Original Article

Health Informatics Journal

Health Informatics Journal
1–13

DOI: 10.1177/1460458220918539
journals.sagepub.com/home/jhi

Understanding the scope of downtime threats: A scoping review of downtime-focused literature and news media

Ethan P Larsen
Houston Methodist Research Institute, USA; Children's Hospital of Philadelphia, USA

Arjun H Rao
Texas A&M University, USA

Farzan Sasangohar
Texas A&M University, USA; Houston Methodist Research Institute, USA

Abstract

Electronic health record downtimes are any period where the computer systems are unavailable, either for planned or unexpected events. During an unexpected downtime, healthcare workers are rapidly forced to use rarely-practiced, paper-based methods for healthcare delivery. In some instances, patient safety is compromised or data exposed to parties seeking profit. This review provides a foundational perspective of the current state of downtime readiness as organizations prepare to handle downtime events. A search of technical news media related to healthcare informatics and a scoping review of the research literature were conducted. Findings ranged from theoretical exploration of downtime to empirical direct comparison of downtime versus normal operation. Overall, 166 US hospitals experienced a total of 701 days of downtime in 43 events between 2012 and 2018. Almost half (48.8%) of the published downtime events involved some form of cyber-attacks. Downtime contingency planning is still predominantly considered through a top-down organizational focus. We propose that a bottom-up approach, involving the front-line clinical staff responsible for executing the downtime procedure, will be beneficial. Significant new research support for the development of contingency plans will be needed.

Keywords

downtime, electronic health records, healthcare informatics, hospitals, patient safety

Corresponding author:
Ethan P Larsen, Radiology Services, Children's Hospital of Philadelphia, 3401 Civic Center Blvd, Philadelphia, PA 19104, USA.
Email: larsene@email.chop.edu

Introduction

Motivated by the 2009 Health Information Technology for Economic and Clinical Health or HITECH Act, 96 percent of US hospitals have installed and use an electronic health record (EHR) system.[1,2] The rapid and thorough adoption of EHRs has brought a number of benefits to healthcare operations including improved efficiency, clinical decision support (CDS), and patient record portability.[3–6]

Despite the benefits of EHRs, their widespread adoption has also introduced potential new safety issues.[7,8] One such safety issue is a downtime event, which is a period of time when the EHR and associated systems are unavailable. Downtime events occur regularly for planned maintenance and upgrades and can also be triggered by hardware issues, software errors, computer viruses, and deliberate attacks.[9–11] Planned downtime events are typically scheduled for low-impact hours on evenings and weekends; clinicians are given advance notice of the downtime and patient care needs are shifted to accommodate the downtime. Unplanned downtime events occur without warning and can be significantly more severe, as the entire EHR and supporting infrastructure can be suddenly taken offline.

While downtime may affect only specific systems and departments, such connectivity issues may not be immediately visible to the rest of the organizational network. One such system that could be impacted is the CDS which generates alerts when clinician orders may induce risk to patients, during certain downtime scenarios CDS may be offline and unable to generate warnings. A clinician may be unaware of a CDS-related downtime and can mistakenly assume a lack of error notification to mean a safe order has been submitted.[12,13] In reality, with the CDS and computerized physician order entry (CPOE) systems compromised, a physician could easily prescribe a medication for a patient with a known allergy, yet remain unaware until the patient experiences an adverse reaction.

During a downtime event, clinicians may be unfamiliar with downtime contingency plans and paper-based workflows.[7,12] Anecdotal evidence from a large northeastern medical center in the United States suggests that in one downtime event, the loss of pharmacy connectivity and CPOE systems meant that physicians had to complete paper prescription pads. During this particular event, a number of junior physicians, who had never received prior training to use a paper prescription pad before, were on duty. As a result, several prescriptions that were included in patient discharge packets were improperly filled out (personal correspondence, anonymized for confidentiality). There were also reports of nurses devising their own unofficial downtime procedures which resulted in poor clinical decision-making, leading to high-risk, near-miss incidents involving medication overdoses and other misadministration events (personal correspondence, anonymized for confidentiality).

In light of these risks and despite the prevalence of EHR usage in US healthcare, the research literature has not provided a significant treatment for the issue of downtime. We argue that the issue merits investigation, as the results can inform and provide contextual support for administrators designing contingency plans for downtime.

Methods

This article employs two review processes in order to explore how pervasive the downtime issue may be, and how it is currently being studied in US hospitals. The pervasiveness of downtime is identified by a scoping review of relevant technical news media in order to estimate the number and severity of the downtime events publicly acknowledged by US healthcare facilities. The second approach is a scoping literature review of the current state of downtime research, specifically

Table 1. Technical news media searched.

Sources of information
1. Becker's Hospital Review (https://www.beckershospitalreview.com)
2. EHRIntelligence (https://ehrintelligence.com)
3. HealthITAnalytics (https://healthitanalytics.com)
4. HealthITSecurity (https://healthitsecurity.com)
5. RevCycleIntelligence (https://revcycleintelligence.com)
6. mHealthIntelligence (https://mhealthintelligence.com)
7. HealthPayerIntelligence (https://healthpayerintelligence.com)
8. Patient Engagement HIT (https://patientengagementhit.com)
9. HITInfrastructure (https://hitinfrastructure.com)
10. Healthcare informatics (https://www.healthcare-informatics.com)
11. Google News (https://news.google.com)

Table 2. News media search terms.

