The effects and preventability of 2627 patient safety incidents related to health information technology failures: a retrospective analysis of 10 years of incident reporting in England and Wales

Guy Martin, Saira Ghafur, Isabella Cingolani, Joshua Symons, Dominic King, Sonal Arora, Ara Darzi

Lancet Digital Health 2019; 1: e127–35

See Comment page e104

National Institutes of Health Research Patient Safety Translational Research Centre, St Mary's Hospital, Imperial College London, London, UK (G Martin PhD, D King PhD, S Arora PhD, Prof A Darzi PhD); **Centre for Health Policy, Institute of Global Health Innovation, Imperial College London, London, UK** (S Ghafur MSc); **Big Data and Analytical Unit, Institute of Global Health Innovation, Imperial College London, London, UK** (I Cingolani PhD, J Symons); **and DeepMind Health, London, UK** (D King)

Correspondence to:
Dr Guy Martin, National Institutes of Health Research Patient Safety Translational Research Centre, St Mary's Hospital, Imperial College London, London W21NY, UK
guy.martin@imperial.ac.uk

Summary

Background The use of health information technology (IT) is rapidly increasing to support improvements in the delivery of care. Although health IT is delivering huge benefits, new technology can also introduce unique risks. Despite these risks, evidence on the preventability and effects of health IT failures on patients is scarce. In our study we therefore sought to evaluate the preventability and effects of health IT failures by examining patient safety incidents in England and Wales.

Methods We designed our study as a retrospective analysis of 10 years of incident reporting in England and Wales. We used text mining with the words "computer", "system", "workstation", and "network" to explore free-text incident descriptors to identify incidents related to health IT failures following a previously described approach. We then applied an n-gram model of searching to identify contiguous sequences of words and provide spatial context. We examined incident details, recorded harm, and preventability. Standard descriptive statistics were applied. Degree of harm was identified according to standardised definitions and preventability was assessed by two independent reviewers.

Findings We identified 2627 incidents related to health IT failures. 2557 (97%) of 2627 incidents were assessed for harm (70 incidents were excluded). 2106 (82%) of 2557 health IT failures caused no harm to patients, 331 (13%) caused low harm, 102 (4%) caused moderate harm, 14 (1%) caused severe harm, and four (<1%) contributed to the death of a patient. 1964 (75%) of 2627 incidents were deemed to be preventable.

Interpretation Health IT is fundamental to the delivery of high-quality care, yet there is a poor understanding of the effects of IT failures on patient safety and whether they can be prevented. Failures are complex and involve interlinked aspects of technology, people, and the environment. Health IT failures are undoubtedly a potential source of substantial harm, but they are likely to be under-reported. Worryingly, three-quarters of IT failures are potentially preventable. There is a need to see health IT as a fundamental tenet of patient safety, develop better methods for capturing the effects of IT failures on patients, and adopt simple measures to reduce their probability and mitigate their risk.

Funding The National Institutes of Health Research Imperial Patient Safety Translational Research Centre at Imperial College London.

Introduction

Adverse events leading to unintended harm or injury affect around 3–23% of patients, contribute to 3·6% of avoidable in-hospital deaths,[1–5] and are subject to both mandatory and voluntary reporting at local and national levels. A unified and open approach to reporting such events is crucial to improving the quality and safety of health care.[6,7] In England and Wales, the National Reporting and Learning System (NRLS) was established in 2003; the NRLS is the largest and most comprehensive patient safety reporting system in the world, with more than 18 million incident reports captured since its inception.[8] This voluntary system collects anonymised patient safety incidents, defined as "any unintended or unexpected incident that could have or did lead to harm to one or more patients receiving NHS-funded healthcare", from local health-care organisations in England and Wales and acts to identify safety concerns and provide evidence for key safety alerts at a national level.[9]

The use of heath information technology (IT) is rapidly increasing across all health systems to support improvements in the delivery, quality, and safety of care. There is however an increasing realisation that the unique safety risks posed by new technologies should be carefully considered alongside the potential benefits.[10] Identifying, analysing, and preventing such adverse safety events caused by health IT is hugely challenging. Health IT

Research in context

Evidence before this study

Health information technology (IT) is increasingly seen as the favoured solution to tackle the challenges of quality, cost-effectiveness, and variation in care. Despite the central role of health IT in the delivery of care, the evidence examining the preventability and impact of IT failures on patient safety is scarce. We searched PubMed from its inception to March 6, 2019, for papers published in English using the terms "health information technology failure", "computer-related patient safety", and "health information technology safety". Reference lists from relevant papers were also searched. Several studies were identified describing health IT-related safety incidents. Around 70% of IT failures involve the human–computer interface, and a significant proportion have the potential to cause harm. 96% of hospitals have only partially implemented comprehensive contingency plans to ensure the delivery of safe care when IT systems fail.

Added value of this study

Through an analysis of 2267 patient safety incidents related to health IT failures, our study has shown that a significant proportion directly lead to patient harm and worryingly 74·8% are preventable. This finding highlights that health IT is an important cause of avoidable patient harm.

