7. Are you aware of any unintended consequences of (the intervention)? What are they?

One paper believes advocates using a high-level forum to convene representatives of manufacturers, professional societies, health care organisations (especially hospitals), and end users to agree on appropriate redesign. This group would need sufficient purchasing power to entice manufacturers, as well as technical and clinical expertise to redesign wisely.(58,73) It would be inefficient for each individual organisation to develop its own programs, and an optimal use of resources would be for professional societies to develop these programs for widespread use. National and international leadership is needed to organise this effort.(58)

4.8. Implement recommendations

The difficulties with implementing recommendations and action plans are diverse:

- Action plans tend to focus on relatively minor local changes, while broader “systemic” issues are excluded from consideration. Although this delivers short-term benefits, it does not address the more deep-seated problems affecting the organisation.(49)

- Action plans that require the collaboration of more than one department are often only partially enacted, usually within rather than across clinical areas.(49)
- Action plans that use stronger corrective actions, such as environmental changes/controls or standardisation of equipment, are more likely to be implemented and to be effective.(52)
- System changes that result from RCA may cause problems in other areas of care. In a complex system, process or product changes can unintentionally create an unsafe situation elsewhere without the knowledge of the team.(52,62)
- An impediment to linking a cause to an action may be the veil of secrecy under which RCAs are performed. Although confidentiality is important, sufficient information needs to be shared with the staff members, who will be required to implement changes so that they understand the purpose and importance of the plan.(67)
- Organisations may not be committed to making the permanent changes needed to reduce risk for a variety of political or economic reasons.(56)
- An institution may not have the financial resources to implement expensive changes, such as an increase in workforce staffing.(56)
- Follow-up and measurement of interventions is not done to determine the scope of change and its effect on patient safety.(52,56,58,61) No structured format exists to support implementation of the action plan or to monitor accountability.(67)

The addition of an implementation phase to the RCA framework may ensure that actions are implemented, the time and effort of the RCA process is not wasted, and future incidents are prevented.(52) This should include an action plan to document who is responsible for implementation, the time frame for implementation of change, and how the effectiveness of the interventions in reducing risk will be assessed.(66)

Proposed changes may need to be tested before or after large-scale implementation.(66,67) Over time, unintended consequences should be monitored, and the interventions revised and disseminated throughout the organisation in all applicable areas.(58,67)

CAST recommends having an intervention design team that is separate from the implementation team.(56)

The effect and outcomes of the program should be evaluated (58) and more formal methods to evaluate the effectiveness of interventions for reducing risks are needed.(56)

Examples of specific measures of implementation success may include:

- development of specific protocols to implement the interventions, an example being checklists
- staff awareness of the defined protocols measured through surveys and/or focus groups
- staff adherence to the protocols measured via checklists and/or audits.

The selection of an evaluation method should incorporate cost, risks to future patients, and process feasibility. In general, the attention given to such evaluation should be proportional to the subjective probability or belief by experts that an intervention will reduce harm.(56)

The National Patient Safety Foundation outlines warning signs of the ineffective RCA, which are shown below in Box 4.(53)

Box 4. Warning signs of ineffective RCA.(53)

If any one or more of the following factors are true, then your specific RCA review or your RCA process in general needs to be re-examined and revised because it is failing:

- There are no contributing factors identified, or the contributing factors lack supporting data or information.
- One or more individuals are identified as causing the incident; causal factors point to human error or blame.
- No stronger or intermediate strength actions are identified.
- Causal statements do not comply with the Five Rules of Causation.
- No corrective actions are identified, or the corrective actions do not appear to address the system vulnerabilities identified by the contributing factors.
- Action follow-up is assigned to a group or committee and not to an individual.
- Actions do not have completion dates or meaningful process and outcome measures.
- The incident review took longer than 45 days to complete.
- There is little confidence that implementing and sustaining corrective action will significantly reduce the risk of future occurrences of similar incidents.

In their review, Nicolini et al (50) used an ethnographic approach to follow 10 RCAs. Lessons learnt from the review are summarised in Box 5 below.

Box 5. Lessons learnt from Nicolini et al review on RCAs.(50)

Forming the investigation team and gathering evidence

- Ensure that the investigation team is well-balanced and include the necessary constituency to produce a robust analysis and facilitate the implementation of the results.
- Use short training and information sessions as ways to prevent anxiety and resistance to being involved in root cause analysis (RCA).
- Ensure management support is clear and visible, techniques such as using a formalized escalation procedure should be considered.

Conducting the analysis and identifying root causes

- Ensure that RCA meeting facilitators have a recognised status comparable to that of the most authoritative practitioners present.
- Use RCA practitioners who have previous familiarity with the existing area of practice.
- Train reputable clinicians as RCA leads.
- Utilize analytic tools that are attuned to the mindset of the practitioners involved.

Formulating and implementing service improvements

- Ensure RCA reports are considered as stepping stones in the change process and not the end result of the activity.
- Use RCA investigations to identify trends and establish change initiatives.
- Ensure that RCA investigations build on previous experience and available evidence.
- Share results within the organisation.
- Establish formal mechanisms to audit the implementation of recommendations.
- Train RCA practitioners in change management techniques and help them perceive themselves as change agents rather than professional investigators.

4.9. Chapter summary

- RCA is a toolbox of techniques. There are many options for gathering information and brainstorming, some of which are highlighted in this report; however, developing a range of options may be valuable as a resource.
- Simulation is a valuable data-gathering technique. Translated into the e-health environment, this equates to testing or reproducing incidents.
- When undertaking data gathering, do not assume that what policies say necessarily reflects what happens day-to-day. This means data collection and interviewing techniques are crucial.
- Aggregating the findings across multiple RCAs and other data sources, such as reported incidents, allows identification of key risks and proactive development of improvement programs.
- RCA team members should have a diverse set of expertise to develop effective interventions including human factors engineering, and organisational psychology/sociology.
- Using metrics to measure the effectiveness and sustainability of the RCA process may be useful if large numbers of investigations are undertaken.

- Using standardised classifications systems can assist in the RCA process as well as provide a common understanding of key risks when aggregating findings from multiple RCAs.
- Developing recommendations that are effective and sustainable presents significant challenges. Developing formal processes and techniques to prioritise recommendations may be valuable. Using tools to rate recommendations by strength is also important.
- Most of the problems outlined are not functions of deficits in the RCA technique itself, but originate in the complexity of the organisations in which they are being undertaken, the well-described challenge of managing inter-professional teams, and the inherent tendencies of people to invoke personal agendas and to be subject to cognitive biases.

5. London Protocol

The ‘London Protocol’ was developed by Sally Taylor-Adams & Charles Vincent at Imperial College, London, with the second edition released in 2004.(74) The purpose of the protocol is to ensure a ‘comprehensive and thoughtful investigation and analysis’ of an incident, ‘going beyond the more usual identification of fault and blame’.

Like RCA, a modified version Accident Causation Model (75) provides a theoretical underpinning (Figure 7). In this model, fallible decisions at the higher echelons of the management structure are transmitted down departmental pathways to the workplace, creating task and environmental conditions that can promote unsafe acts of various kinds. Defences and barriers are designed to protect against hazards and to mitigate the consequences of equipment and human failure. These may take the form of physical barriers (such as a fence), natural barriers (such as distance), human actions (such as checking) and administrative controls (such as training). In the analysis of an incident, each of these elements is considered in detail, starting with unsafe acts and failed defences and working back to the organisational processes. The first step in any analysis is to identify active failures – unsafe acts or omissions committed by those at the “sharp end” of the system (for example, pilots, air-traffic controllers, anaesthetists, surgeons, nurses) whose actions can have immediate adverse consequences. The investigator then considers the conditions in which errors occur and the wider organisational context, which are known as contributory factors.

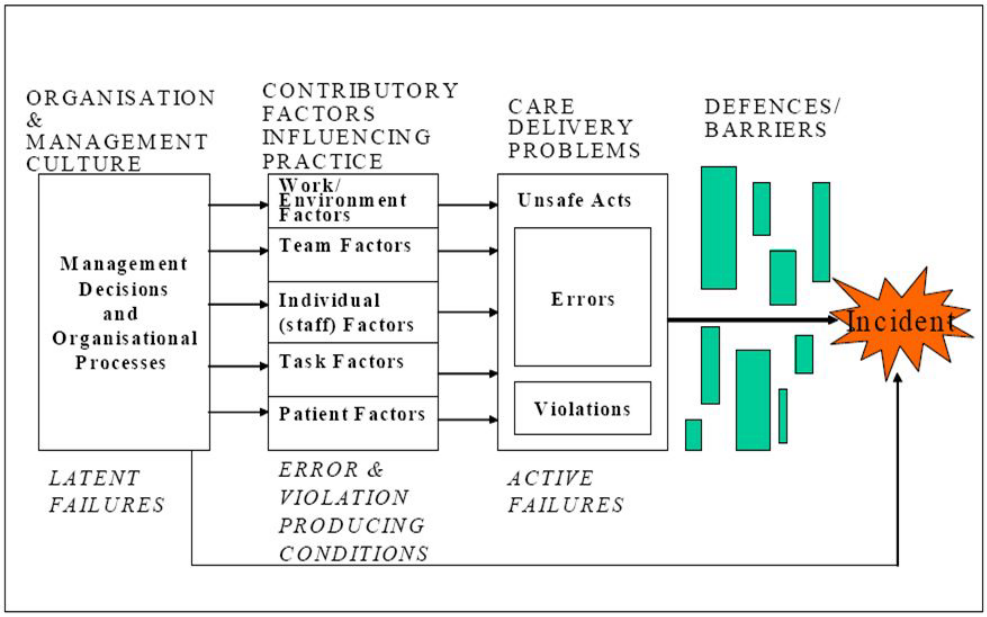


Figure 7.The Accident Causation Model (75) modified for the London Protocol (74).

The Protocol has developed a contributing factors framework which is designed to be specific to health care. It comprises the broad categories (74):

- Patient Factors Condition (complexity and seriousness)
- Language and communication
- Personality and social factors

- Task and Technology Factors Task design and clarity of structure
- Availability and use of protocols
- Availability and accuracy of test results
- Decision-making aids
- Individual (staff) Factors Knowledge and skills.

A key difference between RCAs and the London Protocol is the introduction of the term “care delivery problems” (CDP). This is an overall description of errors or violations. They may be slips, such as picking up the wrong syringe, lapses of judgement, forgetting to carry out a procedure or, rarely, deliberate departures from safe operating practices, procedures or standards. The rationale for the use of the term “care delivery problems” compared to “unsafe acts” is that it is neutral terminology and because a problem often extends over some time and is not easily described as a specific unsafe act; for example, failure of monitoring of a patient may extend over hours or days. CDPs have two essential features:

- Care deviated beyond safe limits of practice
- The deviation had at least a potential direct or indirect effect on the eventual adverse outcome for the patient, member of staff or general public.

The process for undertaking the London Protocol technique is outlined in Figure 8 below. The process is similar to a RCA; the technique is retrospective, the investigation is commissioned by the organisation and a small multi-disciplinary team is used that has a diverse range of skills including management, knowledge of the process being studied and human factors.

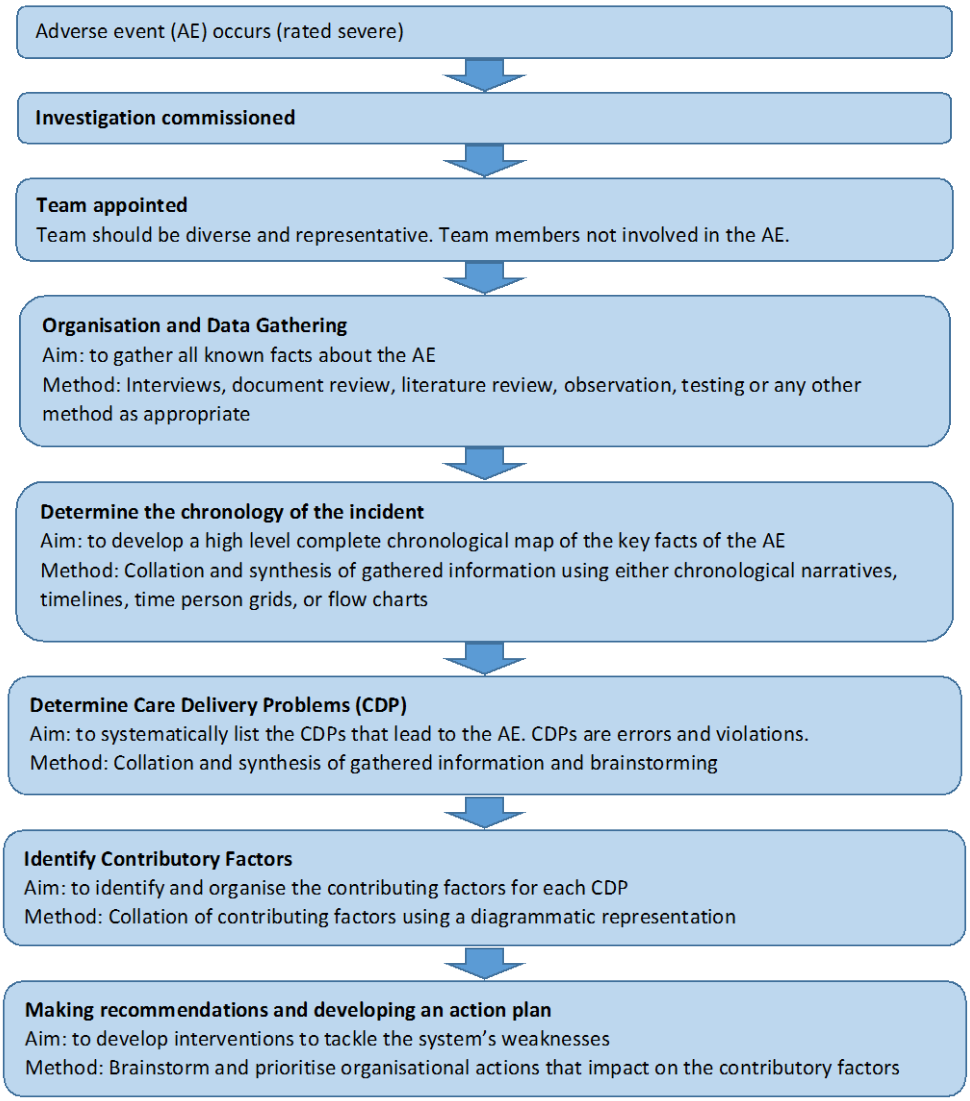


Figure 8. High level steps of the London Protocol.(74)

Unlike a RCA, the first step is data gathering, including undertaking interviews. The interview structures are more structured than generally advocated in a RCA with questions asked regarding the chronology of the incident, CDPs and contributing factors (see Figure 9). RCA questions tend to be "open". The aims and methods of the rest of the investigation are quite similar to a RCA.