"EHR" *OR* "Computer" *OR* "Electronic Health Record" OR "EMR" OR "Electronic Medical Record"	*AND*	"Downtime" *OR* "Outage" *OR* "Down"

research involving contingency planning for downtime. The research review is focused on determining how downtime contingency plans are currently approached and the scope of relevant studies. Through the two reviews, a holistic depiction of the current state of downtime research will be established, with suggestions for continued research focus.

Scoping review of technical news media

A search of downtime events at US hospitals was conducted within major healthcare informatics media listed in Table 1, as well as Google News. Healthcare informatics in news media platforms are the main source of news on EHRs, and issues with downtime are likely to be reported in such platforms to ensure a broader reach to healthcare informatics professionals, as opposed to the mainstream news media or the academic literature. The news outlets were queried with the terms listed in Table 2. All results were reviewed for relevance and included only if the content of the article contained an indication that the EHR was truly offline. Any downtime events indicated before HITECH's launch in 2009 were excluded.

The news stories identified through the search were reviewed for any indications of the downtime origin, duration, and extent. Some downtime events have the ability to impact an entire system of the hospitals simultaneously, so a simple tally of downtime events does not represent the entire situation. To understand the full extent, the duration as the sum total of days a US hospital experienced downtime must be captured. The hospital-day unit is intended to represent the sum of all days all hospitals encountered downtime whether independently or simultaneously. For example, if a five-hospital system experienced a system-wide 2-day downtime, that downtime event would have impacted five hospitals for 2 days, or a hospital-day measure of 10 hospital-days of downtime

$$\text{Hospital days} = \left(n \text{ hospitals impacted}\right) \times \left(m \text{ days incident duration}\right) \quad (1)$$

Table 3. Scoping review search terms.

"Information Technology" *OR* "Electronic Medical Record" *OR* "Electronic Health Record"	*AND*	"Downtime" *OR* "Offline" *OR* "Outage" *OR* "Delay" *OR* "Contingency" *OR* "Failure"

Scoping literature review of downtime contingency planning

In order to understand the current state and scope of downtime research and hospital readiness for downtime events, as well as current gaps in research, a scoping literature review was conducted. The review was structured using the PRISMA-ScR checklist, an extension of the original PRISMA guidance for systematic reviews designed for scoping review exercises.[14] A pre-planned search strategy was developed to query MEDLINE and CINAHL databases using search terms identified in Table 3. A summary of the data study collection and inclusion process is illustrated in the PRISMA diagram in Figure 1.[15]

Study selection

Studies were considered for inclusion if they were (1) published between 2009 and September 2018; (2) written in English; (3) conducted in a US-based facility; and (4) studying aspects of EHR downtime events. Aspects of method, hospital domain, or scope were not restricted. A study was excluded if one or more inclusion criteria were missing. The assembled studies were initially screened by their abstracts for potential inclusion. The search strings returned a significant number of papers related to biomedical studies which were rapidly excluded based on review of the titles and the abstracts. The full text of the remaining 40 articles was screened manually by the lead author for inclusion, domain, and scope. The identified papers were analyzed thematically for focus, subject, methods, and conclusions.

Results and discussion

Scoping review of news media

Since the initiation of HITECH in 2009, there have been 43 reported instances of EHR-related downtime in US hospitals. Based on the available information, the identified events were classified by their origin, outlined in Table 4.

The primary cause for the reported downtimes is cyber-attack compromising the EHR, accounting for 48.8 percent ($n=21$) of downtime events (Figure 2). The second most prevalent source was identified as the facility, accounting for 18.6 percent ($n=8$) of events, which included failures of non-health IT (HIT) systems such as when the fire suppression system was activated in the server room of the hospital. Provider-driven outages, while accounting for about 4.7 percent ($n=2$) of events, are notable due to the data structure typically used in hospitals—the EHR provider is also the data host, so if the EHR provider loses connectivity, all subscriber hospitals also lose connectivity.

Although there were no publicly reported downtime events found in the news media before 2012, 43 downtime events impacted 166 US hospitals between 2012 and 2018 (Figure 2) with a total of 701 hospital-days of EHR downtime. Many of the downtime events impacted multiple hospitals at the same time. Though a positive trend in the number of downtime events is apparent, inference of specific trends may be limited since the availability of data may be affected by the lack of events rising to national-level attention, and by reluctance to report publicly due to liability concerns.