Implications of all the available evidence

Our study has reinforced the importance of developing a better understanding and awareness of both the benefits and potential risks of health IT to deliver a balanced judgment of its effects on patients. The majority of health IT failures that affect patients are preventable, and all health-care organisations could take simple steps to reduce their likelihood and mitigate the risk to deliver safer care. Future work should focus on triangulating all sources of data to establish the true number of IT-related safety incidents and change the culture of health care so that health IT is seen as a fundamental tenet of patient safety.

safety events are commonly multifaceted and involve not only hardware and software, but also user behaviours, organisational characteristics, and rules and regulations that interact in a way that is complex and poorly understood.[11,12]

There is growing evidence for the effects of IT-related safety events, but given the central role of IT in the delivery of care, the data evaluating the preventability of such incidents are scarce. An analysis of a national medication error database in the USA identified more than 1000 errors related to computerised ordering systems,[13] another analysis identified 44 injuries and six deaths over 2 years due to failures in health IT,[14] and a further study identified 120 unique safety events associated with electronic health record systems.[15] In an Australian database, 99 incidents related to health IT were identified,[16] and in the UK, 850 individual patient safety events associated with the National Programme for IT were reported over a 6 year period.[17] The majority of safety events related to technology are a result of the non-technical aspects of technology, such as disruptions in workflow, poor usability or functionality, and failures in the human–computer interface.[15,18] The potential for such failures to cause harm has been highlighted in a study of 1·735 million safety events that identified 1956 incidents related to these non-technical aspects of health IT, of which 557 had the potential to cause patient harm.[19] A further study identified 3243 medication incidents related to the usability of electronic systems, of which 609 had the potential to cause harm.[20] Finally, a Finnish study identified 2379 incidents, of which 73% were due to failures in the human–computer interface.[21]

There is a need to establish further evidence for the preventability and effects of health IT failures on patient safety; as such, the NRLS database provides a unique and potentially important repository of evidence. The use of national reporting allows trends and patterns to emerge, which are too infrequent to appear at a local level. Our study aims to identify and examine preventable health IT-related harm reported at a national level in England and Wales since 2003.

Methods

For the purposes of this study, we did a retrospective analysis of 10 years of incident reporting in the England and Wales NRLS. Data extraction occurred on Aug 8, 2016.

Database search strategy

Approaches to identifying health IT-related incidents from free-text event descriptors have been described previously.[22] In our study, we used a bag-of-words approach to identify an initial corpus from incident free-text descriptors. This approach generates an orderless representation of the corpus without any spatial context.[23] Despite these limitations, the approach provides greater search precision than more complex phrase-based or topic-based approaches to classification.[24] The initial words selected were "computer", "system", "workstation", and "network". We selected these broad terms to capture all aspects of health IT, including software (eg, electronic health records, prescribing systems, and picture archiving and communication systems [PACS]) and hardware (eg, laboratory systems, IT networks, and IT devices). We then applied an n-gram model of searching to identify contiguous sequences of words within the corpus and reduce potential problems presented by polysemous words (eg, "computer system" *vs* "plumbing system") and to provide spatial context. An initial bigram approach identified 1643 prefixes and 1393 suffixes. Manual review of these prefixes and suffixes led to 348 unique prefixes

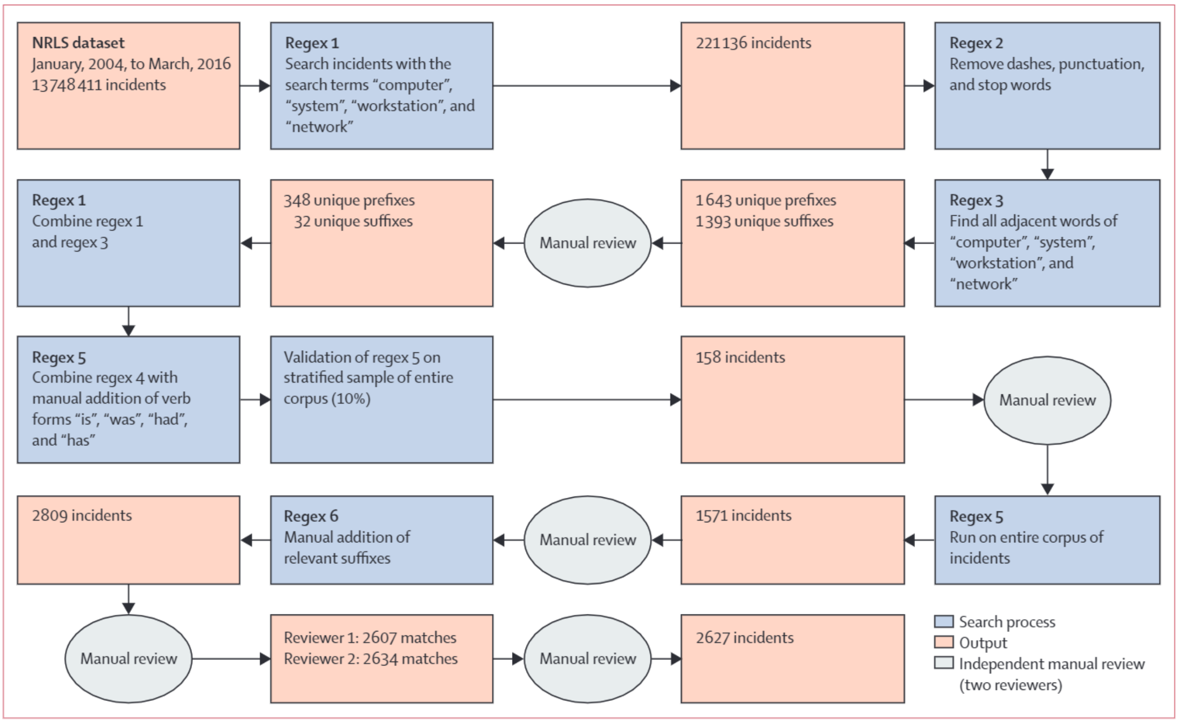
NRLS dataset
January, 2004, to March, 2016
13 748 411 incidents
Regex 1
Search incidents with the search terms “computer”, “system”, “workstation”, and “network”
221 136 incidents
Regex 2
Remove dashes, punctuation, and stop words
Regex 1
Combine regex 1 and regex 3
348 unique prefixes
32 unique suffixes
Manual review
1 643 unique prefixes
1 393 unique suffixes
Regex 3
Find all adjacent words of “computer”, “system”, “workstation”, and “network”
Regex 5
Combine regex 4 with manual addition of verb forms “is”, “was”, “had”, and “has”
Validation of regex 5 on stratified sample of entire corpus (10%)
158 incidents
Manual review
2809 incidents
Regex 6
Manual addition of relevant suffixes
Manual review
1571 incidents
Regex 5
Run on entire corpus of incidents
Manual review
Reviewer 1: 2607 matches
Reviewer 2: 2634 matches
Manual review
2627 incidents
Search process
Output
Independent manual review (two reviewers)