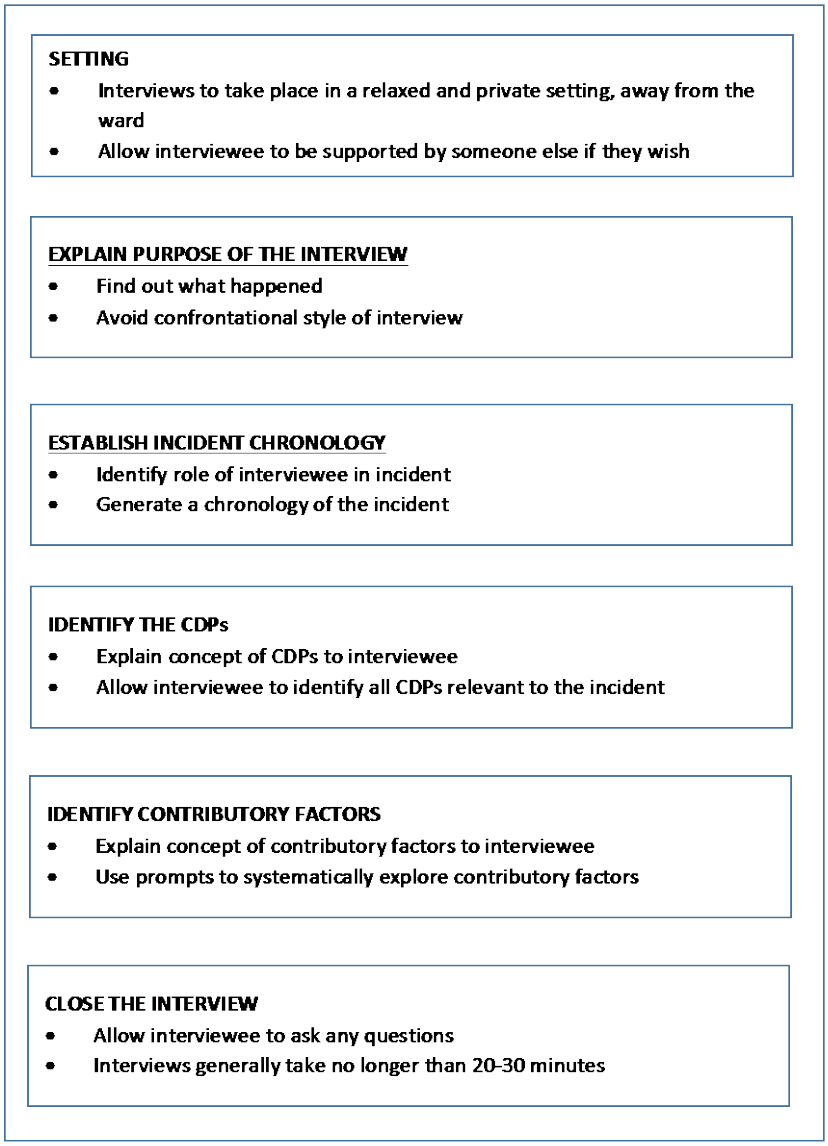


Figure 9. London Protocol interview structure.(74)

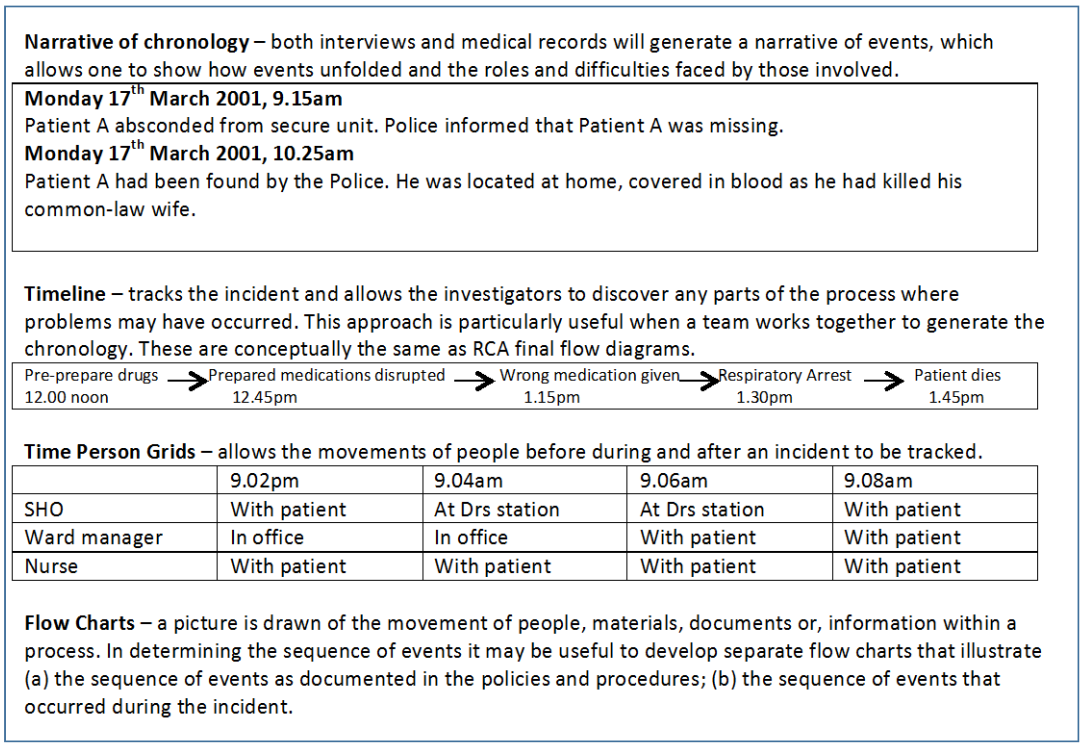
The London Protocol authors make two distinctions between RCA and their method:

1. "To us the term Root Cause Analysis, while widespread, is misleading in a number of respects. To begin with it implies that there is a single root cause, or at least a small number. Typically however, the picture that emerges is much more fluid and the notion of a root cause seems a gross oversimplification. Usually there is a chain of events and a wide variety of contributory factors leading up to the eventual incident."

2. "A more important and fundamental objection to the term Root Cause Analysis relates to the very purpose of the investigation. Surely the purpose is obvious? To find out what happened and what caused it? We believe that this is not the most penetrating perspective. Certainly it is necessary to find out what happened and why in order to explain to the patient and family and others involved. However, if the purpose is to achieve a safer healthcare system, then finding out what happened and why is only a way station in the analysis. The real purpose is to use the incident to reflect on what it reveals about the gaps and inadequacies in the healthcare system."

The first distinction is not supported by the literature on RCA. In the numerous papers on RCA, it is clear that the vast majority of advice is that multiple root causes exist and these must be identified. Indeed, most of the RCA advice states that single root causes are rare. The second distinction is more subtle and depends on the various RCA methods; however, most methods are trying to broaden the investigation from not just what happened during the incident, but what are the deficits in the care delivery system.

A number of methods of developing a chronology of incidents are outlined in Figure 10 which may have applicability for RCAs.(74)



Narrative of chronology – both interviews and medical records will generate a narrative of events, which allows one to show how events unfolded and the roles and difficulties faced by those involved.

Monday 17th March 2001, 9.15am
Patient A absconded from secure unit. Police informed that Patient A was missing.
Monday 17th March 2001, 10.25am
Patient A had been found by the Police. He was located at home, covered in blood as he had killed his common-law wife.

Timeline – tracks the incident and allows the investigators to discover any parts of the process where problems may have occurred. This approach is particularly useful when a team works together to generate the chronology. These are conceptually the same as RCA final flow diagrams.

Pre-prepare drugs 12.00 noon → Prepared medications disrupted 12.45pm → Wrong medication given 1.15pm → Respiratory Arrest 1.30pm → Patient dies 1.45pm

Time Person Grids – allows the movements of people before during and after an incident to be tracked.

	9.02pm	9.04am	9.06am	9.08am
SHO	With patient	At Drs station	At Drs station	With patient
Ward manager	In office	In office	With patient	With patient
Nurse	With patient	With patient	With patient	With patient

Flow Charts – a picture is drawn of the movement of people, materials, documents or, information within a process. In determining the sequence of events it may be useful to develop separate flow charts that illustrate (a) the sequence of events as documented in the policies and procedures; (b) the sequence of events that occurred during the incident.

Figure 10. Methods for developing a chronology of incidents.(74)

5.1. Findings from the literature

One paper was found in our search of the literature that discusses in sufficient detail the use of the London Protocol. The paper reported on 30 reviews conducted with the protocol in a neonatal unit in Canada (76). The lessons from their experience were:

- Critical occurrences usually have multiple contributory factors
- Writing recommendations is easy, implementation is challenging
- The Protocol provides structure for interviews and the search for information
- The complexity of human factors science requires expertise to tease out contributory factors, root causes and the context in which they occurred
- A human factors consultant is invaluable in guiding the team.

5.2. Chapter summary

- The London Protocol process is similar to that of RCA, with the technique based on the Accident Causation Model; being retrospective, the investigation is commissioned by the

organisation and a small multi-disciplinary team is used that has a diverse range of skills including management, knowledge of the process being studied and human factors.

- The London Protocol introduces usable concepts, such as care delivery problems, and outlines more variants of displaying incident chronologies. These can be part of the "toolbox of techniques" for undertaking investigations.
- Although the RCA and London Protocol have some differences, these are relatively minor. We believe that the less minor methodological differences mean that the Protocol is similarly vulnerable to the main problems besetting RCAs. Indeed, most of these problems are not functions of deficits in the RCA technique (or Protocol) itself, but originate in the complexity of the organisations in which they occur, the well-described challenge of managing teams, and the inherent tendencies of people to invoke personal agendas and to be subject to cognitive biases.
- Similarly, the potential solutions to these problems, for example appointing a well-balanced team with adequate knowledge of the method and including human factors skills and knowledge, providing training to team members, ensuring management support, formulating "strong" interventions that are likely to work in the long terms, and measuring outcomes are generic to both techniques.
- The lessons to be taken from the London Protocol are using a standardised contributing factors framework, possibly structuring interviews differently, providing a conceptual distinction between CDFs and contributory factors, and using a variety of methods to develop the chronology of incidents. Some or all of these can be embedded in an RCA or London Protocol method as appropriate, without changing its intent or integrity of its method.

6. Failure Mode and Effect Analysis (FMEA)

Failure Mode and Effect Analysis (FMEA) is a systematic method of identifying and preventing product and process problems **before they occur**. A key difference between FMEA and Root Cause Analysis (RCA) is that it is p**ro-active** not **retrospective;** in other words, it does not rely on something going wrong as the trigger for an investigation. FMEA was developed as a US military procedure, and in the late 1940s was later used in aerospace and the rocket industry as well as other industries.

FMEA includes review of the following:

- Steps in the process (process mapping)
- Failure modes (What could go wrong?)
- Failure causes (Why would the failure happen?)
- Failure effects (What would be the consequences of each failure?).(77)

FMEA is particularly useful in evaluating a new process prior to implementation and in assessing the impact of a proposed change to an existing process.(77) FMEA enables system redesign of high-priority processes.(66) The key similarities and differences between FMEA and RCA are outlined below in Table 3 and the main steps are shown in Figure 11.

Table 3. Similarities and differences of RCAs and FMEAs.

Similarities
Interdisciplinary teams
Flow diagrams
Focus on systems issues
Actions and outcomes measures developed
Scoring matrix (severity/probability)
Use of triage/triggering, cause and effect
Differences
Process vs. chronological flow diagram
Prospective (what if) analysis
Choose topic for evaluation
Include detectability and criticality in evaluation
Emphasis on testing intervention
FMEA possibly less than confronting because not dealing with a particular adverse event

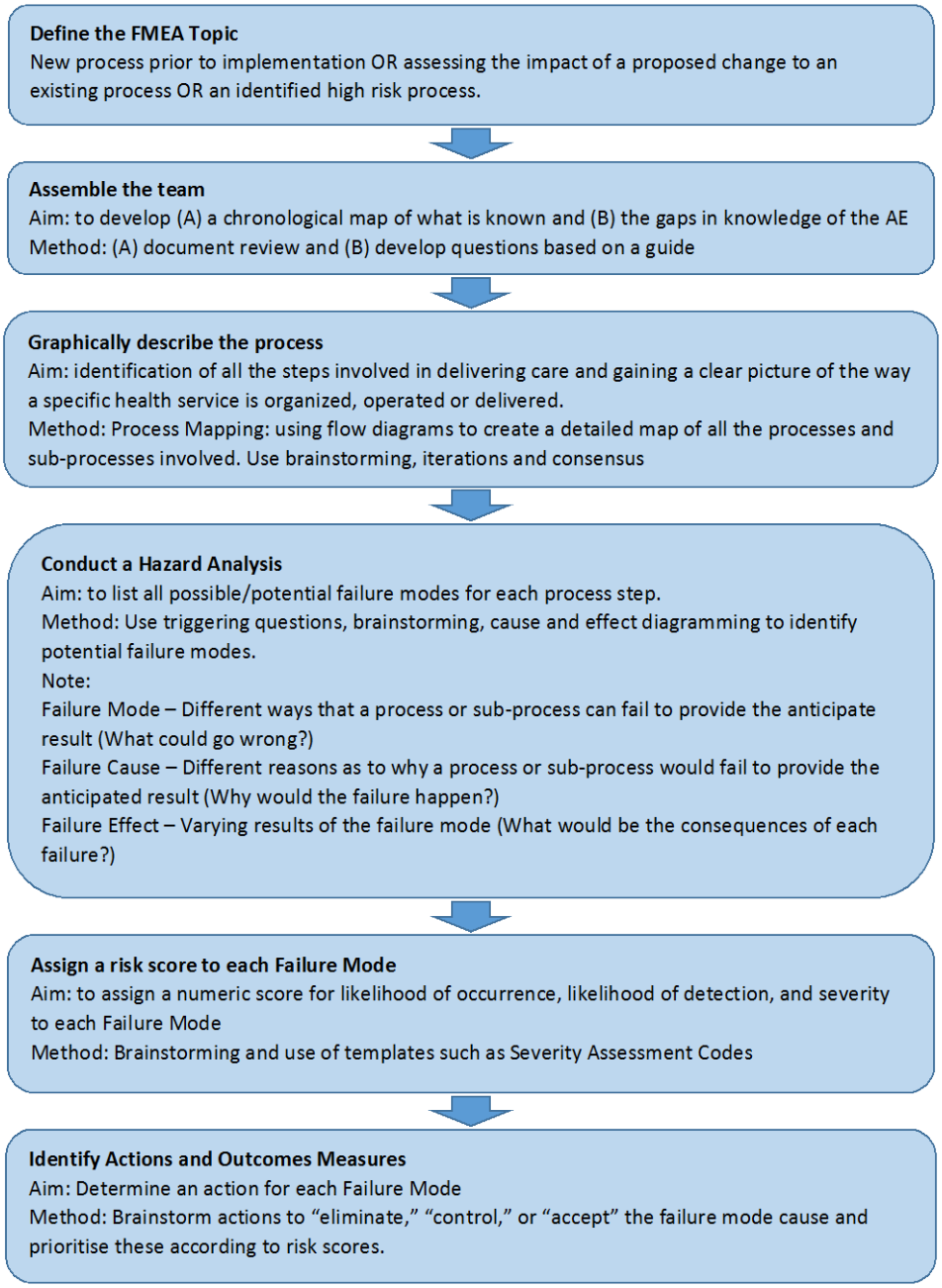


Figure 11. Steps in the FMEA process.(78)

The use of FMEA in health care incorporates many lessons that can be applied to the e-health sector, both in terms of challenges with, and potential ways to strengthen the method. These are outlined below.