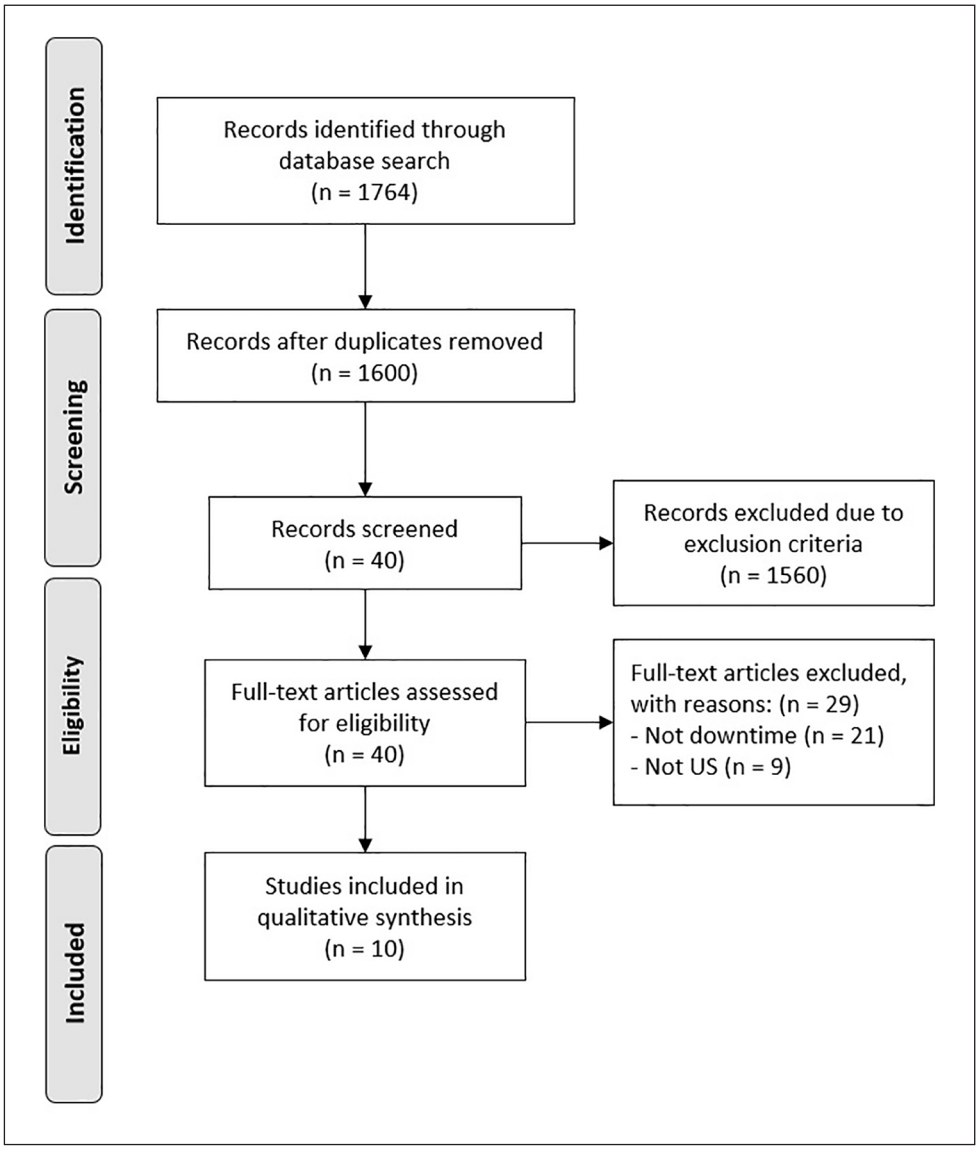

Figure 1. PRISMA-ScR flow diagram.

These results show that downtime events are a growing issue in healthcare. They originate from sources that are difficult to control and can be highly disruptive. Even the accidental activation of fire suppression systems in a server room would likely entail a process of hardware rescue and data reconstruction, triggering a slowdown as backup systems are called into action. The performance and patient care threats of any unplanned downtime event are always present and should be accounted for in the downtime procedures.

We found that cyber-attacks represented a large proportion of the reported downtime events noted in the technical literature. Ransomware viruses encrypt the entire file system and display messages demanding monetary ransom in exchange for the decryption key.[11,22] Defending against

Table 4. Origins of unplanned EHR downtime events.

Origin	Frequency	Definition	Exemplar
EHR provider	2	The provider as the host of the data loses connectivity; all subscriber hospitals experience downtime.	Temporary power outage affects dozens of hospitals' access to medical records.[16]
Nature	2	Downtime triggered by external "act of God" such as a destructive storm.	The impact of hurricanes.[17]
Internal IT	7	Failure of hardware or software within hospital IT system.	Coping with prolonged EHR downtime.[18]
Facility	8	Failure of a non-IT related service or system within the hospital such as accidental activation of a fire suppression system.	System-wide epic EHR downtime affects 24 sutter health hospitals.[19]
Cyber-attack	21	Any form of virus infection, deliberate hack, ransomware, or other malicious data access attempt.	Ransomware leads to EHR downtime in DC-area health system.[20]
Unknown	3	The event reached notice for publication in a news story, but the cause was not indicated in the news release.	All in a health recovers from system-wide stint of EHR downtime.[21]

EHR: electronic health record; IT: information technology.