Figure: Summary flow diagram of search methods to explore free-text descriptions of 13 738 411 patient safety incidents to identify those related to health IT failures

Regex is a sequence of characters that define a search pattern. NRLS=National Reporting and Learning System. IT=information technology.

and 32 unique suffixes being retained. We expanded this method to create several regular expressions (regex) that were then run sequentially. A regex is a sequence of characters that describes a specific search pattern and is widely used for automated pattern matching and searching.[25] Throughout, a manual process of review and validation was done by a minimum of two independent reviewers (one doctor and one digital health policy fellow; GM, SG, and JS) to improve the precision of the search strategy with discrepancies resolved through consensus. Health IT failures were defined according to an existing classification and included any reported problems caused by the interaction of humans with IT, software or hardware issues, and other contributory sociotechnical variables.[17,26] The final regex produced 2809 incidents and an independent manual review of all incidents produced an agreement of 95·83% with a Cohens Kappa of 0·687. The final number of incidents included for analysis was 2627 incidents. A summary workflow of the search strategy is provided in the figure, and a complete search list of search bigrams and counts in the appendix.

Data analysis

Standard descriptive statistics were employed to explore the extracted data. All data were arranged, structured, and analysed utilising Microsoft Excel for Mac V15.22 and IBM SPSS for Mac V23. We assessed the data for clustering (year, incident type, organisation, and degree of harm), and none was present. Given that each incident has a unique identifier, the system prevents the duplication of data. In addition, the chance of the same incident being logged twice under separate identifiers is very low.

The degree of harm for each incident was initially recorded at the time of reporting and was subsequently confirmed or updated following the conclusion of a local incident investigation. Standardised definitions were used, including low harm (any unexpected or unintended incident that required extra observation or minor treatment and caused minimal harm to one or more people), moderate harm (any unexpected or unintended incident that resulted in further treatment, possible surgical intervention, cancelling of treatment, or transfer to another area, and which caused short-term harm to one or more people), severe harm (any unexpected or unintended incident that caused permanent or long-term harm to one or more people), and death (any unexpected or unintended event that caused the death of one or more people).

Each incident was assessed for preventability by two independent reviewers on the basis of previously established methods; incidents were independently coded on a 6-point Likert scale, with those scoring an average of 4 or more deemed to be preventable.[27,28] This study did not require ethical approval as we used routinely collected data. Data are stored and processed by Imperial College London on behalf of NHS Improvement under an existing data sharing agreement. NHS Improvement reviewed and approved the manuscript for publication.

See Online for appendix

Panel 1: Detailed examination of 2627 health IT-related patient safety incidents by recorded incident category

721 incidents related to infrastructure (including staffing, facilities, and environment)

- 498 incidents associated with IT or telecommunications failure or overload
- 49 incidents associated with absence of suitably trained or skilled staff
- 13 incidents associated with failure or delay in collection or delivery systems
- 161 incidents associated with other types of incident categories

440 incidents related to clinical assessment (including diagnosis scans, tests, and assessments)

- 249 incidents associated with failure, delays in receiving, or incorrect or missing test results or reports
- 65 incidents associated with delays or failure of diagnosis or tests
- 61 incidents associated with inadequate, incomplete, or missing scans, x-rays, or sample specimens
- 65 incidents associated with other types of incident categories

367 incidents related to documentation (including electronic and paper records, identification, and drug charts)

- 262 incidents associated with missing, inadequate, or wrong documentation, or no access or delays in obtaining documentation
- 28 incidents associated with incorrectly identified patients
- 17 incidents associated with appointment recording errors
- 14 incidents associated with failure or delays in receiving test results or reports
- 46 incidents associated with other types of incident categories

259 incidents related to medical devices or equipment

- 192 incidents associated with failure of devices or equipment
- 40 incidents associated with the absence or unavailability of devices or equipment
- 27 incidents associated with other types of incident categories

171 incidents related to medication

155 incidents related to treatment or procedures

- 101 incidents associated with delay or failure of the treatment or procedure or the inappropriate or wrong treatment or procedure
- 54 incidents associated with other types of incident categories

153 incidents related to access, admission, transfer, or discharge (including missing patients)

- 53 incidents associated with delays or failure in transport, transfer, or patient discharge
- 30 incidents associated with delay or failure in access or admission to hospital and care
- 16 incidents associated with failures in the referral process
- 54 incidents associated with other types of incident categories

145 incidents related to consent, communication, and confidentiality

- 74 incidents associated with communication failure
- 23 incidents associated with IT or telecommunications failure or overload

216 incidents associated with other types of incident categories

IT=information technology.