6.1. Potential benefits

In an evaluation of 62 FMEA team members, Habraken *et al.* found about 90% of people thought that the FMEA was meaningful, that the investigated process would be safer, and that they would recommend the process to others.(79) On the other hand, Wetterneck *et al.* found team members were slightly more negative on the impact and benefits of FMEAs.(80) Guidelines for FMEA success are outlined in Box 6 below.

Box 6. Guidelines for FMEA Team Success. (80)

1) Ensure that the team objective is well defined with established scope boundaries.

2) Obtain a skilled and effective leader and facilitator for the FMEA team.

3) Ensure visible top leadership support for team activities and patient safety.

4) Ensure that teams are multidisciplinary and include process owners and frontline staff.

5) Emphasise, support and monitor attendance. Management must support adequate time off from clinical duties for staff to attend FMEA meetings and compensation for meeting time. Over-recruiting frontline staff to ensure that at least one person from every discipline attends each meeting.

6) Assess baseline knowledge of the FMEA process and the process and/or technology to be evaluated. Train team members to assure adequate knowledge before or early in team process.

7) Inform team members of expected time commitment based on FMEA project scope. Long processes and technology evaluations will take months to complete. Plan-related technology implementation for months after the FMEA team has completed its work to allow time for needed process and technology changes.

8) Encourage and support communication and active participation among team members. Be aware of grouping and dominating team members.

9) Monitor progress of FMEA team towards its goal.

10) Evaluate outcomes of FMEA team, and develop lessons learned for future FMEA teams and similar team activities.

6.2. Time taken to do an FMEA

The main criticism of FMEA is that it can be time-consuming and resource-intensive for health care organisations.(79-83) Various studies show that the average number of meetings necessary to conduct a FMEA is approximately six-eight meetings. Each meeting takes a mean duration of 1.5 hours with an average of eight participants per meeting. This corresponds to 96 hours of healthcare professionals' time per FMEA (see Table 4 for some examples).(79,82,84) The high number of meetings and the length of time required for each meeting may result in inconsistent attendance due to work schedules and time commitments of healthcare professionals, resulting in loss of expertise and continuity.(82)

Table 4. Metrics on 13 FMEAs in the Netherlands.(79)

ID	Health care process	Health care setting	Facilitator[a]	Team size[b]	Number of meetings	Number of person-hours[c]	Number of failure modes	Number of actions
	MAASTRO clinic							
1	Documentation of treatment	Radiotherapy	PR	5	4	30.0	32	17
2	Electronic Portal Imaging	Radiotherapy	MH	8	6	72.0	109	33
3	Treatment on linear accelerator	Radiotherapy	JR	5	8	60.0	70	30
4	Release of accelerator after maintenance	Radiotherapy	PR	4	5	30.0	50	22
	UMC Utrecht							
5	Communication of unexpected findings	Radiology Cardiology	MH	7	5	52.5	19	7
6	Diet food process	Children's Hospital	MH	13	7	136.5	39	18
7	Physically restraining patients	Neurosurgery	MH	7	7	73.5	31	17
8	Ordering repeat prescriptions	Primary care	DZ	8	8	96.0	50	12
9	Patients with hip fractures	Emergency Room Radiology Ward Operating Room	MH	8	6	72.0	120	7
10	Medication administration (pumps)	Intensive Care Unit	MH	6	6	54.0	46	22
11	Admission of cardiac patients	Emergency Room Cardiac Cath Room Coronary Care Unit	CP	6	6	54.0	44	6
12	Use of a PICC line (catheter)	Neonatal Intensive Care Unit	MH	8	8	96.0	37	8
13	Administration of blood products	Laboratory Haematology ward	MH	8	6	72.0	27	11
			Mean	7.2	6.3	69.1	51.8	16.2
			SD	2.2	1.3	28.7	30.6	8.8

Suggested methods for reducing the length of the time commitment include asking a subgroup of the team to map the selected process in advance. During the first meeting with the entire team, the other team members could then be asked to verify the graphical process description. This is done commonly during RCAs. Another possible way to save time is to first carry out both a hazard analysis and determine appropriate actions for one process step before investigating the next one. By doing so, the team members will master the different steps of FMEA more quickly, allowing a faster handling of the other process steps. Moreover, if time constraints force the team to stop the analysis, a complete FMEA analysis has been conducted for at least one or more process steps.(79)

6.3. Assembling the FMEA teams

FMEA teams are similar to RCAs. Teams should be multi-disciplinary.(80,81,84,85) Effective communication skills were seen as important to promote understanding of different working cultures and professional language and to sustain more reliable results.(79,81) Teams should include individuals who can characterise the process, identify failure modes (80), and understand their effect, as well as those who can design and implement new processes.(79) Finding a team of busy health care professionals with the appropriate knowledge, skill mix, and logistical availability for regular meetings is, however, a serious challenge.(84,86)

The role of the facilitator is crucial.(79) An external facilitator to lead the group through subsequent steps can be considered. The facilitator may not have domain knowledge of the process, but rather this individual should stimulate the participation of all team members.(66) The alternative may be to develop organisation-wide FMEA experts to facilitate and be team members for ongoing FMEAs.(80)

Training was noted as being required for regular team members before starting the FMEA process, as was just-in-time training for members who were participating for only short periods (for example, front-line staff).(80,81) The facilitators should be trained in using a

system and in a human factors approach.(79) It was noted that there was a lack of written guidance on the identification of failure mode causes and effective actions, and this lack of a standardised guide might influence the quality of the outcomes of a FMEA.(79)

6.3.1. The involvement of patients or consumers in an FMEA

In a national FMEA evaluation, respondents had differing views on the benefits of patient involvement.(79) The respondents of teams in which a patient participated nearly all believed the involvement of the patient was useful. On the other hand, only a few respondents who participated in FMEA analysis without patient involvement thought that patient participation would have been valuable. The usefulness of patient involvement also is likely to depend on the type of process to be analysed. However, the results might also indicate that clinicians do not recognise the merits of patient involvement in risk analysis until they actually see it happen.(79)

6.4. Management and organisation support

The FMEA process should be guided by a well-defined objective for the team with a limited and bounded scope and visible support from the top leaders in the organisation, for both the process itself and a commitment to use team findings to improve safety. It is important for team members to know that the team activities are important to the organisation and that the team recommendations will be acted on to improve safety.(80,83)

6.5. Graphically describe the process (process mapping)

The stage of FMEA involving multidisciplinary process mapping seems the most valuable step with good reliability and validity.(82,85) As FMEA is time consuming, choosing a complex and long process(81) is not recommended (an example being the entire medication management process). Breaking up the process into its component parts (such as prescribing, dispensing, administration) and tackling each separately with an FMEA is likely to be more manageable. Two representations may be needed: the way that the process is intended to occur and the way that it actually occurs.(66)

When an FMEA is conducted, teams must be aware that the conclusions of FMEA are usually short-lived. As guidelines and protocols continue to be periodically updated, along with the introduction of new technologies – such as electronic prescribing, clinical decision support or bar-coding – a given set of process maps may only be valid for a limited time period and should therefore be updated regularly.(85) Figure 12 shows an example of a process map from an FMEA.

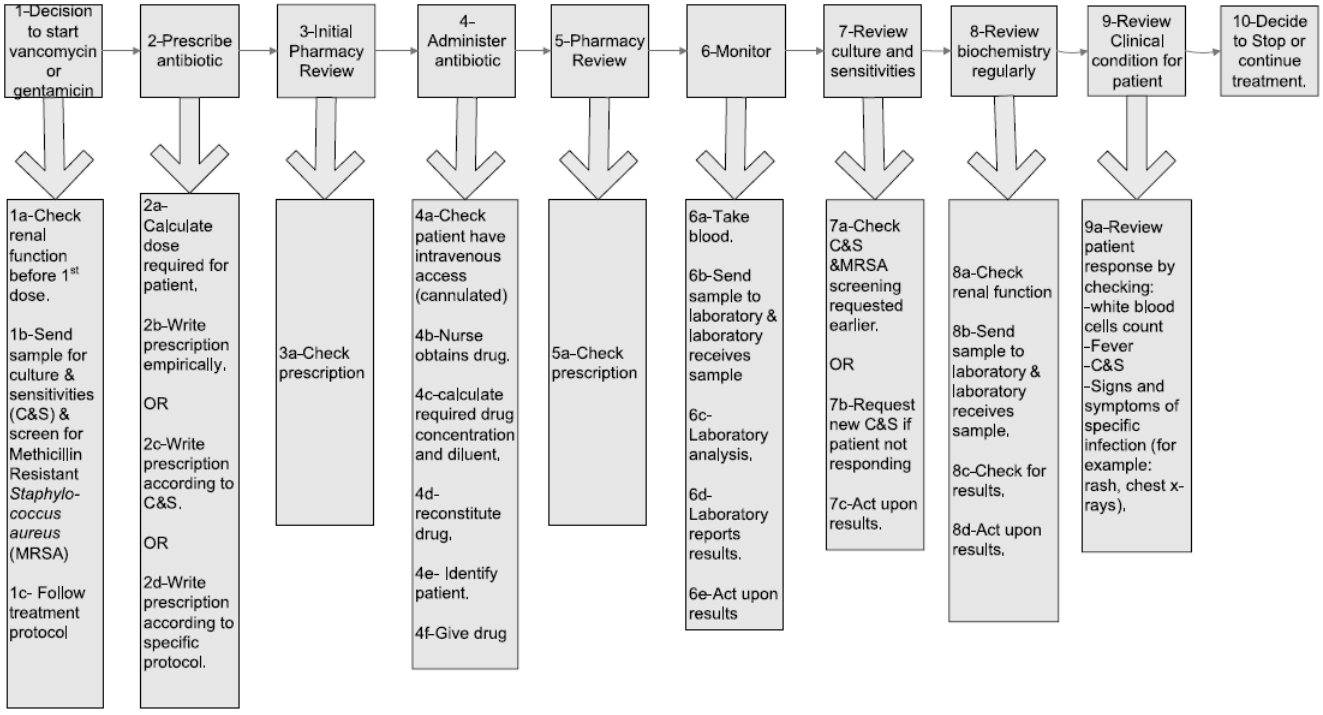


Figure 12. Vancomycin and gentamicin process map.(81)

6.6. Conduct a hazard analysis

The literature describing FMEA hazard analysis suggests that this process is difficult to carry out due to its complexity, and its reliability and validity has been questioned.(79) One study found two groups analysing the same process identified only 20% failure modes common to both.(81) In another study, a FMEA team, reviewing a high-risk medicine process, did not identify the most frequently occurring incident type in the incident reporting system – omitted medicines. On the other hand, another study points out that in a head-to-head comparison of failure modes in radiation therapy, 17% of possible process failures were detected by incident reports only, and 57% were detected by FMEA only.(87) This underlies the well-established principle in patient safety that multiple data sources are ideal to capture the large variety of things that go wrong.(44) If only a FMEA is being performed, it must be realised that preventing errors that have *never occurred* is an important purpose, if not one of the main purposes, of this tool.(88) Content validity of the FMEA outputs may be achieved by allowing the FMEA teams to use other sources, besides their experience and knowledge, such as hospital audits or incident report databases, to list as many potential failures as possible.(85)

A key point when conducting a hazard analysis is that failures at one stage of a process can be mitigated if the failure is readily observed. Even a serious failure that occurs frequently may have little effect on patients if it is noted at once and downstream steps are able to respond to the previous failure. In comparison, tightly coupled processes in which there is little ability to buffer the effects of previous failure are more likely to lead to a cascade of events that result in patient harm.(66)

6.7. Assign a risk score to each Failure Mode

There are three major problems with assigning a risk or numeric score to failure modes. Firstly, the FMEA was originally developed for use in engineering, in which systems are largely deterministic and failure rates more easily quantifiable. However, in health care, *human-based* systems introduce variation, which is much harder to quantify.(82, 89)

Secondly, the FMEA process is subjective, but the use of numerical scores gives an unwarranted impression of objectivity and precision.(82) Thirdly, the numeric score is calculated by multiplying three ordinal scales: severity scores, probability scores and the detectability scores. In an ordinal scale, the categories have an ordered or ranked relationship relative to each other; the amount of difference between ranks is not specified. However, ordinal numbers cannot meaningfully be multiplied or divided.(89) Multiplying the three scales to produce a numeric score breaches the mathematical properties of the ordinal scales.(85)

The scores might be useful to guide the team, but the scores should not become the main focus of the process where the aim of the FMEA becomes reducing the numeric score values rather than finding solutions to avoid failures or errors from reaching the patient. Furthermore, focusing the FMEA on reducing the numeric score values may result in biased results as participants' focus shifts from patient safety to lowering numerical values.(85) In summary, using FMEA as a quantitative technique to prioritise, promote or study patient safety interventions should be avoided.(82)

Some potential solutions include:

- Acknowledging that the scoring system is subjective.(81,86) The success or failure of the FMEA should not be measured by the reduction in numeric scores alone but instead by implementing and evaluating changes within the process of care to ensure patient safety.(81)
- Using a consensus scoring procedure as it allows variability in individuals' scores and rationales to become apparent and to be discussed and resolved by the team.(81,86)
- Using more defined and reliable categories for probability of occurrence. This may reduce the likelihood of team members placing their own interpretation on the categories. For instance, one could use categories such as 'weekly', 'monthly', 'yearly' and 'less'.(79)
- Replacing numbers with ordinal scale categories, such as 'very high risk', 'high risk', 'low risk' and 'very low risk' with accompanying red or green shades of colour.(79)
- Using Pareto charts whereby mitigations are first provided for the most severe events, in order of their decreasing frequency of occurrence.