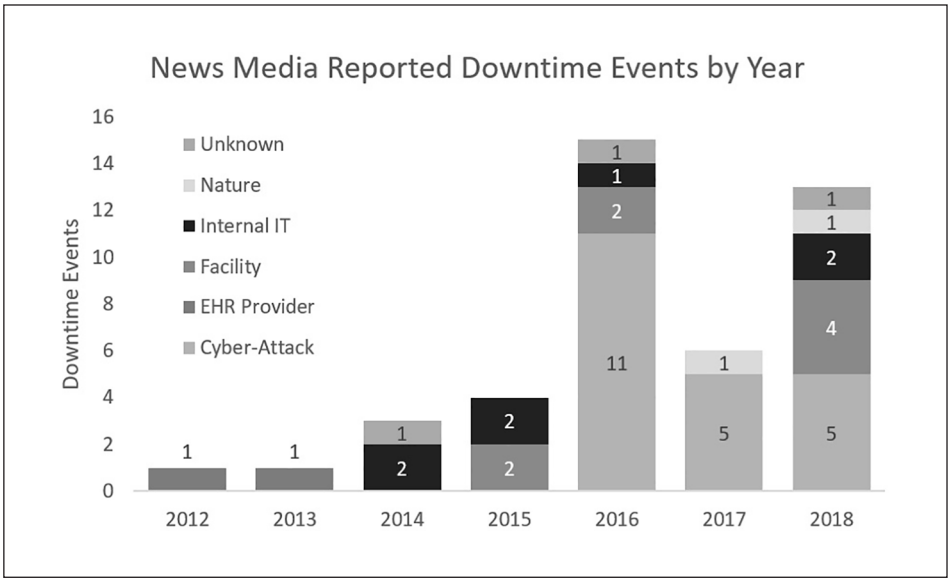

Figure 2. Downtime events in the US news 2012–2018 (categories defined in Table 4).

ransomware is even more challenging, as some variants have embedded code that enables silent duplication through all connected computers within a network, remaining dormant until an activation signal encrypts all infected systems at once. Many hospitals have chosen to shut down all computers during a ransomware attack; these shutdowns stop all electronic transmission of information, forcing fallback to rarely-practiced paper workflows.

According to the Identity Theft Resource Center, which tracks and reports data breaches annually, healthcare industry data breaches represented the highest proportion—at 44 percent ($n = 374$)—of all compromised records reported in 2016 ($n = 1091$).[23] Healthcare- and non-finance-based businesses led the overall proportion of breach events, reported at 55 percent ($n = 870$) and 23 percent ($n = 374$) of 2017 breaches, respectively, and such breaches have seen continued growth.[23–27] It is likely that hospital data will continue to be a desirable target for cyber-attack and compromise. While not all healthcare downtime events include a related data breach, the growing interest and value placed on healthcare data suggests that the data breach issue will continue to grow. The upward trends in cyber-breaches may make healthcare systems prone to excessive amounts of downtime during which alternative methods and contingency plans need to be utilized.

Recent trends suggest cyber-attacks on hospital and EHR data systems are likely to increase. EHR systems are expanding both in terms of extent of patient information and recent integration of interconnected mobile technologies, providing new avenues for access. The EHR information is comprehensive enough that it could be possible for a "medically insured identity" to be compromised and sold, similar to how credit card numbers and legal identities have been compromised and sold in the past. A recent white paper suggests that an individual's basic identity information such as a social security number is valued at US$1 on the black market, while an individual's healthcare data are valued at US$50, and some indicate the value disparity may be even greater.[28] Also, a breach of this nature would constitute a Health Insurance Portability and Accountability Act (HIPAA) privacy violation for failure to protect the patient's information and incur significant fines and potential lawsuits for the institution found to be responsible for protecting that data. In most of the downtime events to date, cyber-criminals have elected to disrupt operations and hold the computer systems hostage, often demanding monetary ransom to allow the hospital to regain control of its computers.[29–31] Some of the hospitals targeted for cyber-attack have admitted to potential breaches of their patient information databases.[32–34] Currently, authorities do not advise hospitals to pay the ransom demand, because it is not always assured that the hackers will return control of the systems, as the Kansas Heart Hospital encountered in 2016.[35,36] As hackers evolve their methods with security developments, and as Internet-connected healthcare devices increase, it is unlikely that the cyber-attack threat will ever be completely eliminated.

Scoping review of downtime research

In Figure 1, 1764 studies were found to be potentially related to downtime; 1724 studies were found to be related to biomedical research where the search strings returned false positives. After elimination of the false positives, 40 studies were reviewed in full, with 29 removed based on failure to meet all inclusion criteria, and 10 studies were included within the scope of this review. Table 5 summarizes the reviewed papers using the criteria described above.