Role of the funding source

The funder of the study had no role in study design, data collection, data analysis, data interpretation, or writing of the report. The corresponding author had full access to all the data in the study and had final responsibility for the decision to submit for publication.

Results

13 738 411 incidents were reported by 2576 different organisations between Jan 1, 2004, and March 31, 2016. All the organisations that reported incidents use health IT, although variation in the digital maturity and number and extent of systems used by each organisation exists. The mean number of incidents reported by each organisation was 365 (range 1–56 844, SD 1925). 2627 of these incidents were identified as being related to failures in health IT, which represents 0·00019% of all incidents reported. Only 337 (13%) of 2576 organisations reported an incident related to health IT, with a mean number of incidents of 8 (range 1–64, SD 9). Incidents occurred in a range of care settings, with 2162 (82%) of 2627 incidents reported by acute or general hospitals, 311 (12%) by community nursing, medical, and therapy services, 80 (3%) by mental health services, 25 (1%) by general practice, and 49 (2%) in other care settings.

Incidents are recorded against a specific predefined category, and a detailed examination of all 2627 incidents by recorded category type is shown in panel 1. Pertinent results show that 721 (27%) of 2627 incidents were related to infrastructure failures, with the majority of these (498 [69%] of 721) as a direct result of IT or telecommunications failures. 440 (17%) of the 2627 incidents were due to failures in clinical assessment, with the majority of these (249 [56%] of 440) being due to incorrect, missing, or delayed test reports and results. 367 (14%) of 2627 incidents were due to failures in documentation with the majority (262 [71%] of 367) due to missing, inadequate, or absent documentation. Importantly, direct failures in IT, missing or delayed test results, missing, inadequate, or absent documentation, and the direct failure of equipment are all plausibly linked to failures in either hardware, software, or the human–technical interface.

Panel 2: Examples of incident descriptors for level of reported harm reported in 2557 patient safety incidents related to failures in health IT

2106 (82%) of 2557 incidents reported to have caused no harm

- "[...] system down so cannot do electronic discharge letter"
- "Arrived to the ward after being closed over the weekend to find all the network system was down and the computers were unable to access anything; therefore patients could not be admitted to the unit and blood cards could not be printed for patients on the unit"

331 (13%) of 2557 incidents reported to have caused low harm

- "A new patient was admitted to the unit and we had difficulty obtaining a medical record number for them due to the computer system failing. It was 5 h after they arrived on the unit before we managed to obtain an emergency number. This resulted in a delay to their treatment as medical tests cannot be ordered without a medical record number"
- "Patient currently on iv heparin and requires 6 hourly blood test monitoring as infusion rate needs constant adjustments; due to pathology system [being] unavailable [there will be] no blood results for 24 h. Patient safety at risk"

102 (4%) of 2557 incidents reported to have caused moderate harm

- "Patient gent [gentamicin] level not available as computer system crashed. Phoned lab - they are unable to access results also; therefore, gentamycin dose not given to cardiac baby on 3 antibiotics"
- "[...] system error resulted in approximately 1700 patient records having missing data items on attached specimen records. This caused multiple specimens to be inaccessible"

14 (1%) of 2557 incidents reported to have caused severe harm

- "Main server for pharmacy IT system failed. No 24 h maintenance contracted for from server provider. No 24 h internal IT cover. Result [is] complete failure of pharmacy operational system"
- "Computer system down since 1230 h in the afternoon. [The site] has had no access to [the] network, preventing staff from doing their jobs properly. No change at 2100 h"

Four (<1%) of 2557 incidents reported to have caused death

- "Patient became acutely unwell overnight, had been seen by on call team during the previous day... Found to be in probable urinary sepsis. Later died. [Results] system not working properly and so positive MSU [mid-stream urine] from 4/7 [4 days] earlier had been missed by ward team and on call team"
- "Patient arrived to emergency department as a priority call at 1259 h [...] PAS system was down at the time and initial bloods taken were ordered on paper form. Medical Registrar saw patient at approximately 1600 h but no results on system. Called lab who stated that they could not find bloods. Many other samples had gone missing on this day [....] Results from repeat bloods available on system at 1949 h and many results were critical. Patient deteriorated clinically and died"

IT=information technology. PAS=patient administration system.

The degree of patient harm reported for each incident is categorised following completion of a local incident investigation and closure of the event. 70 (3%) of 2627 incidents were related to delays in the recording of incidents due to failures in the electronic incident management software itself and were therefore excluded from further analysis. 2106 (82%) of 2557 incidents were recorded as causing no harm, 331 (13%) of 2557 incidents as causing low harm, 102 (4%) of 2557 incidents as causing moderate harm, 14 (1%) of 2557 incidents as causing severe harm, and four (<1%) of 2557 incidents contributed to a patient death. This pattern of harm is consistent with that seen across all incidents reported (examples of incidents related to each category of harm are shown in panel 2).[29]

Of the 102 incidents reported to have caused moderate harm, 24 incidents (24%) were caused by failures in laboratory or pathology systems, 21 (21%) by failures in PACS or other radiology systems, 16 (16%) by multiple system failures across a hospital network, 12 (12%) by problems with electronic patient records systems, eight (8%) by failures in patient administration systems and other administration systems, three (3%) by issues with pharmacy systems or electronic prescribing, and 18 (18%) by failures in miscellaneous systems, such as those used for appointments, equipment ordering, or follow-up. Of the 14 incidents reporting severe harm to patients, four (29%) of 14 were caused by failures in pathology or laboratory systems, three (21%) by failures in pharmacy or electronic prescription systems, two (14%) by failures in electronic patient record systems, two (14%) by failures in radiology or PACS systems, and a single incident (7%) was reported from failures in appointment booking systems and equipment ordering systems. Importantly, four (<1%) of the 2557 incidents reported were associated with the death of a patient, two (<1%) incidents were related to the failure of a laboratory system leading to delays in obtaining safety-critical results, one (<1%) incident was related to delays in the correct diagnosis and treatment following the failure of an electronic records system, and one (<1%) incident was due to the administration of incorrect antimicrobial therapy following the failure of a pathology system.