6.8. Identify actions and outcome measures

As with RCAs, selecting appropriate error reductions strategies also can be a difficult challenge for FMEA teams.(83) Emphasis must be placed on identification of root causes, not just proximate causes of the failure modes.(66) In general, there are three approaches to redesign: the prevention of failure modes; improved detection of failures; and implementation of recovery processes that mitigate the effects of failure, this means preventing failures that do occur from reaching the patient).(66) As with RCA, each mitigation represents a design change to the process and itself represents a risk that 1) the mitigation is not sufficiently effective, or 2) the mitigation causes new errors.(88) The process for measuring the effectiveness of recommendations is similar to RCAs.

6.9. Alternative techniques

6.9.1. Sociotechnical Probabilistic Risk Assessment (ST-PRA)

Where there is no component failure but rather a probabilistic deviation from intention and expectation, using FMEA can be problematic.(90) Sociotechnical Probabilistic Risk

Assessment (ST-PRA) is a complex, high-end risk modelling tool, that provides an opportunity to visualise system risk in a manner that is not possible through FMEA.(91) An example of an ST-PRA is shown in Figure 13. Probabilistic Risk Assessment (PRA) is a process for modelling the combinations of multiple failures leading to a specific undesirable outcome. When the modelling includes the contributions of behaviours or human error as a cause of the adverse outcome, it becomes known as ST-PRA.

Compared with FMEA, PRA uses a ‘‘top-down’’ approach that identifies the undesirable outcome to be modelled first, and then investigates and models all combinations of process failures that may lead up to this event. ST-PRA is distinguished from FMEA as FMEA starts with a process to be analysed, whereas ST-PRA starts with an undesirable outcome.(91)

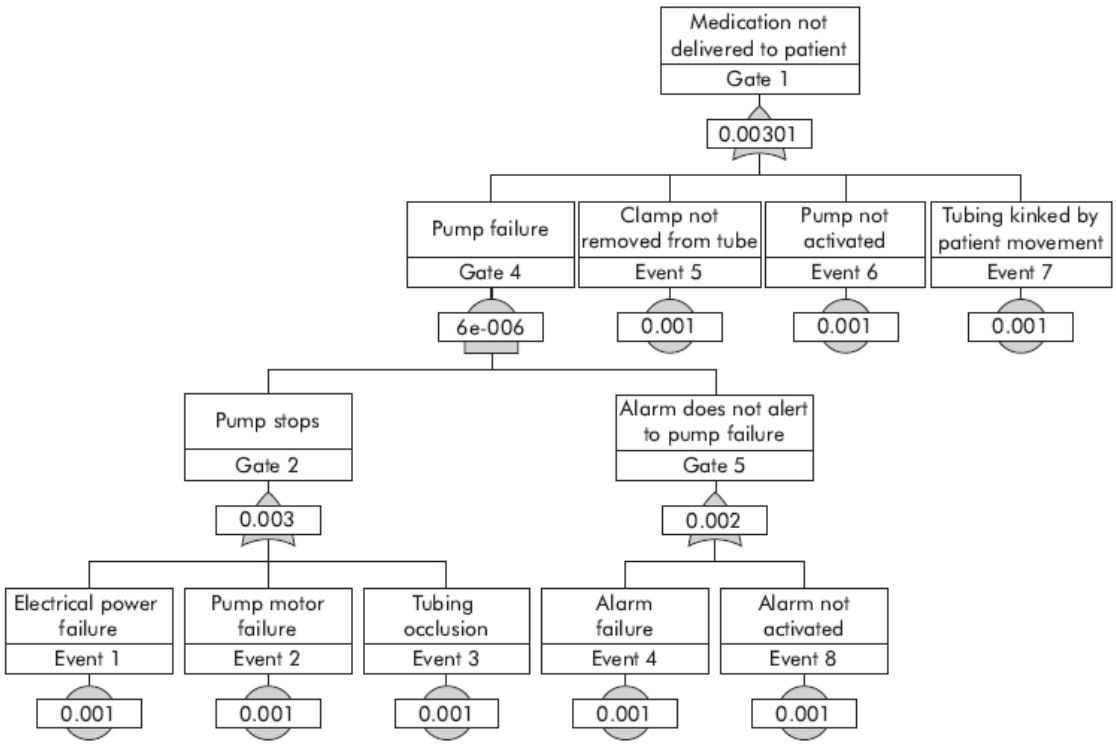


Figure 13. An example of a Sociotechnical Probabilistic Risk Assessment (ST-PRA).(91)

6.9.2. Fault Tree Analysis

A FMEA does not provide a hierarchical perspective necessary to represent a complex or sequential mode failure that is systematic. For these, fault tree analyses (FTA) are necessary. A FTA provides a way to define and depict the sequence of events and conditions that lead to undesired outcomes. Individual pathways through the event tree are referred to as event sequences.(92)

6.9.3. Simulation

Similar to studies which reviewed simulation and RCA, Nielsen *et al.* (2014) explored whether additional data were found when a traditional FMEA was augmented with simulation. The nature of simulation allows for a detailed examination of every single step in the process, revealing vulnerabilities that may be missed when just brainstorming the process map. Overall, the simulations were effective in identifying additional failure effects (60%) and causes (40%), and to a lesser extent failure modes (25%), than brainstorming the process map alone.(93) The additional types of failure modes were mainly associated with practical coordination issues between crews. Brainstorming did not reveal the complexity of

crew coordination when crews were cooperating face-to-face regarding the same patient. Simulation forced participants to experience the consequences if the process did not proceed optimally (for example, waiting time, uncertainty over what the other crew was doing, and prioritising tasks between the crews). Brainstorming only entails talking about actions, not actually fulfilling the actions. However, the additional resources required for the simulation in additional to traditional FMEA need to be weighed against potential benefits.(93)

6.10. Chapter summary

- A key distinguishing feature of FMEA is that it is a proactive method of identifying and preventing problems, in contrast to RCAs and the London Protocol, which are retrospective.
- One of the important purposes of FMEA is identifying and preventing errors that have *never occurred.*
- One of the main barriers to undertaking an FMEA is that it is time-consuming. Topics should be well-defined and scoped and there be reasonable certainty that they are high risk if an investment in FMEA is to be undertaken.
- The most valuable FMEA step, from a learning perspective, seems to be the process mapping. This step has good reliability and validity. However, this step may need to be reviewed and updated if technologies and processes are changing.
- The hazard analysis is the most challenging step. Applying numerical scores should not become the main focus of the process but rather a means to an end of finding solutions to avoid system failures.
- Other proactive alternatives also exist, such as a Sociotechnical Probabilistic Risk Assessment and Fault Tree Analysis.
- Like with RCA, simulation can provide another valuable data source for the FMEA; however, its value must be balanced against the additional resources that are necessary.

7. Interview findings: Current practices for investigating IT incidents

7.1. Key informants

In consultation with the Commission and international experts in HIT safety, a snowball sampling strategy was used to refine and expand an initial list of 10 organisations for our study (Appendix C: List of interviewees). Key informants were identified and invited to participate in an interview about their processes to investigate incidents. Additional informants identified at interview were followed-up.

7.2. Method for interviews

Informants who agreed to participate were interviewed by telephone. Informants were asked to describe their organisation's approach to IT safety and processes to investigate incidents. We recorded responses to a series of questions about the incident investigation team, use of formal techniques (such as the London Protocol, RCA, FMEA, Fault Tree Analysis) and information sources were used to reconstruct the sequence of events leading to an IT incident. Informants were invited to share any tools or templates used to support processes. Background information about the organisation, types of clinical IT systems, total number of incidents, harms arising from the incidents, effectiveness of processes was gathered at the end of the interview (see Appendix D: Interview schedule).

7.3. Analyses

Structured responses and free-text descriptions provided rich data about current practices to investigate IT incidents locally and internationally. Interview data was validated against any documentation provided by informants.

7.4. Findings: overview of incident investigation processes reviewed

We examined processes for investigating IT incidents in nine national-level programs and centres of excellence, as shown in Table 5. Amongst the programs that responded to our invitation, two were associated with national IT safety initiatives and patient safety incident monitoring in England and the USA. One was part of a regional program in England (Taunton and Somerset NHS Foundation Trust) and another was in the USA (Pennsylvania Patient Safety Authority). Three were within major health systems in the USA (Department of Veterans Affairs, Kaiser Permanente, Memorial Hermann Health System). And two were within hospitals in the USA (Brigham and Women's Hospital, Boston) and Australia (Alfred Health, Melbourne). Two US organisations did not respond to our invitation (The Bon Secours Health System and Medstar Health).

Table 5. Organisations in which HIT investigation processes were examined.

	Organisation	Country
National/regional level	**1.** Health & Social Care Information Centre	England
	2. Taunton and Somerset NHS Foundation Trust	England
	3. ECRI Institute	USA
	4. Pennsylvania Patient Safety Authority	USA
Health systems	**5.** Department of Veterans Affairs	USA
	6. Kaiser Permanente	USA
	7. Memorial Hermann Health System, Texas	USA
Hospitals/ hospital networks	**8.** Brigham and Women's Hospital	USA
	9. Alfred Health, Melbourne	Australia

Of the nine programs reviewed, seven were specifically associated with HIT implementation which had the general characteristics of a) combining commercial and “home-grown” HIT configurations, and; b) having incident management processes at varying stages of maturity.

7.4.1. Commercial or combination of home-grown and commercial configurations dominated

Most HIT implementations were a combination of home-grown HIT systems (developed internally by the organisation) and commercial software systems that were procured from one or more vendors and then adapted to local requirements. The hub-and-spoke model, in which a range of commercial systems were integrated with home-grown interfaces, was a commonly employed configuration. A notable exception was the US Department of Veterans Affairs, where software systems were fully home-grown configurations.

7.4.2. Incident management processes varied in maturity

The reviewed processes to manage incidents varied in maturity. One example was the process within England's safety management program for HIT (94), which had evolved over 12 years with more than 2000 incidents. This is perhaps one of the most notable uses of safety cases in health care. For national scale systems, software manufacturers are required to create a safety case which sets out the evidence of how hazards have been identified and managed. This program has also implemented two standards for managing clinical risks in the design, implementation and use of HIT.(95,96) These standards are consistent with those for safety critical software (such as the International Electrotechnical Commission IEC 61508) and medical devices (such as the International Organisation for Standardisation ISO 14971), and were formally adopted as NHS standards in 2009. At Kaiser Permanente, processes had been operational since implementation of the electronic medication record (EMR) began in 2005.

7.4.3. Scope of review

It was outside the scope of this review to consider the effectiveness of which incident investigation practices were working best. There was a high degree of variability on program maturity and the extent to which strategies were used across the reviewed programs.

7.5. Themes emerging from interviews

7.5.1. Incident review part of broader HIT safety processes

Processes to investigate and review incidents were part of routine system operation and were closely linked with other safety processes in the technology life cycle. The majority of programs reported having processes to proactively assess and mitigate HIT-related hazards as part of the HIT system life cycle including design, build, implementation and use.

7.5.2. Detection via IT service desks

Most detection of HIT issues was via calls or reports to service desks. Incidents deemed by service desks to pose clinical risks were forwarded to dedicated patient safety teams for IT. Service desk staff were trained to identify issues that had an actual or potential impact on care delivery or patient safety, although such incidents could be explicitly identified by reporters. Some service desks were accredited – for example, Information Technology Infrastructure Library (ITIL) Service Operation version 3.

7.5.3. Triage based on severity, impact and previous occurrence

Severity assessment was based on local schemas. For example, the SAC was used in the US Department of Veterans Affairs. The impact of incidents, meaning the number of patients, users or systems impacted in the immediate setting, was considered in making this assessment. The potential for other users of the system in different settings was also examined. Only those with a high severity rating or with a high impact that have not been previously encountered underwent a detailed investigation. Those with known issues were reviewed to examine the effectiveness of previous controls and to investigate reasons for their failure.

7.5.4. Multidisciplinary expertise essential

In dedicated IT safety programs, review and investigation was undertaken by multidisciplinary teams. Where IT was investigated as part of mainstream patient safety processes, respondents emphasised the importance of having Informatics expertise present at the RCA table or close involvement in RCA processes. In one US health system that was highly computerised, the chief medical information officer (CMIO) participated in the weekly review of all safety incidents. This was considered to be essential to clearly identify the role of HIT because a new system could be wrongly blamed for other breakdowns in clinical work processes. Interviewees highlighted that procedures to audit and check HIT systems needed to be undertaken by an individual who understood the clinical context of use as well as the technical configuration of the system. In one organisation, the RCA process was supported by an application support team whose role was to confirm issues described in incident reports.

7.5.5. Vendors participated

Software vendors were reported to be active participants on investigative teams. In one program, the majority of patient safety issues were reported by vendors. These had either been identified through internal testing by the vendor or by another client. In another case,

vendors reportedly worked with the HIT safety team to build test scenarios to examine performance at system boundaries.

7.5.6. Quality of investigation highly dependent on team skills and experience

Interviewees emphasised the importance of team skills and experience in conducting investigations. In one US health system, team skills were developed by keeping the same team members for multiple investigations. The HIT safety team at the central office was responsible for training and supporting local teams in conducting RCAs. Attention to detail was highlighted as a key requirement.

7.5.7. Multiple data sources utilised

Interviewees emphasised the importance of leveraging all sources to detect, investigate and review incidents. Detection was based on reports from vendors, IT service desks, mainstream patient safety incident monitoring systems and proactive monitoring of HIT systems. Hazard registers were linked to HIT incident databases for triage and management of safety issues. For example, if the issue had been previously detected and had a control in place, the investigation would focus on the control and the reasons for its failure. Reviews of HIT service desk reports were also reported to be useful in proactively identifying issues that could pose risks. For example, one review of help desk tickets found that over 100 clinicians had reported an EHR safety feature to be confusing.

7.5.8. Event sequence replicated in actual system

Reconstruction of the sequence of user interactions and system transactions was fundamental to uncovering use errors and machine errors that may have contributed to adverse events. In addition to problems with the system user interface, this process was used to identify software issues that may have caused HIT to behave in an unexpected manner. Such analyses were used to examine the event timeline in the system as well as application settings and display. Potential solutions were also examined as part of this process. Access to a copy of the live system was thus essential to investigation. One national program maintained copies of all current versions of software so that solutions could be tested before they were deployed. In many cases this included representative databases such as anonymised versions of actual system databases.