A concentration on specific downtime events was present in 70 percent ($n = 7$) of the literature, potentially related to growing interest in the area. However, this review suggests a general gap in quantifying the impacts of downtime on healthcare systems and patient safety despite the apparent high frequency of events. One possible reason could be the lack of, or limited access to, sufficient viable data from downtime events to statistically test hypotheses.[10] In particular, only two studies[13,39] studied the outcomes of downtimes. Hanuscak et al.[13] surveyed pharmacy staff who had experienced an EHR downtime to uncover the nature and the frequency of medication errors during downtime events. The study found a total of 39 medication errors occurring during downtime events in 1 year, 14 of which impacted the patient, with one mistake resulting in an increased length of stay. Sittig et al.[39] surveyed 50 hospitals that had successfully implemented an EHR into their system; 96 percent of the hospitals responded that they had experienced at least one unplanned

Table 5. Scoping review summary.

Citation	Focus	Method	Subjects	Conclusion
Hanuscak et al.[13]	Determination of the cause and frequency of medication errors during computer downtime.	Online survey	Individual clinicians from a sample of 78 identified hospitals.	Need for more attention to downtime contingency plans; errors occur despite established backup systems.
Huryk[37]	Nursing staff attitudes toward HIT.	Literature search	Practicing nurses	Attitudes are generally positive, but with concerns for slowdowns and downtime.
Genes et al.[38]	After-action reporting of a medical center's response to an unplanned EHR downtime.	Review of after-action reports	Hospital working through a computer compromise due to broken patch in software update.	Definite impact to emergency department performance with compromised computer systems; patients noted as leaving without receiving care.
Sittig et al.[39]	Hospital survey of EHR downtime contingency practices and compliance with SAFER.	Survey of hospital practices.	A total of 57 hospitals with successful EHR adoption.	EHR downtime fairly common, most hospitals only achieved partial compliance with SAFER. Three hospitals indicated patient harm incident due to downtime.
Oral et al.[40]	Alteration of procedures during downtime involving advance ordering, printing from analyzers, and EHR scanning.	Chart review	Random selection of ED and ICU patients.	Procedures improved laboratory performance over prior downtime. Need for clinician support and an interdisciplinary team to create procedures.
Bulson et al.[41]	Historical downtime event analysis with suggestions for future, integration of emergency protocols in downtime response.	Case study of incident management implementation.	Hospital organization.	Reduction in the number of downtime events post integration, improve response with emergency management response.
Kashiwagi et al.[42]	Development of an organizational toolkit for downtime protocol development.	Case study of organizational process to develop and maintain downtime readiness.	Hospital organization	Benefit to multidisciplinary team identifying organizational needs and improvement to enhancement of existing downtime plans.
Larsen et al.[8]	Analysis of voluntary patient safety event data.	Open coding of free text content in downtime relevant reports.	Incidents reported at multi hospital organization.	Frequent occurrence of medication and lab related issues in addition to complications in patient identification and communication of clinical information. Adherence to downtime procedures may not be consistent.
Little et al.[43]	Use of after-action reporting to inform future downtime development.	Review of after-action reports.	Teaching hospital	Significant benefits in after-action reviewing but the time-consuming aspect may limit widespread adoption.
Zhao et al.[44]	Changes in communication patterns during downtime.	Interviews	General surgery residents.	Need for face-to-face interaction during downtime increases team cohesiveness and collaboration in the organization.

HIT: health information technology; EHR: electronic health record; SAFER: Safety Assurance Factors for Electronic Health Record Resilience; ED: emergency department.

downtime event within the prior 3 years. In addition, three hospitals were able to attribute some form of patient harm in one or more patients during a downtime event of any type. Despite the predominantly negative presentation of downtime, Zhao et al.[44] indicate that downtime events can have a positive impact, suggesting that the lack of computer systems forces face-to-face interactions and collegiality to increase in the opinion of surgical residents.

Current state of downtime preparation from research literature

The current body of research supports contingency planning for downtime events of any origin; however, in the face of the growing cyber-attack-based threat, robust downtime contingency planning is becoming more critical and warrants more attention.[10] The approaches recently published[8,39–42,45] vary in departmental scope, technical approach, and healthcare worker involvement. In most reviewed downtime events, clinical staff had been reported as making their own downtime procedures and exposing patients to new risks, such as delay in care, increase incidence of wrong dose, and wrong medication administration.[8,10,46] While the reasons for these unsanctioned adaptations are unknown, possible reasons could be the absence of official downtime procedures that support continuing necessary work and perception among front-line staff that the unsanctioned adaptation is better than existing procedures. Human-centered efforts focused on the front-line staff behaviors, adaptations, and obstacles could shed more light on this issue.

The fragmented and relatively sparse literature retrieved in this scoping review indicates that there is significant opportunity for numerous and simultaneous mixed-methods explorations into downtime planning. The literature retrieved ranged from a systematic review of sentiments published regarding healthcare informatics seen in the works of Huryk[37] to Zhao et al.,[44] conducting interviews directly with surgical residents who had to work through a downtime event during their residency.