	Number of incidents (n=2627)	Example of incident descriptor
663 (25%) of 2627 incidents were unpreventable		
Score 1	106 (4%)	"[...] a clinician arrived, was informed of the computer failing and stated his clinic was cancelled. Another clinical area was offered where the IT system was working"
Score 2	230 (9%)	"[...] prescribing system down, unable to access any computer on the ward, paper copies of medication drug charts being completed"
Score 3	327 (12%)	"Arrived on the mobile unit to find there was no paperwork for the days screening clients we were able to download the list from [a system], but if the computer system went down we would be forced to cancel the clinic as we would be unable to perform adequate identity checks [...]"
1964 (75%) of 2627 incidents were preventable		
Score 4	1253 (48%)	"Blood science and microbiology laboratory IT system failed at 1115 h and was not restored until 1310 h causing a significant delay in processing and reporting laboratory tests [...]"
Score 5	605 (23%)	"The system crashed at 0915 h. The US dept is paperless, so no patient records could be tracked and patient details accessed. Although all original referral forms are kept they are not filed in either alphabetical or chronological order - the consequence of this was that it took ninety minutes to trace patient cards. This is the second time this has happened"
Score 6	106 (4%)	"Whole EPR system failure from 1430 h. No 24-h cover provided by the company who provide the EPR service. Unable as yet to identify cause of problem. Possible corruption in web server. No timescales identified for restoring the system at present. No data lost but issues with access. [IT company] will work until 2100 h then return to work on the system again at 0900 h on the May 9"

Examples of incidents are provided to show the increases in severity between preventable and non-preventable incidents. Incidents with a score of 4 or higher are deemed to be preventable. IT=information technology. US=ultrasound. EPR=electronic patient record.

Table: **Preventability score ratings of 2627 health IT-related patient safety incidents**

A summary of the preventability assessment together with examples of each scoring category is displayed in the table. There were some challenges in establishing preventability. All IT systems can fail, and so key factors considered included whether the IT failure was managed with effective downtime procedures, the duration of the failure, and whether the incident could have been foreseen or avoided. In addition, a small number of incidents in which relevant training or education was inadequate, resulting in staff being unable to effectively use the systems, were also considered to be preventable. Despite these difficulties, the overall inter-rater coding agreement was excellent, with an intraclass correlation coefficient of 0·926 (0·907–0·942, p<0·0001). Overall, 1964 (75%) of 2627 incidents were deemed to be preventable.

Although all IT systems will undoubtedly be affected by system failures, robust and effective back-up procedures and policies must be in place to prevent these failures causing delays in care or harm to patients; organisations should be able to provide timely and safe care in spite of IT failures. One record that came up in our search reported that the "[...] computer system not available for 13 hours overnight. Patient bleeding in theatre [...] theatre staff were desperate for the products and there was a delay. Practical procedure followed but paperwork not available within time specified for blood products."

A further key factor influencing the preventability of several incidents was a failure of IT departments to effectively communicate planned downtime to users, a failure to do these planned tasks outside core business hours, when the effects on patients would be reduced, or a failure to do previous risk assessments. "There was a significant IT systems failure resulting in a trust wide IT systems failure for several hours [...] it is believed that the failure may have been precipitated by an electrical shutdown which caused overheating and over loading of the IT servers. There doesn't appear to have been a necessary risk assessment carried out prior to the work commencing or contingencies put into place in case things went wrong."

A further factor leading to preventable safety incidents was the failure of organisations to provide effective IT support for their systems. This absence of adequate support was particularly evident with IT systems supported by external providers who frequently were not contracted to provide out-of-hours support, resulting in unnecessary delays to return of service and avoidable harm to patients. "Laboratory computer system failure. All areas affected. Attempt to re-boot system failed. As a result, laboratory without computer system for more than 24 h. System support (external supplier) is 8am–8pm Mon–Fri and Saturday morning only. Manual systems were used over weekend. Support contacted Monday AM and fault rectified within 1 h [...]."

Discussion

Health IT is ubiquitous and is increasingly seen as the favoured solution to tackle the challenges of variation in care, increasing demand, and challenging fiscal realities. Despite its central role in the delivery of care, evidence examining the preventability of such incidents and their effects on patient safety is scarce. By examining 13 738 411 patient safety incidents recorded over more than a decade in England and Wales we have identified 2627 individual events related to failures in health IT. This study has shown that a large proportion of these incidents lead to harm, the majority are preventable, and that all health-care organisations could take simple steps to reduce the likelihood of these incidents and mitigate the risk by lessening their effects.