7.5.9. Formal hazard assessment techniques seldom used

Four programs reported finding formal hazard assessment approaches such as root cause analysis and FMEA useful for investigating HIT incidents. The Healthcare Failure Mode and Effect Analysis (HFMEA) was used at the US Department of Veterans Affairs. Interviews reported using a range of different methods until root causes were uncovered. It was reported that compared to Aerospace, where systems were well-defined and procedures of operation were fixed, HIT systems had multiple interfaces, were not well-defined and there was a high degree of variability in the way there were used. Thus methods that had been developed for tightly bounded systems in Aerospace and other safety critical industries, where all possible hazards had been assessed as part of design, needed to be used in conjunction with other techniques as HIT hazards often related to issues not examined as part of proactive safety assessment processes.

7.5.10. Monitoring to support early detection

Monitoring, including the use of automated methods, was increasingly being seen as a way to overcome the limitations of current mechanisms, which are based on lagging indicators of safety and which largely rely on clinicians, consumers and vendors to detect and report

safety issues. Interviewees felt that automated methods were needed because many safety problems – particularly issues with data integrity and overlaid records – were harder to detect with increasing system complexity. This included regular audits of system transactions and system databases.

In one organisation, an audit of system transactions revealed a dramatic increase in the number of patients lost to follow-up. This was due to a system issue that had cancelled all future appointments when patients were discharged from hospital. In another hospital, an email follow-up of prescribers who had discontinued medications prescribed in error identified usability issues with the prescribing interface that had led to those prescribing errors. At the database level, audits detected the presence of duplicate patient records due to use errors; for example, new records were wrongly created when existing records could not be located in the system. Interviewees recommended continuous monitoring of a subset of databases and transactions where risks were high, such as alerts relating to high risk medications.

7.6. Chapter summary

- The investigation and review of HIT incidents occurs in context of the technology life cycle. Detection of safety problems, their investigation and review of aggregate patterns are part of routine system use, and are closely linked to processes undertaken to identify and address hazards during system design, build and implementation.
- As HIT safety overlaps the domains of patient safety and IT service management, detection, investigation and review need to be managed by a multidisciplinary team with skills in health informatics, HIT systems, clinical safety and systems safety engineering. For detailed investigations, informatics representation on the investigative team is essential.
- Replication of HIT system events leading to an adverse event is fundamental to detailed investigation.
- Given the complexity of HIT implementations formal hazard assessment techniques are seldom used. A range of different methods are used until root causes are identified.
- With increased system complexity, the use of automated methods to proactively monitor HIT systems has become essential for detection of safety problems using leading indicators.

8. Discussion: a proposed model to investigate and review HIT incidents

Based on our findings we propose a model for investigating and reviewing incidents in context of the technology life cycle, spanning design, build, implementation and use in a clinical setting (Figure 14). The model brings together key functions for learning from incidents including detection of safety problems, their investigation and review of aggregate patterns. These functions are part of routine system use, and are closely linked to processes undertaken to identify and address hazards during system design, build and implementation. As HIT safety overlaps the domains of patient safety and IT service management, these functions need to be managed by a multidisciplinary team with skills in health informatics, IT systems, clinical safety and systems safety engineering.

8.1. Detection

Early detection is critical to minimise disruptions to care delivery and to prevent patient harm. There are multiple ways to detect safety problems. As HIT services drive production, disruption to these services tends to have greater visibility with potential to significantly impact the delivery of care. In addition to incidents reported by clinicians and consumers to IT service desks and to mainstream patient safety incident monitoring systems, software vendors play a key role in proactively identifying safety problems, particularly issues with software that emerge as systems are developed and updated. For example, a vendor might issue a patch to fix an issue associated with upgrading the software operating system.

Safety problems can also be detected before they impact care delivery or patient safety. One way to do this is by proactively monitoring HIT systems using automated methods. There now is significant interest in automated methods because they can detect new emergent behaviours that only become evident after HIT systems, especially complex configurations with multiple disparate components are deployed in the real world. They can also detect software problems that may go undetected by users who are not expert in technology. Automated monitoring is possible at three levels to detect anomalies in the delivery and speed of message between HIT systems, the content of messages between HIT systems and user interactions with HIT systems.(47)

When incidents are detected, their severity is assessed using a local schema (such as the SAC). Only those with a high severity rating or with a high impact that have not been previously encountered undergo a detailed investigation. Those with known issues are reviewed to examine the effectiveness of previous controls and to investigate reasons for their failure. Similar models for recognising and responding to incidents have been developed at a national level for general patient safety (98), and these could provide guidance in the structure of such a system for HIT. Additionally, the scale of incidents – the number of users, patients or their records as well as their potential to occur in other similar contexts – needs to be considered. Unlike other risks to patient safety, IT incidents can, because of their scale and scope, increase the risk of harm to many patients from the delivery of health services. Consider, for example, the investigation of an incident in a general practice where a patient received the wrong medication and had seizures because sodium valproate modified release (m/r) 200mg was incorrectly mapped to sodium valproate 200mg in the drug database of the software system used to prescribe the medication. In addition to other patients in the practice, the potential for this problem to affect other practices using the same prescribing system and other prescribing systems using the same drug database also need to be considered as part of the process to assess severity.

8.2. Investigation

Safety emerges from the collective interactions among all system components, including technology, people, workflow, organisation and the external environment. The purpose of investigation is to examine interactions between system components so that the interactions leading to an incident and contributing factors can be uncovered. Methods such as the London Protocol and RCA can be used to systematically approach and undertake investigations. For HIT incidents, Sittig and Singh's Sociotechnical Model (34) can be used at the operational level to guide the selection of methods as it takes a systems view to safety grouping problems into eight broad dimensions (Table 6). Indeed many of the methods used to identify and mitigate hazards as part of system design and implementation may be used during investigation. Examples of these include the Failure Mode and Effect Analysis (FMEA), Fault Tree Analysis and Sociotechnical Probabilistic Risk Assessment (ST-PRA).

8.3. Aggregate review

Low- and medium-severity incidents are routinely reviewed to understand aggregate patterns. High-severity incidents may also undergo review periodically. For example, an organisation may aggregate RCA findings to find that HIT incidents mostly involve medications and most adverse events involve problems with the user interface, workflow and communication, and clinical content. There are many other sources of information about HIT problems that are amenable to aggregate review. These include mainstream incident monitoring, IT service desk reports, registers of equipment failure and hazards, medications reporting and malpractice claims. Current schemas to undertake such aggregate reviews include the AHRQ Hazard Manager Ontology (40), the Magrabi *et al.* classification (21) and Sittig and Singh's Sociotechnical Model.(34) As reports do not represent a systematic sample, they cannot be used to examine the frequency of safety problems. However, new aspects of known problems may come to light, and new, unforeseen problems may be identified for the first time, potentially allowing the timely application of remedial strategies at systemic as well as local levels.

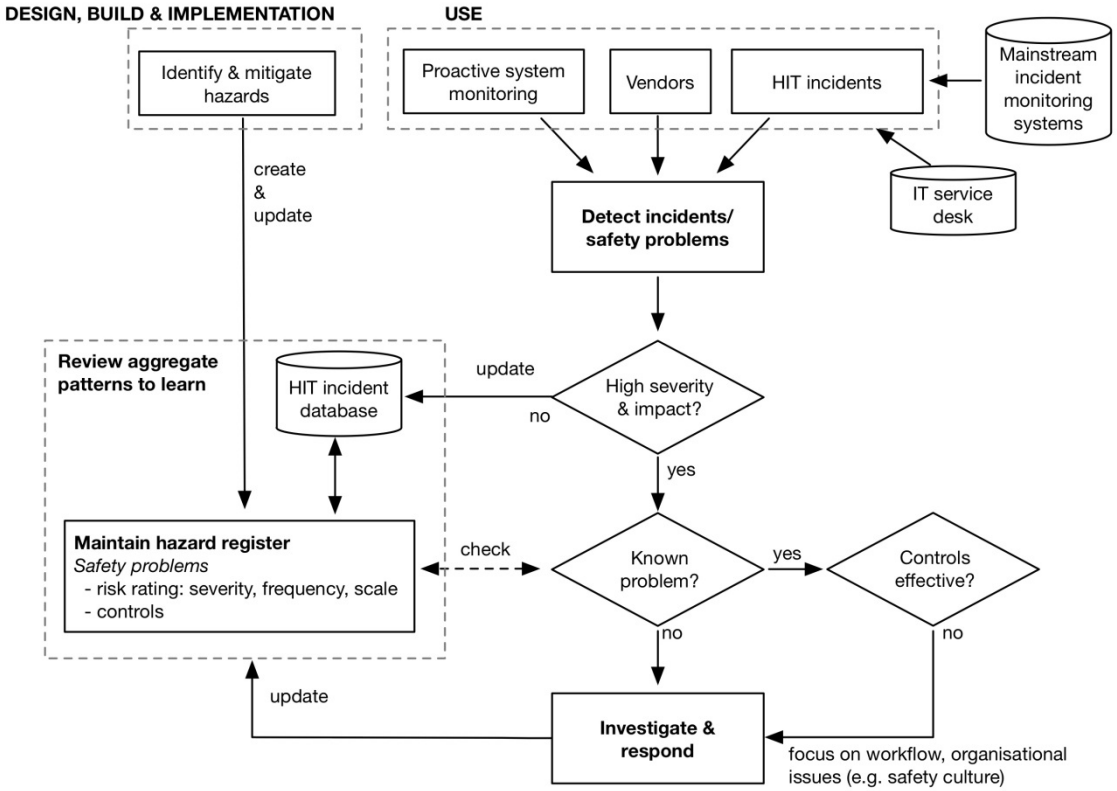


Figure 14. General model of processes to detect and manage incidents involving HIT systems in the context of the technology life cycle.

8.4. Maintain hazard register

The hazard register is integral to detection, investigation and aggregate review because it serves as a central repository of all known safety problems, their risks and controls. It is linked to the incident monitoring database and IT service database. For HIT, general purpose issues tracking software are commonly adapted to support the tracking of hazards throughout the system life cycle. The AHRQ Health IT Hazard Manager is an example of a purpose built tool.(40)

Table 6. Examples of methods and data sources to investigate the 8 dimensions of HIT safety, after.(34)

Dimension	Methods and data sources (example)
Hardware and software	• Computer logs (e.g. critical test results not accessed) • Replication of incident in IT system • IT system availability data including downtimes • IT problems logged by helpdesk • Design process and documentation
Clinical content	• Audit system configuration and settings (e.g. decision rules, settings for alerts, in-built order sets, user customisation)
Human–computer interface	• Heuristic usability inspection • Think Aloud protocol • Interviews about problems with using interface • FMEA • Simulation
People	• Surveys (e.g. safety culture) • Interviews including software vendors, teams responsible for system design, implementation and operation
Workflow and communication	• Participant observation • Communication logs • Handover sheets • FMEA • Simulation
Internal organisational features	• Policy and procedures vs. actual practice • IT access policy • Information governance (e.g. critical test result was only visible to ordering clinician)
External rules and regulations	• Documentation
Measurement	• Proactive system and user level monitoring

and monitoring	• Clinical process and outcome indicators (e.g. funnel plots to compare patterns)

9. Conclusion: an overview of findings

The aim of any Health Information Technology (HIT) safety system is to prevent harm from occurring associated with the system, and should such an event occur, to prevent its recurrence.

Proactive monitoring and testing of HIT systems requires teams with a blend of both technical and clinical expertise, well-resourced to explore the potential effect of new releases in simulated clinical environments. It is important to support and develop these activities, as clearly the identification of hazards has a major impact on ultimately preventing incidents and harm.

The retrospective investigation of incidents and system failures commences with an ability of users to detect issues, and then have access to a feasible reporting system that allows them to communicate and provide feedback about identified problems. Incident reporting and learning systems are more successful when reporters are engaged and involved at a local level with a strong, non-punitive reporting culture, and participate in the generation of solutions and feedback of findings from lessons learnt.(99,100) These systems should ideally operate at a local level and allow fast responses to any threats to patient safety, as well as having the ability to have their data aggregated at a regional and national level, so that specialist teams can conduct detailed analyses, identify recurrent issues, generate findings, and feed these back to all of the HIT system stakeholders with the aim of preventing a repetition of any safety threats to the system or its users.

Important consideration should be given to the design and positioning of local, regional and national incident data collection systems, and the composition of specialist groups to review, investigate and generate findings from the interrogation of both aggregated incident data, and in depth analyses of incidents such as those with a high potential for harm, or new events that were not able to be predicted with proactive monitoring and simulation testing. These various local, regional and national structures also need the ability to feedback to stakeholders in a timely manner and broadly disseminate the findings from lessons learnt in the incident analysis process.

There are limitations of the findings presented in this report, which aimed to present a detailed review of hazard and incident analysis methodologies relating to HIT. There are a number of important related areas which were beyond the scope of this piece, and further work is recommended to consider these other areas. For example, the methods associated with incident reporting and learning systems, and issues of engagement of users with these systems, including issues around anonymity, confidentiality and legal protections.

It is important also to consider the value of adequately investing in technical research and development as an adjunct to other approaches of ensuring the safety of complex HIT systems. Historical examples such as the large-scale failure of the London Ambulance System’s attempts to introduce a computerised system for receiving calls and dispatching crews highlight the importance of these factors, and the dangers of trying to implement high technology projects without adequate research to support its implementation.(102)

Numerous methods exist that may be used in combination to investigate system safety and incidents. There is no one method that will fit all of the requirements across the spectrum of proactive monitoring, retrospective analysis, aggregation of data, and development and dissemination of key findings. Each component of any safety system requires a tailored approach and should draw from a palette of multiple methods.