Opportunities to improve future downtime handling

In terms of developing regulatory guidance, Sittig et al.[39] utilized organizational survey responses about downtime handling. The responses helped to inform the Safety Assurance Factors for Electronic Health Record Resilience (SAFER) guides which are currently the accepted best practices for EHR implementation.[47] Also significant is the study of Little et al.[43] in which the after-action sessions from a downtime event formally guided revision to procedures to be implemented in future downtimes. Larsen et al.[8] utilized voluntarily submitted downtime incident reports from a range of departments to develop suggestions for improvements to downtime, finding interdepartmental communication of downtime and formal downtime training to be recurring issues. Bulson et al.[41] proposed that hospitals should deploy their incident command procedures in response to a downtime event (similar to deploying procedures for a hurricane) and demonstrated that such actions could reduce downtime event duration by as much as 48 percent per month.

The recent increase in the number of downtime events in the last decade, while unfortunate, has yielded sufficient organizational data and employee experiences to encourage in-depth downtime studies in the future. However, this review shows that the wealth of organizational experiences is not well leveraged yet. Future studies should focus on and utilize the experiential knowledge that most, if not all, hospitals possess from downtimes. This experiential knowledge may be obtained using techniques similar to the after-action reporting analysis from Genes et al.[38] and Little et al.,[43] the general historical review from Bulson et al.,[41] or the survey data collection from Sittig et al.[39] Continued research into the abstract concept of downtime events without regarding the available concrete experiences misses an opportunity to expand our knowledge of downtime. Similarly, in

order to move beyond the accepted belief that downtime events impact safety and performance in general, analyzing records of prior events can identify specific areas of the hospital that are heavily impacted and, therefore, should be the focus for improvement efforts.

Expanding current best practice and guidelines

In its current iteration, the SAFER guides indicate that procedures be developed for downtime events, that the procedures encompass communication plans, and that they are made readily available, with staff aware of and trained on those procedures. Despite these guidelines, the SAFER falls short in specifying how the downtime procedures should be developed. The present regulatory and guideline instructions to have a plan in place and to practice it are insufficient for downtime readiness, especially when faced with increasing threats as the valuation of health information increases. Work is needed to provide detailed best practice guidance on downtime plan development and assessment.

Limitations

The scoping review of news media articles is limited to publicly acknowledged downtime events. It is likely that there are other events outside the public record. Many hospitals may choose to protect the knowledge that an incident has even occurred. Without a news media report of the event, external stakeholders may not become aware of the frequency and severity of downtime events and may develop a biased risk perception related to downtimes. The same concerns for acknowledging a downtime event may also hinder researchers from gaining access to better study the downtime issue. Furthermore, any existing data from a downtime event are likely from a period of significant organizational and technological disruption, making data quality an issue.

Conclusion

The risk of a hospital experiencing an EHR downtime event is ever-present and potentially growing. Present research efforts are starting to examine downtime readiness and planning, but many studies may miss the mark by not incorporating the organizational knowledge available from prior events. The base of healthcare workers who now have experience working through downtime events and any associated records from those prior events should be leveraged where possible in holistic user-centered frameworks for study and improvement.

Regardless of the origin, downtime events should be planned for and those plans practiced. While a downtime event is complicated and chaotic, the risk in waiting to determine the origin before reacting—especially when there is potential breach of patient data ongoing—places patients' information and the hospital at significant financial risk. Hospitals need to be prepared to identify the origin rapidly and respond appropriately. While ideally the shutdown of computer systems should be avoided, it may be necessary. Delays in enacting such a response could result in significant breach of patient data and financial cost to the organization.

Researchers should make use of the existing organizational knowledge to understand the downtime events in detail. While each event is unique, the healthcare workers and event documentation can be utilized to explore aspects of resilience, for example, in the context of work-as-imagined versus work-as-performed.[48–51] This approach would be particularly useful to unpack the issues surrounding unsanctioned downtime procedures enacted by individuals, to identify why the procedures are being employed, and what gaps motivate them.

The study of downtime procedures and development of operational contingency plans to continue care are critical to modern healthcare. While information technology specialists may develop more secure data systems and detection programs, those who seek to compromise or disrupt healthcare information technology systems will continue to advance their methods as well. There will always be motivation to compromise healthcare data, and so cyber-attack based-downtimes in particular will likely continue indefinitely. These findings from the limited relevant literature highlight the importance of proactive measures and resilience to address potentially complex downtime scenarios to come.

Acknowledgements

The authors would like to thank Jacob M. Kolman for his editorial assistance in the preparation of this manuscript.

Author contributions

Each author contributed to the conception or design of the work, data analysis and interpretation, critical revision of the article, and final approval of the version to be published.

Declaration of conflicting interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article.