The 2627 incidents identified in this study represent 0·00019% of all reported safety events, which is at the low end of previously reported proportion of incidents related to health IT of between 0·00008% and 0·1%.[13,15,16,19,26] The relatively low number of incidents identified in this study is likely to be because of a failure to report incidents rather than their absence. Large reporting systems substantially underestimate the incidence of adverse safety events and under-report harm; only around 5% of safety incidents in England are thought to be reported to the NRLS.[4] Furthermore, near misses, although more common than adverse events, are less likely to be documented and recorded despite providing valuable lessons.[30] In addition, only 337 (13%) of 2576 organisations reported a health IT incident, which is surprising given the ubiquity of such technology. Finally, just 273 (10%) of 2627 incidents identified in this analysis took place within primary care, despite the fact that they are responsible for the majority of patient contacts within the National Health Service. That the incidents examined in this analysis represent just a small proportion of health IT-related harm caused to patients in England and Wales is highly probable.

Only 14% of adverse events in patients who are admitted to hospital are estimated to be reported,[31] and voluntary reporting of safety incidents and other methods for event identification based on routine administrative data could miss up to 90% of adverse events; this under-reporting has led to the development of new methodologies for improving the capture of safety events.[32] Although there is a need to improve safety incident reporting more generally, to improve the capture of health IT-related incidents bespoke methodologies are needed. The so-called retract-and-reorder tool for identifying incorrect electronic patient orders is an example of such a method.[33] Strategies to minimise the risks of health IT and learn from incidents need to be based upon a full understanding of contributing factors and safety implications.[34] Failure to adequately report health IT incidents might be due to confused messaging as to where and how to report incidents. Indeed, only 498 (22%) of the 2267 incidents identified in this study were actually reported in the IT-related categories of NRLS. The rest were reported under numerous other categories (eg, test results or clinical care, which are pre-defined categories within NRLS). Most IT-related incidents are likely to be reported locally through IT departments, whereas others might be reported to centralised national bodies.[15,17,35] This clear lacuna relates back to the fundamental differences in regulatory regimes, approval processes, and post-market monitoring requirements for health IT compared with other innovations and the subsequent absence of a standardised central repository of health IT failures. Furthermore, staff probably see a computer failure as an IT issue rather than a patient safety issue, and are therefore less likely to report it, and incidents that are reported might also reflect the bias of those reporting the incident who are commonly IT professionals.[36] Future work to triangulate incident reporting data across local and national sources is crucial to provide a better estimation of the true number of health IT-related safety incidents. To facilitate this systematic identification of health IT failures and their effects on patient safety, there is a need to consolidate reporting through a standardised prospective reporting system with a common classification for health IT failures. These events can be difficult to define because they are heterogenous, often occur in temporally or physically separate circumstances, and generally involve complex interactions between multiple technical and non-technical factors.[37,38] Previous studies have attempted to tackle this challenge and have identified up to 32 distinct categories of computer failures, and important work in the development of methods for systematically categorising, evaluating, and understanding health IT failures is underway.[16,39–42]

Both the planned and unplanned failure of health IT can pose substantial safety risks for patients.[43] Although some technology downtime is expected for regular maintenance or updates, much of it is unplanned because of equipment failures, external events (eg, power failures), or cyberattacks (eg, the WannaCry incident in the UK). Underinvestment in health IT increases the risk of unplanned failures and increases the preventable patient harm. In the example of the WannaCry incident, a failure to install a simple operating system patch because of the inadequate funding of support services led to the entirely preventable disruption of care for many thousands of patients. This failure to invest in IT hardware and software was clear in this analysis, with around 30% of safety incidents directly related to infrastructure failures.

Despite 96% of organisations having had unplanned downtime as a result of IT failures in the past 3 years, most have only partially implemented comprehensive contingency plans to maintain safe and effective care when their IT systems are disrupted,[44] despite clear best-practice guidance being available, such as the Contingency Planning SAFER Guide in the USA.[45] The failure to invest in appropriate support services and develop resilient contingency plans was also evident in our study. There were several cases in which systems support was either not provided at all or was out-sourced to external providers with no out-of-hours provision for support, resulting in unnecessary, prolonged, and entirely avoidable patient harm due to delays in resolving faults and returning the availability of crucial services. This low investment was often compounded by inadequate or ignored downtime procedures and an inability of organisations to deliver safe care following even temporary IT failures; a consistent finding in other studies in which around half of all incidents related to health IT are due to downtime procedures not being in place or not being followed.[43] The need to adequately respond to such failures and maintain the provision of safe care is crucial. IT failures and downtime have been shown to lead to 49 h per year of disruption in a typical metropolitan hospital, with only half of this time occurring during normal working hours.[46] Furthermore, downtime has been associated with increased operative duration and length of stay in patients having surgical procedures,[47] and long delays in clinicians responding to pathology results.[48]

Our study is not without limitations. The principal challenge of this study was establishing the accuracy of the search process. We used a rules-based approach to text mining combined with manual validation to identify relevant incidents. Similar techniques have previously been used to identify adverse events with good sensitivity and specificity.[49] Nonetheless, without manual review of all 13 738 411 incidents, the true precision and accuracy of the search methodology that we used cannot be definitively calculated. Although the approach we took would appear robust, there is a high chance that incidents were incorrectly classified or not identified at all, thus limiting the accuracy of the search and resulting in not being able to identify all relevant incidents within NRLS. Finally, although we used an established method to ascertain the preventability of incidents, without complete details and the full context and background for each incident, establishing whether or not the incident was preventable can be challenging and open to differences of opinion.