10. Appendix A: Summary of the 21 studies investigating HIT incidents

Authors (year)	Study period (mths)	Source/ case study	Country	Settings	HIT types	N	Harm, % (death, n)	Case study/ incident analyses methods R: reporting format HIT: problem categories C: consequences	Summary of findings
Horsky *et al.* (2005) (13)		case study	USA	inpatient	CPOE	1	1	- semi-structured interviews with involved clinicians - computer log analysis - usability inspection of CPOE interface - quality assurance reports - case & review notes by Significant Events Committee	An elderly patient suffering from hypokalemia or low potassium (serum potassium was 3.1 mEq/L; creatinine, 1.7) became severely hyperkalemic (serum potassium level, 7.8 mEq/L). Wrong, incomplete and missing information in the hospital order entry system resulted in the patient receiving multiple doses of potassium. In total, 316 mEq potassium chloride (KCl) was administered over 42 hours. Technical problems related to software functionality such as suboptimal screen display and lack of automated checking function. Human factors issues were linked with inadequate training and poor familiarity with the system.
Landman *et al.* (2013) (14)		case study	USA	inpatient	ED- Image viewer		N/A	computer log analysis	An update to Microsoft Internet Explorer severed the link between the ED tracking board and web-based image viewer. The loss of this link resulted in decreased web-based image viewer access rates for ED patients during the 10 days of the incident (2.8 views/study) compared with image review rates for a similar 10-day period preceding this event (3.8 views/study, $p<0.001$).

Authors (year)	Study period (mths)	Source/ case study	Country	Settings	HIT types	N	Harm, % (death, n)	Case study/ incident analyses methods R: reporting format HIT: problem categories C: consequences	Summary of findings
McDonald *et al.* (2006) (15)		case study	USA	inpatient	CPOE	1	-	- medical case history - root-cause analyses - interviews with involved patients and clinicians	Computerised bar-coding patient identification system was associated with a near miss. Human factor issues involved rule violation and integration with workflow such as missing verbal confirmation of patient identification and entering wrong information into a system.
Castro *et al.* (2016) (23)	2010-2013 (42)	Sentinel events to The Joint Commission	USA	inpatient, ambulatory	EHR, CPOE, eMAR, PIS, CDS, imaging, peripheral device, billing, AutoDisp, LIS	120	125^ (66)	**R**: voluntary reports + RCA findings **HIT**: 4 schemas -AHRQ Common Formats -AHRQ Hazard Manager ontology - Magrabi *et al.* classification - Sittig and Singh's sociotechnical model **C**: 15 categories of sentinel events	120 HIT-related sentinel events from 3,375 reported affecting 125 patients. Contributing factors were most frequently associated with the human-computer interface, workflow and communication, and clinical content–related issues. The three most frequently identified event types were (1) medication errors, (2) wrong-site surgery (including the wrong side, wrong procedure, and wrong patient), and (3) delays in treatment.
Cheung *et al.* (2013) (31)	2010-2011 (12)	Dutch central medication incidents registration (CMR)	The Netherlands	inpatient, outpatient pharmacy	CPOE, EHR, AutoDisp, PIS, Infusion pump, eMAR	668	58% (2)	**R:** CMR database **HIT**: - Magrabi *et al.* classification - phases of medication process **C**: reporter classified using CMR event types	Half of the incidents were associated with use error related wrong entry to the system. Technical problems related to poor design of screens were associated with the most incidents in community pharmacies for choosing the wrong medicine.

^actual number of patients harmed

Authors (year)	**Study period (mths)**	**Source/ case study**	**Country**	**Settings**	**HIT types**	**N**	**Harm, % (death, n)**	**Case study/ incident analyses methods** **R: reporting format** **HIT: problem categories** **C: consequences**	**Summary of findings**
Graber *et al.* (2015) (32)	2012-2013 (2)	Malpractice claims	USA	inpatient ambulatory emergency	EHR	248	80% (deaths noted but number not specified not specified)	**R:** CRICO claims database **HIT**: proprietary taxonomy to examine user and system-related sociotechnical factors **C**: reporter classified using CMR event types	58% machine-related 63% involving human factors issues
Lei *et al.* (2013) (19)	2001-2012 (142)	Online news articles and incident reports	China	inpatient, outpatient, general practice	All HIT	116	1 (1)	**R:** not structured **HIT**: IT risk model to examine hardware, software and loss of network connectivity **C**: ad hoc including scope of impact	66% of HIT outage incidents were associated with technical problems such as hardware and software malfunction. 36% of incidents affected more than 100 individuals, of these 9 incidents affected over 1000 individuals. 109 incidents resulted in delaying/cancelling of care. In 21 incidents, patients forced to seek care in other hospitals. One death was associated with HIT outage.
Magrabi *et al.* (2010) (26)	2003-2005 (24)	State-based patient safety incident reporting system	Australia	inpatient, general practice	All HIT	99	3 (none reported) *	**R**: voluntary AIMS reports **HIT**: Magrabi *et al.* classification **C**: reporter classified - AIMS event types - Severity Assessment Code (SAC)	117 HIT problems in 32 categories 55% machine-related, delays a major consequence 45% human-factors, rework major consequence

Authors (year)	**Study period (mths)**	**Source/ case study**	**Country**	**Settings**	**HIT types**	**N**	**Harm, % (death, n)**	**Case study/ incident analyses methods** **R: reporting format** **HIT: problem categories** **C: consequences**	**Summary of findings**
Magrabi *et al.* (2012) (16) & Magrabi *et al.* (2011) (33)	2008-2010 (30)	Equipment failure & hazards reported to the FDA	USA	inpatient	All HIT	436	11 (4)	**R**: voluntary reports to MAUDE **HIT**: Magrabi *et al.* classification **C**: AIMS event types	712 HIT problems in 36 categories 96% machine-related 4% involving human factors *Four deaths* *1/* Entry of a portable x-ray image into a PACS system under the wrong name resulted in a wrong diagnosis and subsequent intubation which may have contributed to death. 2/ A technician mistakenly entered the date of birth of a baby instead of the study date, making a chest x-ray appear older than it was. A radiologist subsequently viewed the image for peripherally inserted central catheter (PICC line) placement. Seeing that the comparison image did not have the line present, it was concluded that the line had been removed. Unfortunately, the line was placed too far in the infant, and the premature baby died. 3/ Orders were not executed and went undetected due to inadequate separation of pre-operative orders from post-operative resulting in a “missed opportunity to diagnose and treat life threatening disease, contributing to death. 4/ A CPOE user interface which did not provide medication doses in milligrams (mg) was associated with administration of three times the maximum dose of an analgesic drug in 24hrs. This resulted in acute renal failure and death.

Authors (year)	**Study period (mths)**	**Source/ case study**	**Country**	**Settings**	**HIT types**	**N**	**Harm, % (death, n)**	**Case study/ incident analyses methods** **R: reporting format** **HIT: problem categories** **C: consequences**	**Summary of findings**
Magrabi *et al.* (2015a) (17)	2005-2011 (74)	All safety events reported to national IT service desk	England	inpatient, outpatient, long-term care, pharmacy, general practice	All HIT	850	3 (3)	**R**: IT help desk Hewlett Packard Quality Centre **HIT**: Magrabi *et al.* classification **C**: AIMS event types, National Reporting and Learning System (NRLS) harm categories	1606 HIT problems 96% machine-related 4% involving human factors 24% impacted care delivery 4% were a near miss 23% were large-scale events. Human factors issues were over-represented in the events involving patient harm. *Three deaths* *1/* A patient who was seen with another patient's records in general practice was prescribed that patient's medication and died later the same day from taking it. No further details were available. 2/ A patient suffering from chest pain advised the receptionist in a GP surgery. The receptionist intended to alert the GP about this patient via the practice software, but sent the message to him or herself instead. The patient later died from a myocardial infarction. 3/ An HIV test ordered during hospital stay was not followed-up after dis- charge. When the patient was re-admitted, the admitting doctors were unable to access the HIV test result because the test request was hidden from them. The patient developed and died from pneumocystis pneumonia.

Authors (year)	**Study period (mths)**	**Source/ case study**	**Country**	**Settings**	**HIT types**	**N**	**Harm, % (death, n)**	**Case study/ incident analyses methods** **R: reporting format** **HIT: problem categories** **C: consequences**	**Summary of findings**
Magrabi *et al.* (2015b) (21)	2012-2013 (19)	Incident reporting study	Australia	general practice	All HIT	90	6 (none reported)	**R**: non-standard, TechWatch study protocol **HIT**: Magrabi *et al.* classification **C**: AIMS event types	42% of the incidents had an observable impact on the delivery of care but were not associated with patient harm. 27% of the incidents were a near miss. Problems with IT disrupted clinical workflow, wasted time, caused frustration and lead to use hybrid record system. Technical problems related to user interfaces, routine updates to software packages and drug databases, and the migration of records from one package to another generated clinical errors.
Meeks *et al.* (2014) (22)	2009-2013 (34)	Investigation of safety concerns	USA	inpatient, outpatient, long-term care	EHR	100	N/A	**R**: investigations completed by Informatics Patient Safety Office of the Veterans Health Administration **HIT**: - Sittig and Singh's sociotechnical model - phases of EHR implementation **C**: not examined	70% involved 2 or more sociotechnical dimensions 1. Hardware and software=76 2. Clinical content=38 3. Human-computer interface=29 4. People=20 5. Workflow and communication=35 6. Internal organizational features=6 7. External rules and regulations=2 8. System measurement and monitoring=1 Phase 1: unsafe technology or technology failures (74) Phase 2: unsafe or inappropriate use of technology (25) Phase 3: lack of monitoring of safety concerns (1)

Authors (year)	Study period (mths)	Source/ case study	Country	Settings	HIT types	N	Harm, % (death, n)	Case study/ incident analyses methods R: reporting format HIT: problem categories C: consequences	Summary of findings
Myers *et al.* (2011) (27)	1993-2010 (216)	Equipment failure & hazards reported to the FDA	USA	inpatient	All HIT	120	Patient harm including injury, disability and deaths noted but number not specified	**R**: investigations completed by Informatics Patient Safety Office of the Veterans Health Administration **HIT**: - Sittig and Singh's sociotechnical model - phases of EHR implementation **C**: not examined	12 technical problems related to software functionality and system downtime. Consequences reported including delays in diagnosis or treatments, unnecessary or emergency procedures and/or treatment.
Samaranayake *et al.* (2012) (103)	2006-2010 (60)	Hospital-based incident reporting system	Hong Kong	inpatient, outpatient	CPOE EHR AutoDisp,	243	11 (none reported)	**R**: ad hoc **HIT**: ad hoc **C**: reporter classified, local coding scheme	Most medication errors related to prescribing and were caused by human factors issues. While, most were detected before reaching the patient, 11% of medication errors reached the patient. 6.1% of the errors reached patients causing minor injury and temporary morbidity requiring intervention.
Santell *et al.* (2009) (28)	2001-2005 (54)	US Pharmacopeia, MEDMARX	USA	inpatient, outpatient, long-term care	CPOE	90,876	43 (3)	**R:** MEDMARX, Uni of Pittsburgh Medical Centre **HIT**: ad hoc **C**: reporter classified, National Coordinating Council for Medication Error Reporting and Prevention's (NCC MERP) Index for Categorizing Medication Errors.	Study focussed on medication errors in hybrid systems where manual systems were used in combination with CPOE to process medication orders. Use errors such as partial/omitted typing and rule violations were reported to be the leading cause of prescribing errors.

Authors (year)	**Study period (mths)**	**Source/ case study**	**Country**	**Settings**	**HIT types**	**N**	**Harm, % (death, n)**	**Case study/ incident analyses methods** **R: reporting format** **HIT: problem categories** **C: consequences**	**Summary of findings**
Schiff *et al.* (2015) (29)	2003-2010 (88)	US Pharmacopeia, MEDMARX	USA	inpatient, outpatient	CPOE	10,060	N/A	**R:** MEDMARX **HIT**: ad hoc **C**: not examined	Majority of CPOE related medication incidents were associated with use errors during completing prescribing orders. Human factors issues involved rule violation, lack of system and clinical knowledge, and communication issues. Technical problems related to system functionality, interface with other system, and hybrid systems.
Stewart *et al.* (2012) (104)	2005-2011 (82)	Hospital-based incident reporting system	Australia	inpatient	Radiology systems	21	N/A	**R:** Incident Information Management System (IIMS) **HIT**: WHO International Classification for Patient Safety (ICPS) **C**: not examined	Most of the HIT-related radiology incidents were associated with human-machine interaction, occurring at data entry, transferring, and output. Incidents also involved use error such as uploading wrong file and duplicated test orders.
Warm *et al.* (2012) (24)	2009-2011 (29)	State-based patient safety incident reporting system	UK	inpatient, outpatient, mental health, general practice	All HIT	149	34 (none reported)	**R:** National Reporting and Learning System (NRLS), Wales **HIT**: Magrabi *et al.* classification **C**: reporter classified using NRLS categories	77% linked to technical problems e.g. access issues, computer system down/too slow, display issues, and software malfunction. 10% involving human-machine interaction.
Zhan *et al.* (2006) (30)	2003 (8)	US Pharmacopeia, MEDMARX	USA	inpatient, outpatient	CPOE	7,029	5 (none reported)	**R**: MEDMARX **HIT**: ad hoc **C**: National Coordinating Council for Medication	Technical problems related to faulty computer interface, miscommunication with other systems and inadequate decision support. Human factors issues involved knowledge deficit, distractions, inexperience and data entry errors.

Authors (year)	Study period (mths)	Source/ case study	Country	Settings	HIT types	N	Harm, % (death, n)	Case study/ incident analyses methods R: reporting format HIT: problem categories C: consequences	Summary of findings
								Error Reporting and Prevention's (NCC MERP) Index for Categorizing Medication Errors.	
ECRI Institute (20)	2012 (1.5)	Incident reporting study - Deep Dive	USA	36 inpatient and outpatient settings	EHR, CPOE, eMAR, PIS, CDS, imaging, peripheral device, billing, AutoDisp, LIS	171	6 (3)	**R**: AHRQ's Common Formats (version 1.2) **HIT**: Magrabi *et al.* classification **C**: reporter classified using National Coordinating Council for Medication Error Reporting and Prevention's (NCC MERP) Index for Categorizing Medication Errors.	211 HIT problems in 28 categories 56% machine-related 44% human-factors issues A (circumstance that has the capacity to cause harm): 25, 15% B (error occurs but does not reach the patient): 15, 9% C (error reaches the patient but does not cause harm): 52, 30% D (error reaches the patient and requires monitoring to confirm no harm and/or intervention required): 24, 14% E (error contributes to or results in temporary harm to the patient and requires intervention): 3, 2% F (error contributes to or results in temporary harm and requires initial or prolonged hospitalization): 1, 1% G (error contributes to or results in permanent patient harm): 0, 0% H (error requires intervention to sustain life): 1, 1% I (error may have contributed to or resulted in patient's death): 3, 2%

Authors (year)	Study period (mths)	Source/ case study	Country	Settings	HIT types	N	Harm, % (death, n)	Case study/ incident analyses methods R: reporting format HIT: problem categories C: consequences	Summary of findings
Pennsylvania Patient Safety Authority (25)	2012	State-based patient safety incident reporting system	USA	inpatient, outpatient	EHR	3,099	0% (1)	**R**: Pennsylvania Patient Safety Reporting System (PA-PSRS). **HIT**: Magrabi *et al.* classification **C**: reporter classified using National Coordinating Council for Medication Error Reporting and Prevention's (NCC MERP) Index for Categorizing Medication Errors.	Majority of EHR-related reports involved errors in human data entry, such as entry of "wrong" data or the failure to enter data, and a few reports indicated technical failures on the part of the EHR system. Incident: Unsafe Conditions (A)= 320, 10% Incident: No Harm (B1-D) =2763, 89% Serious Event: Temporary Harm (E-F)=15, 0% Serious Event: Significant Harm (G-I)= 1, 0%

*consequences were available for 68 incidents.