ORCID iD


Ethan P Larsen https://orcid.org/0000-0001-6599-4577

References

1. Blumenthal D. Launching HITECH. *New Engl J Med* 2010; 362(5): 382–385.
2. Henry J, Pylypchuk Y, Searcy T, et al. Adoption of electronic health record systems among U.S. *non-federal acute care hospitals:* 2008-2015, 2016, https://www.healthit.gov/sites/default/files/briefs/2015_hospital_adoption_db_v17.pdf
3. Bates DW and Gawande AA. Improving safety with information technology. *New Engl J Med* 2003; 348(25): 2526–2534.
4. Blumenthal D and Tavenner M. The "meaningful use" regulation for electronic health records. *New Engl J Med* 2010; 363(6): 501–504.
5. Buntin MB, Burke MF, Hoaglin MC, et al. The benefits of health information technology: a review of the recent literature shows predominantly positive results. *Health Affairs* 2011; 30(3): 464–471.
6. Wolfstadt JI, Gurwitz JH, Field TS, et al. The effect of computerized physician order entry with clinical decision support on the rates of adverse drug events: a systematic review. *J Gen Int Med* 2008; 23(4): 451–458.
7. Campbell EM, Sittig DF, Guappone KP, et al. Overdependence on technology: an unintended adverse consequence of computerized provider order entry. *AMIA Annu Symp Proc* 2007; 9: 94–98.
8. Larsen EP, Fong A, Wernz C, et al. Implications of electronic health record downtime: an analysis of patient safety event reports. *J Am Med Inform Assoc* 2017; 25(2): 187–191.
9. ASC Communications. Digital extortion: 26 things to know about ransomware, 2016, http://www.beckershospitalreview.com/healthcare-information-technology/digital-extortion-26-things-to-know-about-ransomware.html (accessed 16 October 2018).
10. Larsen EP (2018) *Macroergonomics to understand factors impacting patient care during electronic health record downtime*. PhD Thesis, Virginia Tech, Blacksburg, VA, USA, https://vtechworks.lib.vt.edu/handle/10919/85041

11. McDermott IE. Ransomware: tales from the CryptoLocker. *Online Search* 2015; 39(3): 35–37.
12. Ash JS, Sittig DF, Campbell EM, et al. Some unintended consequences of clinical decision support systems. *AMIA Annu Symp Proc* 2007; 2007: 26–30.
13. Hanuscak TL, Szeinbach SL, Seoane-Vazquez E, et al. Evaluation of causes and frequency of medication errors during information technology downtime. *Am J Health Syst Pharm* 2009; 66(12): 1119–1124.
14. Tricco AC, Lillie E, Zarin W, et al. PRISMA extension for scoping reviews (PRISMA-ScR): checklist and explanation. *Ann Intern Med* 2018; 169(7): 467–473.
15. Moher D, Liberati A, Tetzlaff J, et al. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *BMJ* 2009; 339: b2535.
16. ASC Communications. Temporary power outage affects dozens of hospitals' access to medical records, 2012, https://www.beckershospitalreview.com/healthcare-information-technology/temporary-power-outage-affects-dozens-of-hospitals-access-to-medical-records.html (accessed 2 August 2019).
17. Spitzer J. The impact of hurricanes: 5 questions with Schneider Regional Medical Center CIO Cameron Aust on paper charting, water-damaged tech, 2018, https://www.beckershospitalreview.com/ehrs/the-impact-of-hurricanes-5-questions-with-schneider-regional-medical-center-cio-cameron-aust-on-paper-charting-water-damaged-tech.html (accessed 29 November 2018).
18. Raths D. Coping with a prolonged EHR downtime, 2018, https://www.healthcare-informatics.com/article/ehr/coping-prolonged-ehr-downtime (accessed 29 November 2018).
19. Monica K. System-wide epic EHR downtime affects 24 Sutter Health Hospitals, 2018, https://ehrintelligence.com/news/system-wide-epic-ehr-downtime-affects-24-sutter-health-hospitals (accessed 29 November 2018).
20. Murphy K. Ransomware leads to EHR downtime at DC-area health system, 2016, https://ehrintelligence.com/news/ransomware-leads-to-ehr-downtime-at-dc-area-health-system (accessed 29 November 2018).
21. Monica K. Allina health recovers from system-wide stint of EHR downtime, 2018, https://ehrintelligence.com/news/allina-health-recovers-from-system-wide-stint-of-ehr-downtime (accessed 30 December 2019).
22. Hansberry A, Lasser A and Tarrh A. Cryptolocker: 2013's Most Malicious Malware, 2014, https://www.cs.bu.edu/~goldbe/teaching/HW55815/cryptolockerEssay.pdf (accessed 29 October2018).
23. Identity Theft Resource Center. *2016 end of year report*. Annual Report, 18 January 2017. San Diego, CA: Identity Theft Resource Center, https://www.idtheftcenter.org/2016databreaches/ (accessed 12 November 2018).
24. Identity Theft Resource Center. *2014 data breach reports*. Annual Report, 31 December 2014. San Diego, CA: Identity Theft Resource Center, https://www.idtheftcenter.org/2014-data-breaches/ (accessed 12 November 2018).
25. Identity Theft Resource Center. *2015 data breach reports*. Annual Report, 29 December 2015. San Diego, CA: Identity Theft Resource Center, https://www.idtheftcenter.org/2015-data-breaches/ (accessed 12 November 2018).
26. Identity Theft Resource Center. *Overview 2005-2016*. Overview Report, January 2017. San Diego, CA: Identity Theft Resource Center, https://www.idtheftcenter.org/images/breach/Overview2005to2016Finalv2.pdf (accessed 12 November 2018).
27. Identity Theft Resource Center. *2017 annual data breach year-end review*. Annual Report, 22 January 2018. San Diego, CA: Identity Theft Resource Center, https://www.idtheftcenter.org/2017-data-breaches/ (accessed 12 November 2018).
28. Coulter C. HITECH, compliance, and the growth of the ransomware economy: a devastating assault on healthcare (White paper). *Cylance*, 2018, https://www.cylance.com/content/dam/cylance/pdfs/white_papers/AssaultOnHeathcare.pdf (accessed 16 October 2018).
29. McCarthy J. MedStar attack found to be ransomware, hackers demand Bitcoin, 2016, https://www.healthcareitnews.com/news/medstar-attack-found-be-ransomware-hackers-demand-bitcoin (accessed 9 October 2018).