We identified some core failings that, if addressed, might help reduce the occurrence of incidents and mitigate risk by lessening their effects; three-quarters of incidents identified were potentially preventable. First, the majority of incidents identified were due to the non-availability of patient data or the failure of systems to support the timely delivery of correct test results; the dependence on legacy systems and inadequate investment in technology was evident in a large number of these incidents. Second, clearly, all IT systems can fail. However, when these systems are crucial and fundamental for the continuing delivery of safe care, there is an absolute need for robust, tested, and effective back-up systems and downtime procedures. Third, failures in health IT often led to avoidably prolonged harm due to inadequacies in technical support and difficulties in the timely resolving of IT failures. Finally, failings in health IT are likely to be under-reported given the small number identified in our study; the culture must change, with the successes and failures of health IT viewed as a fundamental tenet of patient safety.

Contributors

GM, SG, IC, JS, DK, SA, and AD all contributed to this Article. GM designed and led the study. Data extraction and analysis was done by GM, SG, IC, and JS. GM wrote the manuscript with contributions from SG, IC, JS, DK, and SA. AD was responsible for overall supervision and is the guarantor for the study. All authors have access to all the data and take responsibility for the integrity of the data and accuracy of the data analysis.

Declaration of interests

We declare no competing interests. DK is an employee of DeepMind Health as well as an honorary lecturer at Imperial College London (London, UK). The views expressed are our own and not necessarily those of the National Health Service (NHS), the National Institutes of Health Research, or the Department of Health.

Data sharing

All relevant data and supporting study documentation are available from the corresponding author following reasonable request and dependent upon permission from NHS Improvement. All data sharing requests should be made to Guy Martin (Department of Surgery and Cancer, Imperial College London, St Mary's Hospital, London, UK; guy.martin@imperial.ac.uk).

References

1 Brennan T, Leape L, Laird N, et al. Incidence of adverse events and negligence in hospitalized patients. Results of the Harvard Medical Practice Study I. *N Engl J Med* 1991; **324:** 370–76.

2 Vincent C, Neale G, Woloshynowych M. Adverse events in British hospitals: preliminary retrospective record review. *Br Med J* 2001; **322:** 517–19.

3 Hogan H, Zipfel R, Neuburger J, Hutchings A, Darzi A, Black N. Avoidability of hospital deaths and association with hospital-wide mortality ratios: retrospective case record review and regression analysis. *Br Med* 2015; **351:** 1–6.

4 Sari A, Sheldon T, Cracknell A, Turnbull A. Sensitivity of routine system for reporting patient safety incidents in an NHS hospital: retrospective patient case note review. *Br Med J* 2007; **334:** 79.

5 Landrigan C, Parry G, Bones C, Hackbarth A, Goldmann D, Sharek P. Temporal trends in rates of patient harm resulting from medical care. *N Engl J Med* 2010; **363:** 2124–34.

6 Donaldson L. An organisation with a memory. *J Royal Coll Physicians* 2000; **2:** 452–57.

7 Runciman WB. Lessons from the Australian Patient Safety Foundation: setting up a national patient safety surveillance system: is this the right model? *Qual Saf Health Care* 2002; **11:** 246–51.

8 National Reporting and Learning System. National patient safety incident reports: 26 September 2018. NRLS Q. Data Workb. 2018. https://improvement.nhs.uk/resources/national-patient-safety-incident-reports-26-september-2018/ (accessed July 27, 2016).

9 National Health Service Improvement. NRLS official statistics publications: guidance notes. 2018 https://improvement.nhs.uk/documents/2549/NRLS_Guidance_notes_March_2018.pdf (accessed March 3, 2019).

10 Sittig D, Singh H. Electronic heath records and national patient-safety goals. *N Engl J Med* 2012; **367:** 1854–60.

11 Harrison M, Koppel R, Bar-Lev S. Unintended consequences of information technologies in healthcare: an interactive sociothecnical analysis. *J Am Med Informatics Assoc* 2007; **14:** 542–49.

12 Sittig D, Singh H. A new sociotechnical model for studying health information technology in complex adaptive healthcare systems. *Qual Saf Healthc* 2010; **19** (suppl 3): i68–74.

13 Zhan C, Hicks R, Blanchette C, Keyes M, Cousins D. Potential benefits and problems with computerized prescriber order entry: analysis of a voluntary medication error-reporting database. *Am J Heal Pharm* 2006; **63:** 353–58.

14 US Office of the National Coordinator for Health IT. HIT Policy Committee, Adoption/Certification Workgroup. 2007. http://healthit.hhs.gov (accessed April 7, 2016).

15 Myers R, Jones S, Sittig D. Review of reported clinical information system adverse events in US Food and Drug Administration databases. *Appl Clin Inform* 2011; **2:** 63–74.

16 Magrabi F, Ong M-S, Runciman W, Coiera E. An analysis of computer-related patient safety incidents to inform the development of a classification. *J Am Med Informatics Assoc* 2010; **17:** 663–70.

17 Magrabi F, Baker M, Sinha I, et al. Clinical safety of England's national programme for IT: a retrospective analysis of all reported safety events 2005 to 2011. *Int J Med Inform* 2015; **84:** 198–206.

18 Meeks D, Smith M, Taylor L, Sittig D, Scott J, Singh H. An analysis of electronic health record-related patient safety concerns. *J Am Med Informatics Assoc* 2014; **21:** 1053–59.

19 Howe J, Adams K, Hettinger Z, Ratwani R. Electronic health record usability issues and potential contribution to patient harm. *J Am Med Assoc* 2018; **319:** 1276–78.

20 Ratwani R, Savage E, Will A, et al. Identifying electronic health record usability and safety challenges In pediatric settings. *Health Aff* 2018; **37:** 1752–59.