Abbreviations: HIT: health information technology; Observ: Observational study ; CPOE: computerised provider order entry; EHR: electronic health record; ePS: electronic prescribing system; CDS: clinical decision support; ADS: automated dispensing system; AutoDisp: automated dispensation of medication; eMAR electronic medication administration record; AED: automated error detection system; PIC: Pharmacy information system; LIS: laboratory information system.

11. Appendix B: Summary of classifications used to examine problems with HIT

Authors (year)	AHRQ Common Formats	AHRQ Hazard Manager	Magrabi *et al.* classification	Sittig and Singh's sociotechnical model	Ad hoc categories	Other
Castro *et al.* (2016) (23)	x	x	x	x		
Cheung *et al.* (2013) (31)			x			medication phases
Graber *et al.* (2015) (32)						proprietary taxonomy of sociotechnical factors
Lei *et al.* (2013) (19)						IT risk model
Magrabi *et al.* (2010) (26)			x			
Magrabi *et al.* (2012) (16) & Magrabi *et al.* (2011) (33)			x			
Magrabi *et al.* (2015a) (17)			x			
Magrabi *et al.* (2015b) (21)			x			
Meeks *et al.* (2014) (22)				x		
Myers *et al.* (2011) (27)			x			
Samaranayake *et al.* (2012) (103)					x	
Santell *et al.* (2009)					x	
Schiff *et al.* (2015)					x	
Stewart *et al.* (2012)						AIMS event types

Warm *et al.* (2012)			x			
Zhan *et al.* (2006)					x	
ECRI Institute (2012)			x			
Pennsylvania Patient Safety Authority (2012)			x			

12. Appendix C: List of interviewees

Interviews were conducted in June 2016. In total, 10 key informants were interviewed individually or as a team about their organisational process for investigating IT incidents.

Organisation	**Position of interviewee/s**
1. Health & Social Care Information Centre	Head Of Safety Engineering Clinical Safety/Solution Assurance Operational & Assurance Services
2. Taunton and Somerset NHS Foundation Trust	IT Clinical Safety Lead & ePMA Programme Manager EPR programme
3. ECRI Institute & Pennsylvania Patient Safety Authority	Director, Patient Safety Reporting Programs Medical Director, Patient Safety, Quality, and Risk Group
4. Department of Veterans Affairs	Director of Informatics and Patient Safety VA Office of Informatics and Analytics/Health Informatics.
5. Kaiser Permanente	KP Healthconnect PART Team Manager
6. Memorial Hermann Health System, Texas	former Chief Medical Information Officer
7. Brigham and Women's Hospital	Scientist
8. Alfred Health, Melbourne	Director, Clinical Governance
9. NEHTA Clinical Safety Unit	CSU team, NEHTA
10. ACSQHC Clinical Safety Consultant	Director Health, Ageing and Human Services Sector KPMG

13. Appendix D: Interview schedule

Use of HIT

1. How many patients does your organisation look after? (e.g. 600-bed hospital, 10 hospital health system)_____

2. Indicate the level of HIT use within your organisation
   - 100% electronic
   - 50%, list departments/systems not covered_____
   - <50%, list departments/systems not covered_____

3. Indicate the nature of clinical systems:
   - Home-grown
   - Commercial
   - Combination:___% home-grown;___% commercial

4. Do you have a shared electronic medical records system? (i.e. EMR is shared with external providers such as ambulatory care/GP/family physician)
   - Yes
   - No

5. Indicate which patient engagement tools are currently in use:
   - patient portal
   - shared EHR/PHR
   - smartphone applications
   - email
   - interactive kiosks

6. How do you approach HIT safety in your organisation? (e.g. there is an HIT safety governance approach/framework within which the incident investigation process operates)

7. How does HIT safety relate to broader governance processes for patient safety? (e.g. HIT safety is integrated with patient safety processes or it is separate)

Incident investigation process

8. What is the process to investigate patient safety incidents within your organisation? Please describe the process from initiation to closure. Are HIT incidents treated differently in any way?

9. Do you use any formal techniques such as the London Protocol, RCA, FMEA, Fault Tree Analysis?

10. If not covered, how do you:

- Establish what has gone wrong
- Identify events that may have triggered the incident
- Understand order of events (incl. reconstruct sequence of events that led to the HIT incident)
- Confirm impact (number & range of users)
- Searches of knowledge base and previous incidents

11. What sources of information do you use to reconstruct the events leading to an HIT incident (e.g. logs of software, content of files/database, screen shots etc.)?

12. Have you developed any tools or templates to support the process?

13. If yes, can you provide us with a copy of documentation?

14. Does the process comply with any particular standard or policy? (e.g. local, national, jurisdictional policy directive)

15. If yes, can you provide us with a copy of documentation?

16. Who is on the incident investigation team? (size and skill mix)

17. What is the role of vendors in the investigation and diagnosis of incidents?

Descriptive statistics and effectiveness of process

18. For how long has the incident investigation process been operational?

19. What is the total number of HIT incidents managed by this process? Any patient harms? (including main incident types associated with harm)

20. Can you comment on the effectiveness of your process? What are three things that can be improved or changed?

14. Abbreviations

Abbreviation	Definition
ACSQHC	Australian Commission on Safety and Quality in Health Care
ADS	Automated dispensing system
ADHA	Australian Digital Health Agency
AED	Automated error detection system
AHRQ	Agency for Healthcare Research and Quality
AIMS	Advanced Incident Management System
CAST	Commercial Aviation Safety Team
CCA	Compliance, Conformance and Accreditation
CDP	Care Delivery Problems
CDS	Clinical decision support
CMIO	Chief Medical Information Officer
CMS	Centers for Medicare & Medicaid Services
CPOE	Computerised provider order entry
CSOC	Clinical Safety Oversight Committee
CSU	Clinical Safety Unit
DHS	Department of Human Services
EHR	Electronic Health Record
eMAR	Electronic medication administration record
EMR	Electronic Medication Record
ePS	Electronic proscribing system
FDA	Food and Drug Administration
FMEA	Failure Modes and Effects Analysis
HFACS	Human Factors Analysis and Classification System
HFMEA	Healthcare Failure Mode and Effect Analysis
HIPAA	Health Insurance Portability and Accountability Act of 1996
HIT	Health Information Technology
HITS	Health Information Technology Safety
ICPS	International Classification for Patient Safety
IT	Information technology
ITIL	Information Technology Infrastructure Library
LIS	Laboratory information system

NASH	National Authentication Service for Health
NCC MERP	National Coordinating Council for Medication Error Reporting and Prevention
NEHTA	National eHealth Transition Authority
NHS	National Health Service
NIO	National Infrastructure Operator
NPDR	National Prescription and Dispense Repository
NRLS	National Reporting and Learning System
OA	Opportunity Analysis
PA-PSRS	Pennsylvania Patient Safety Reporting System
PIC	Pharmacy information system
RCA	Root Cause Analysis
ROI	Return on investment
SAC	Severity Assessment Code
SO	System Operator
ST-PRA	Sociotechnical Probabilistic Risk Assessment
WHO	World Health Organisation

15. References

1. Australian Government Department of Health. Welcome to My Health Record [Available from: https://myhealthrecord.gov.au/internet/mhr/publishing.nsf/content/home.
2. Donaldson L. When will health care pass the orange-wire test? Lancet. 2004;364(9445):1567-8.
3. Vincent C, Amalberti R. Safer Healthcare: Strategies for the Real World 2016. Available from: http://www.springer.com/gp/book/9783319255576.
4. Ericson CA. Hazard analysis techniques for system safety. Second edition. ed. Hoboken, New Jersey: Wiley; 2016. xxiii, 616 pages p.
5. Waterson PE, Jenkins DP, editors. Lessons learnt from using AcciMaps and the risk management framework to analyse large-scale systemic failures. The International Conference on Contemporary Ergonomics and Human Factors 2011; 2011; London: Taylor and Francis.
6. Leveson N, Samost A, Dekker S, Finkelstein S, Raman J. A Systems Approach to Analyzing and Preventing Hospital Adverse Events. Journal of patient safety. 2016.
7. Ladkin P. The Why-Because Analysis Homepage Bielefeld University Faculty of Technology2012 [Available from: http://www.rvs.uni-bielefeld.de/research/WBA/.
8. Qureshi Z. A Review of accident modeling approaches for complex sociotechnical systems. In: Cant T, editor. Australian Computer Society, Inc 12th Australian Workshop on Safety Related Programmable Systems (SCS'07); Adelaide: Conferences in Research and Practice in Information Technology; 2007.
9. Cleland G, Habli I, Medhurst J, Sujan M-A. Evidence: Using safety cases in industry and healthcare. London: Health Foundation; 2012. Available from: http://www.health.org.uk/sites/health/files/UsingSafetyCasesInIndustryAndHealthcare.pdf.
10. Sujan MA, Habli I, Kelly TP, Pozzi S, Johnson CW. Should healthcare providers do safety cases? Lessons from a cross-industry review of safety case practices. Safety Science. 2016(84):181-9.
11. Stavert-Dobson A. Health Information Systems- Managing Clinical Risk. Switzerland: Springer; 2016 [cited 2016. Available from: http://download.springer.com/static/pdf/974/bok%3A978-3-319-26612-1.pdf?originUrl=http%3A%2F%2Flink.springer.com%2Fbook%2F10.1007%2F978-3-319-26612-1&token2=exp=1475817427~acl=%2Fstatic%2Fpdf%2F974%2Fbok%3A978-3-319-26612-1.pdf%3ForiginUrl%3Dhttp%3A%2F%2Flink.springer.com%2Fbook%2F10.1007%2F978-3-319-26612-1*~hmac=711d527a50a50e8e93570e3b8fbf5cb7a63248b5466552f7db377a9bb4ce8424.
12. Victorian Health Incident Management System [Available from: https://www2.health.vic.gov.au/hospitals-and-health-services/quality-safety-service/clinical-risk-management/investigation-of-incidents/investigations-responsibilities.
13. Horsky J, Kuperman GJ, Patel VL. Comprehensive analysis of a medication dosing error related to CPOE. J Am Med Inform Assoc. 2005;12(4):377-82.
14. Landman AB, Takhar SS, Wang SL, Cardoso A, Kosowsky JM, Raja AS, et al. The hazard of software updates to clinical workstations: a natural experiment. J Am Med Inform Assoc. 2013;20(e1):e187-90.
15. McDonald CJ. Computerization can create safety hazards: a bar-coding near miss. Ann Intern Med. 2006;144(7):510-6.
16. Magrabi F, Ong MS, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc. 2012;19(1):45-53.

17. Magrabi F, Baker M, Sinha I, Ong MS, Harrison S, Kidd MR, et al. 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. 2015;84(3):198-206.
18. Dudzinski DM, Hebert PC, Foglia MB, Gallagher TH. The disclosure dilemma--large-scale adverse events. The New England journal of medicine. 2010;363(10):978-86.
19. Lei J, Guan P, Gao K, Lu X, Chen Y, Li Y, et al. Characteristics of health IT outage and suggested risk management strategies: an analysis of historical incident reports in China. International journal of medical informatics. 2014;83(2):122-30.
20. DeepDive™ on Health Information Technology-related safety events, ECRI Institute Patient Safety
Organization, December 2012.
21. Magrabi F, Liaw T, Arachi D, Runciman WB, Coiera E, Kidd MR. Identifying patient safety problems associated with Information Technology in general practice: an analysis of incident reports. BMJ Qual Saf. (published online 5 Nov 2015).
22. Meeks DW, Smith MW, Taylor L, Sittig DF, Scott JM, Singh H. An analysis of electronic health record-related patient safety concerns. J Am Med Inform Assoc. 2014;21(6):1053-9.
23. Castro GM, Buczkowski L, Hafner JM. The Contribution of Sociotechnical Factors to Health Information Technology-Related Sentinel Events. Jt Comm J Qual Patient Saf. 2016;42(2):70-9.
24. Warm D, Edwards P. Classifying Health Information Technology patient safety related incidents - an approach used in Wales. Applied clinical informatics. 2012;3(2):248-57.
25. The Role of the Electronic Health Record in Patient Safety Events, Pennsylvania Patient Safety Advisory Vol. 9, No.4 December 2012.
26. Magrabi F, Ong MS, Runciman W, Coiera E. An analysis of computer-related patient safety incidents to inform the development of a classification. J Am Med Inform Assoc. 2010;17(6):663-70.
27. Myers RB, Jones SL, Sittig DF. Review of Reported Clinical Information System Adverse Events in US Food and Drug Administration Databases. Applied clinical informatics. 2011;2:63-74.
28. Santell JP, Kowiatek JG, Weber RJ, Hicks RW, Sirio CA. Medication errors resulting from computer entry by nonprescribers. Am J Health Syst Pharm. 2009;66(9):843-53.
29. Schiff GD, Amato MG, Eguale T, Boehne JJ, Wright A, Koppel R, et al. Computerised physician order entry-related medication errors: analysis of reported errors and vulnerability testing of current systems. BMJ quality & safety. 2015;24(4):264-71.
30. Zhan C, Hicks RW, Blanchette CM, Keyes MA, Cousins DD. Potential benefits and problems with computerized prescriber order entry: analysis of a voluntary medication error-reporting database. Am J Health Syst Pharm. 2006;63(4):353-8.
31. Cheung KC, van der Veen W, Bouvy ML, Wensing M, van den Bemt PM, de Smet PA. Classification of medication incidents associated with information technology. J Am Med Inform Assoc. 2013.
32. Graber ML, Siegal D, Riah H, Johnston D, Kenyon K. Electronic Health Record-Related Events in Medical Malpractice Claims. Journal of patient safety. 2015.
33. Magrabi F, Ong MS, Runciman W, Coiera E. Patient safety problems associated with heathcare information technology: an analysis of adverse events reported to the US Food and Drug Administration. AMIA Annual Symposium proceedings / AMIA Symposium AMIA Symposium. 2011;2011:853-7.
34. Sittig DF, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. Qual Saf Health Care. 2010;19 Suppl 3:i68-74.