30. Siwicki B. Hollywood Presbyterian declares emergency after hackers cut off data, demand $3.4 million ransom, 2016, http://m.healthcareitnews.com/news/hollywood-presbyterian-declares-emergency-after-hackers-cut-data-demand-34-million-ransom?platform=hootsuite (accessed 16 October 2018).
31. Sullivan T. More than half of hospitals hit with ransomware in last 12 months, 2016, http://m.healthcareitnews.com/news/more-half-hospitals-hit-ransomware-last-12-months (accessed 16 October 2018).
32. Monica K. Computer virus potentially exposes PHI of 2.5K at OR clinic, 2017, https://healthitsecurity.com/news/computer-virus-potentially-exposes-phi-of-2.5k-at-or-clinic (accessed 29 October 2018).
33. Snell E. Metropolitan urology ransomware attack affects 18K patients, 2017a, https://healthitsecurity.com/news/metropolitan-urology-ransomware-attack-affects-18k-patients (accessed 29 October 2018).
34. Snell E. Urology Austin ransomware attack possibly affects 279K, 2017b, https://healthitsecurity.com/news/urology-austin-ransomware-attack-possibly-affects-279k (accessed 29 October 2018).
35. Landi H. Kansas Heart Hospital hit with ransomware; hackers do not unlock files after receiving ransom payment, 2016, https://www.healthcare-informatics.com/news-item/kansas-heart-hospital-hit-ransomware-hackers-do-not-unlock-files-after-receiving-ransom (accessed 30 October 2018).
36. United States Government. How to protect your networks from ransomware (File). *Federal Bureau of Investigation, United States Government*, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view (accessed 8 March 2019).
37. Huryk LA. Factors influencing nurses' attitudes towards healthcare information technology. *J Nurs Manag* 2010; 18(5): 606–612.
38. Genes N, Chary M and Chason KW. An academic medical center's response to widespread computer failure. *Am J Disaster Med* 2013; 8(2): 145–150.
39. Sittig DF, Gonzalez D and Singh H. Contingency planning for electronic health record-based care continuity: a survey of recommended practices. *Int J Med Inform* 2014; 83(11): 797–804.
40. Oral B, Cullen RM, Diaz DL, et al. Downtime procedures for the 21st century: using a fully integrated health record for uninterrupted electronic reporting of laboratory results during laboratory information system downtimes. *Am J Clin Pathol* 2015; 143(1): 100–104.
41. Bulson J, Van Dyke M and Skibinski N. Rebooting healthcare information technology downtime management. *J Bus Continuity Emer Plan* 2017; 11(1): 63–72.
42. Kashiwagi DT, Sexton MD, Souchet Graves CE, et al. All clear? Preparing for IT downtime. *Am J Med Qual* 2017; 32(5): 547–551.
43. Little CM, McStay C, Oeth J, et al. Using rapid improvement events for disaster after-action reviews: experience in a hospital information technology outage and response. *Prehosp Disaster Med* 2018; 33(1): 98–100.
44. Zhao JY, Kessler EG and Guo WA. Interprofessional communication goes up when the electronic health record goes down. *J Surg Edu* 2018; 76(2): 512–518.
45. Campos F, Luna D, Sittig DF, et al. Design, implementation and evaluation of an architecture based on the CDA R2 document repository to provide support to the contingency plan. *St Heal T* 2015; 216: 173–177.
46. Wang Y, Coiera E, Gallego B, et al. Measuring the effects of computer downtime on hospital pathology processes. *J Biomed Inform* 2016; 59: 308–315.
47. Office of the National Coordinator for Health Information Technology. Contingency planning: the safety assurance factors for EHR resilience (SAFER) guides, https://www.healthit.gov/sites/default/files/safer/guides/safer_contingency_planning.pdf
48. Hollnagel E. *Resilience engineering in practice: a guidebook*. Farnham; Burlington, VT: Ashgate, 2011.
49. Hollnagel E, Wears RL and Braithwaite J. *From safety-I to safety-II: a white paper* (White paper), 2015, https://psnet.ahrq.gov/resources/resource/29228 (accessed 8 November 2018).
50. Hollnagel E, Sujan M and Braithwaite J. Resilient health care: making steady progress. *Saf Sci* 2019; 120: 781–782.
51. Hollnagel E and Braithwaite J. *Resilient health care*. Boca Raton, FL: CRC Press, 2019.