21 Palojoki S, Mäkelä M, Lehtonen L, Saranto K. An analysis of electronic health record-related patient safety incidents. *Health Informatics J* 2017; **23:** 134–45.

22 Fong A, Adams K, Gaunt M, Howe J, Kellogg K, Ratwani R. Identifying health information technology related safety event reports from patient safety event report databases. *J Biomed Inform* 2018; **86:** 135–42.

23 Salton G, McGill M. Introduction to modern information retrieval. New York, NY: McGraw-Hill Book Co, 1983.

24 Conway M, Doan S, Kawazoe A, Collier N. Classifying disease outbreak reports using n-grams and semantic features. *Int J Med Inform* 2009; **78:** 47–58.

25 Thompson K. Regular expression search algorithm. *Communications of the ACM* 1968; **11:** 419–22.

26 Magrabi F, Ong M-S, Runciman W, Coiera E. Using FDA reports to inform a classification for health information technology safety problems. *J Am Med Informatics Assoc* 2012; **19:** 45–53.

27 Symons N, Almoudaris A, Nagpal K, Vincent C, Moorthy K. An observational study of the frequency, severity, and etiology of failures in postoperative care after major elective general surgery. *Ann Surg* 2012; **257:** 1–5.

28 Wilson RM, Runciman WB, Gibberd RW, Harrison BT, Newby L, Hamilton JD. The Quality in Australian Health Care Study. *Med J Aust* 1995; **163:** 458–71.

29 Howell AM, Burns E, Bouras G, Donaldson L, Athanasiou T, Darzi A. Can patient safety incident reports be used to compare hospital safety? Results from a quantitative analysis of the english national reporting and learning system data. *PLoS One* 2015; **10:** 1–15.

30 Neale G, Woloshynowych M. Retrospective case record review: a blunt instrument that needs sharpening. *Qual Saf Healthc* 2003; **12:** 2–3.

31 Roehr B. US hospital incident reporting systems do not capture most adverse events. *Br Med J* 2012; **344:** e386.

32 Classen D, Resar R, Griffin F, et al. 'Global trigger tool' shows that adverse events in hospitals may be ten times greater than previously measured. *Health Aff* 2011; **30:** 581–89.

33 Adelman J, Kalkut G, Schechter C, et al. Understanding and preventing wrong-patient electronic orders: a randomized controlled trial. *J Am Med Informatics Assoc* 2013; **20:** 305–10.

34 Goodman K, Berner E, Dente M, et al. Challenges in ethics, safety, best practices, and oversight regarding HIT vendors, their customers, and patients: a report of an AMIA special task force. *J Am Med Informatics Assoc* 2011; **18:** 77–81.

35 Food and Drug Administration. Manufacturer and User Facility Device Experience. 2018. https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfmaude/search.cfm (accessed May 29, 2018).

36 Runciman W, Kluger M, Morris R, Paix A, Watterson L, Webb R. Crisis management during anaesthesia: the development of an anaesthetic crisis management manual. *Qual Saf Healthc* 2005; **14:** e1.

37 Singh H, Sittig D. Measuring and improving patient safety through health information technology: the Health IT Safety Framework. *BMJ Qual Saf* 2016; **25:** 226–32.

38 Walker J, Carayon P, Leveson N, et al. EHR safety: the way forward to safe and effective systems. *J Am Med Informatics Assoc* 2008; **15:** 272–77.

39 Koppel R, Metlay J, Cohen A, et al. Role of computerized physician order entry systems in facilitating medication errors. *J Am Med Assoc* 2005; **293:** 1197.

40 Singh H, Ash J, Sittig D. Safety assurance factors for electronic health record resilience (SAFER): study protocol. *BMC Med Inform Decis Mak* 2013; **13:** 46.

41 Yusof M, Kuljis J, Papazafeiropoulou A, Stergioulas L. An evaluation framework for Health Information Systems: human, organization and technology-fit factors (HOT-fit). *Int J Med Inform* 2008; **77:** 386–98.

42 Kuziemsky C, Kushniruk A. A framework for contexual design and evaluation of health information technology. *Stud Health Technol Inform* 2015; **210:** 20–24.

43 Larsen E, Fong A, Wernz C, Ratwani RM. Implications of electronic health record downtime: An analysis of patient safety event reports. *J Am Med Informatics Assoc* 2018; **25:** 187–91.

44 Sittig D, Gonzalez D, Singh H. Contingency planning for electronic health record-based care continuity: A survey of recommended practices. *Int J Med Inform* 2014; **83:** 797–804.

45 The Office of the National Coordinator for Health Information Technology. Safety Assurance Factors for EHR Resilience. 2016. https://www.healthit.gov/sites/default/files/safer/guides/safer_contingency_planning.pdf (accessed March 3, 2019).

46 Chen J, Wang Y, Magrabi F. Downtime in digital hospitals: an analysis of patterns and causes over 33 months. *Stud Health Technol Inform* 2017; **239:** 14–20.

47 Harrison AM, Siwani R, Pickering BW, Herasevich V. Clinical impact of intraoperative electronic health record downtime on surgical patients. *J Am Med Informatics Assoc* 2019; published online April 4. DOI:10.1093/jamia/ocz029.

48 Wang Y, Coiera E, Gallego B, et al. Measuring the effects of computer downtime on hospital pathology processes. *J Biomed Inform* 2016; **59:** 308–15.

49 Botsis T, Nguyen M, Woo EJ, Markatou M, Ball R. Text mining for the Vaccine Adverse Event Reporting System: medical text classification using informative feature selection. *J Am Med Informatics Assoc* 2011; **18:** 631–38.