35. Sittig DF, Singh H. Electronic health records and national patient safety goals. The New England journal of medicine. 2012;367(19):1854-60.
36. Runciman W, Hibbert P, Thomson R, Van Der Schaaf T, Sherman H, Lewalle P. Towards an International Classification for Patient Safety: key concepts and terms. International journal for quality in health care : journal of the International Society for Quality in Health Care / ISQua. 2009;21(1):18-26.
37. Sherman H, Castro G, Fletcher M, Hatlie M, Hibbert P, Jakob R, et al. Towards an International Classification for Patient Safety: the conceptual framework. International journal for quality in health care : journal of the International Society for Quality in Health Care / ISQua. 2009;21(1):2-8.
38. Sittig DF, Singh H. Defining health information technology-related errors: new developments since to err is human. Archives of internal medicine. 2011;171(14):1281-4.
39. Agency for Healthcare Research and Quality. Common formats. Rockville, Maryland: US Department of Health and Human Services [Available from: http://www.pso.ahrq.gov/common.
40. Walker JM, Agency for Healthcare Research and Quality. Health Information Technology Hazard Manager (Pennsylvania) Pennsylvania, USA2012 [Available from: healthit.ahrq.gov/ahrq-funded-projects/health-information-technology-hazard-manager.
41. Walker JM, Hassol A, Bradshaw B, Rezaee ME. Health IT Hazard Manager Beta-Test: Final Report. (Prepared by Abt Associates and Geisinger Health System, under Contract No. HHSA290200600011i, #14). AHRQ Publication No. 12-0058-EF. Rockville, MD: Agency for Health care Research and Quality. May 2012. .
42. NHS. National Patient Safety Agency Patient Safety Incident Data 2012 [Available from: http://www.npsa.nhs.uk.
43. Makeham MA, Kidd MR, Saltman DC, Mira M, Bridges-Webb C, Cooper C, et al. The Threats to Australian Patient Safety (TAPS) study: incidence of reported errors in general practice. The Medical journal of Australia. 2006;185(2):95-8.
44. Runciman WB, Williamson JA, Deakin A, Benveniste KA, Bannon K, Hibbert PD. An integrated framework for safety, quality and risk management: an information and incident management system based on a universal patient safety classification. Qual Saf Health Care. 2006;15 Suppl 1:i82-90.
45. Singh H, Sittig DF. Measuring and improving patient safety through health information technology: The Health IT Safety Framework. BMJ quality & safety. 2016;25(4):226-32.
46. Sittig DF, Ash JS, Singh H. The SAFER guides: empowering organizations to improve the safety and effectiveness of electronic health records. Am J Manag Care. 2014;20(5):418-23.
47. Coiera E. Guide to health informatics, third edition. Boca Raton, FL, USA: CRC Press, Taylor & Francis Group; 2015.
48. Kim MO, Coiera E, Magrabi F. Problems with health information technology and their effects on care delivery and patient outcomes: A systematic review. under review.
49. Nicolini D, Waring J, Mengis J. Policy and practice in the use of root cause analysis to investigate clinical adverse events: mind the gap. Social science & medicine (1982). 2011;73(2):217-25.
50. Nicolini D, Waring J, Mengis J. The challenges of undertaking root cause analysis in health care: a qualitative study. Journal of health services research & policy. 2011;16 Suppl 1:34-41.
51. Woloshynowych M, Rogers S, Taylor-Adams S, Vincent C. The investigation and analysis of critical incidents and adverse events in healthcare. Health Technol Assess. 2005;9(19):1-143, iii.

52. Percarpio KB, Watts BV, Weeks WB. The effectiveness of root cause analysis: what does the literature tell us? Jt Comm J Qual Patient Saf. 2008;34(7):391-8.
53. National Patient Safety Foundation. RCA2 - Improving Root Cause Analyses and Actions to Prevent Harm. Boston: NPSF, 2015.
54. Diller T, Helmrich G, Dunning S, Cox S, Buchanan A, Shappell S. The Human Factors Analysis Classification System (HFACS) applied to health care. American journal of medical quality : the official journal of the American College of Medical Quality. 2014;29(3):181-90.
55. Tamuz M, Thomas EJ, Franchois KE. Defining and classifying medical error: lessons for patient safety reporting systems. Qual Saf Health Care. 2004;13(1):13-20.
56. Pham JC, Kim GR, Natterman JP, Cover RM, Goeschel CA, Wu AW, et al. ReCASTing the RCA: an improved model for performing root cause analyses. American journal of medical quality : the official journal of the American College of Medical Quality. 2010;25(3):186-91.
57. Iedema R, Jorm C, Braithwaite J. Managing the scope and impact of root cause analysis recommendations. Journal of health organization and management. 2008;22(6):569-85.
58. Wu AW, Lipshutz AK, Pronovost PJ. Effectiveness and efficiency of root cause analysis in medicine. Jama. 2008;299(6):685-7.
59. Braithwaite J, Westbrook MT, Mallock NA, Travaglia JF, Iedema RA. Experiences of health professionals who conducted root cause analyses after undergoing a safety improvement programme. Qual Saf Health Care. 2006;15(6):393-9.
60. Latino RJ. How is the effectiveness of root cause analysis measured in healthcare? Journal of healthcare risk management : the journal of the American Society for Healthcare Risk Management. 2015;35(2):21-30.
61. Hettinger AZ, Fairbanks RJ, Hegde S, Rackoff AS, Wreathall J, Lewis VL, et al. An evidence-based toolkit for the development of effective and sustainable root cause analysis system safety solutions. Journal of healthcare risk management : the journal of the American Society for Healthcare Risk Management. 2013;33(2):11-20.
62. Card AJ, Ward J, Clarkson PJ. Successful risk assessment may not always lead to successful risk control: A systematic literature review of risk control after root cause analysis. Journal of healthcare risk management : the journal of the American Society for Healthcare Risk Management. 2012;31(3):6-12.
63. Middleton S, Chapman B, Griffiths R, Chester R. Reviewing recommendations of root cause analyses. Australian health review : a publication of the Australian Hospital Association. 2007;31(2):288-95.
64. Carroll JS, Rudolph JW, Hatakenaka S. Lessons learned from non-medical industries: root cause analysis as culture change at a chemical plant. Qual Saf Health Care. 2002;11(3):266-9.
65. Gosbee J, Anderson T. Human factors engineering design demonstrations can enlighten your RCA team. Qual Saf Health Care. 2003;12(2):119-21.
66. Ursprung R, Gray J. Random safety auditing, root cause analysis, failure mode and effects analysis. Clinics in perinatology. 2010;37(1):141-65.
67. Grissinger M. Building patient-safety skills: avoiding pitfalls in conducting a root cause analysis. P & T : a peer-reviewed journal for formulary management. 2013;38(12):728-9.
68. Weiss AP. Quality improvement in healthcare: the six ps of root-cause analysis. The American journal of psychiatry. 2009;166(3):372; author reply -3.

69. Slakey DP, Simms ER, Rennie KV, Garstka ME, Korndorffer JR, Jr. Using simulation to improve root cause analysis of adverse surgical outcomes. International journal for quality in health care : journal of the International Society for Quality in Health Care / ISQua. 2014;26(2):144-50.
70. Simms ER, Slakey DP, Garstka ME, Tersigni SA, Korndorffer JR. Can simulation improve the traditional method of root cause analysis: a preliminary investigation. Surgery. 2012;152(3):489-97.
71. Boyd M. A method for prioritizing interventions following root cause analysis (RCA): lessons from philosophy. Journal of evaluation in clinical practice. 2015;21(3):461-9.
72. Iedema RA, Jorm C, Braithwaite J, Travaglia J, Lum M. A root cause analysis of clinical error: confronting the disjunction between formal rules and situated clinical activity. Social science & medicine (1982). 2006;63(5):1201-12.
73. Pronovost PJ, Martinez EA, Rodriguez-Paz JM. Removing "orange wires": surfacing and hopefully learning from mistakes. Intensive Care Med. 2006;32(10):1467-9.
74. Taylor-Adams S, Vincent C. Systems Analysis of Clinical Incidents: The London Protocol. London: Imperial College, London, 2004.
75. Reason JT. The human factor in medical accidents. In: C.A V, editor. Medical Accidents Oxford. Oxford: Oxford Medical Publications; 1993.
76. Cronin CM. Five years of learning from analysis of clinical occurrences in pediatric care using the London Protocol. Healthcare quarterly (Toronto, Ont). 2006;9 Spec No:16-21.
77. Institute for Healthcare Improvement. Failure Modes and Effects Analysis (FMEA). 2004.
78. VA National Center for Patient Safety (NCPS). Healthcare Failure Mode and Effects Analysis (HFMEA) [Available from: http://www.whaqualitycenter.org/Portals/0/Tools to Use/Collecting Data and Information/HFMEA Steps.pdf.
79. Habraken MM, Van der Schaaf TW, Leistikow IP, Reijnders-Thijssen PM. Prospective risk analysis of health care processes: a systematic evaluation of the use of HFMEA in Dutch health care. Ergonomics. 2009;52(7):809-19.
80. Wetterneck TB, Hundt AS, Carayon P. FMEA team performance in health care: A qualitative analysis of team member perceptions. Journal of patient safety. 2009;5(2):102-8.
81. Shebl NA, Franklin BD, Barber N. Is failure mode and effect analysis reliable? Journal of patient safety. 2009;5(2):86-94.
82. Dean Franklin B, Shebl NA, Barber N. Failure mode and effects analysis: too little for too much? BMJ quality & safety. 2012;21(7):607-11.
83. Paparella S. Failure mode and effects analysis: a useful tool for risk identification and injury prevention. Journal of emergency nursing: JEN : official publication of the Emergency Department Nurses Association. 2007;33(4):367-71.
84. Ashley L, Armitage G, Neary M, Hollingsworth G. A practical guide to failure mode and effects analysis in health care: making the most of the team and its meetings. Jt Comm J Qual Patient Saf. 2010;36(8):351-8.
85. Shebl NA, Franklin BD, Barber N. Failure mode and effects analysis outputs: are they valid? BMC health services research. 2012;12:150.
86. Shebl N, Franklin B, Barber N, Burnett S, Parand A. Failure Mode and Effects Analysis: views of hospital staff in the UK. Journal of health services research & policy. 2012;17(1):37-43.
87. Yang F, Cao N, Young L, Howard J, Logan W, Arbuckle T, et al. Validating FMEA output against incident learning data: A study in stereotactic body radiation therapy. Medical physics. 2015;42(6):2777-85.

88. Krouwer JS. An improved failure mode effects analysis for hospitals. Archives of pathology & laboratory medicine. 2004;128(6):663-7.
89. McElroy LM, Khorzad R, Nannicelli AP, Brown AR, Ladner DP, Holl JL. Failure mode and effects analysis: a comparison of two common risk prioritisation methods. BMJ quality & safety. 2016;25(5):329-36.
90. Senders JW. FMEA and RCA: the mantras of modern risk management. Qual Saf Health Care. 2004;13(4):249-50.
91. Marx DA, Slonim AD. Assessing patient safety risk before the injury occurs: an introduction to sociotechnical probabilistic risk modelling in health care. Qual Saf Health Care. 2003;12 Suppl 2:ii33-8.
92. Herzer KR, Rodriguez-Paz JM, Doyle PA, Flint PW, Feller-Kopman DJ, Herman J, et al. A practical framework for patient care teams to prospectively identify and mitigate clinical hazards. Jt Comm J Qual Patient Saf. 2009;35(2):72-81.
93. Nielsen DS, Dieckmann P, Mohr M, Mitchell AU, Ostergaard D. Augmenting health care failure modes and effects analysis with simulation. Simulation in healthcare : journal of the Society for Simulation in Healthcare. 2014;9(1):48-55.
94. Baker M, Harrison I, Gray M. Safer IT in a Safer H+NHS: account of a partnership. The British Journal of Healthcare Computing & Information Management. 2006;23(7):11-4.
95. NHS Digital. SCCI0160 Clinical Risk Management: its Application in the Deployment and Use of Health IT Systems 2013 [3:[Available from: http://digital.nhs.uk/isce/publication/SCCI0160.
96. Digital N. SCCI0129 Clinical Risk Management: its Application in the Manufacture of Health IT Systems 2013 [Available from: http://digital.nhs.uk/isce/publication/scci0129.
97. High-Level System Architecture PCEHR System version 1.35 November: National E-Health Transition Authority. 2011.
98. Hibbert PD, Healey F, Lamont T, Marela WM, Warner B, Runciman WB. Patient safety's missing link: using clinical expertise to recognize, respond to and reduce risks at a population level. International journal for quality in health care : journal of the International Society for Quality in Health Care / ISQua. 2015.
99. Carson-Stevens A, Hibbert P, Avery A, Butlin A, Carter B, Cooper A, et al. A cross-sectional mixed methods study protocol to generate learning from patient safety incidents reported from general practice. BMJ open. 2015;5(12):e009079.
100. Zwart DL, Van Rensen EL, Kalkman CJ, Verheij TJ. Central or local incident reporting? A comparative study in Dutch GP out-of-hours services. The British journal of general practice : the journal of the Royal College of General Practitioners. 2011;61(584):183-7.
101. Makeham M, Pont L, Prgomet M, Carson-Stevens A, Lake R, Purdy H, et al. Patient safety in primary healthcare: a review of the literature The Sax Institute and the Australian Commission on Safety and Quality in Health Care, 2015.
102. Hougham M. London Ambulance Service computer-aided despatch system. International Journal of Project Management. 1996;14(2):103-10.
103. Samaranayake NR, Cheung ST, Chui WC, Cheung BM. Technology-related medication errors in a tertiary hospital: a 5-year analysis of reported medication incidents. International journal of medical informatics. 2012;81(12):828-33.
104. Stewart MJ, Georgiou A, Hordern A, Dimigen M, Westbrook JI. What do radiology incident reports reveal about in-hospital communication processes and the use of health information technology? Stud Health Technol Inform. 2012;178:213-8.

AUSTRALIAN COMMISSION
ON SAFETY AND QUALITY IN HEALTH CARE

Level 5, 255 Elizabeth Street, Sydney NSW 2000
GPO Box 5480, Sydney NSW 2001

Phone: (02) 9126 3600
Fax: (02) 9126 3613

Email: mail@safetyandquality.gov.au
Website: www.safetyandquality.gov.au