journal homepage: www.ijmijournal.com

Contingency planning for electronic health record-based care continuity: A survey of recommended practices☆

Dean F. Sittig[a,*], Daniel Gonzalez[b], Hardeep Singh[c]

[a] University of Texas School of Biomedical Informatics and the University of Texas – Memorial Hermann Center for Healthcare Quality & Safety, Houston, TX, USA

[b] Department of Clinical Effectiveness and Performance Measurement, St. Luke's Episcopal Health System, Houston, TX, USA

[c] Houston VA HSR&D Center of Innovation at the Michael E. DeBakey Veterans Affairs Medical Center and the Section of Health Services Research, Department of Medicine, Baylor College of Medicine, Houston, TX, USA

ARTICLE INFO

Article history:
Received in revised form
22 July 2014
Accepted 29 July 2014

Keyword:
Electronic health records

ABSTRACT

Background: Reliable health information technology (HIT) in general, and electronic health record systems (EHRs) in particular are essential to a high-performing healthcare system. When the availability of EHRs are disrupted, alternative methods must be used to maintain the continuity of healthcare.

Methods: We developed a survey to assess institutional practices to handle situations when EHRs were unavailable for use (downtime preparedness). We used literature reviews and expert opinion to develop items that assessed the implementation of potentially useful practices. We administered the survey to U.S.-based healthcare institutions that were members of a professional organization that focused on collaboration and sharing of HIT-related best practices among its members. All members were large integrated health systems.

Results: We received responses from 50 of the 59 (84%) member institutions. Nearly all (96%) institutions reported at least one unplanned downtime (of any length) in the last 3 years and 70% had at least one unplanned downtime greater than 8 h in the last 3 years. Three institutions reported that one or more patients were injured as a result of either a planned or unplanned downtime. The majority of institutions (70–85%) had implemented a portion of the useful practices we identified, but very few practices were followed by all organizations.

Conclusions: Unexpected downtimes related to EHRs appear to be fairly common among institutions in our survey. Most institutions had only partially implemented comprehensive contingency plans to maintain safe and effective healthcare during unexpected EHRs downtimes.

☆ The views expressed in this article are those of the authors and do not necessarily represent the views of the University of Texas, St. Luke's Health System, or Department of Veterans Affairs.

* *Corresponding author at*: University of Texas – Memorial Hermann Center for Healthcare Quality & Safety, 6410 Fannin Street, UTPB 1100.43, Houston, TX 77030, USA. Tel.: +713 500 7977; fax: +713 500 0766.

E-mail address: dean.f.sittig@uth.tmc.edu (D.F. Sittig).

http://dx.doi.org/10.1016/j.ijmedinf.2014.07.007
1386-5056/© 2014 Elsevier Ireland Ltd. All rights reserved.

1. Introduction

The United States of America's (USA) Health Information Technology for Economic and Clinical Health (HITECH) Act of 2009 [1] has led to increased adoption and use of health information technologies (HIT), particularly use of electronic health record systems (EHRs) [2] in previously paper-based healthcare systems. As such, healthcare processes are increasingly dependent on availability of HIT. However, HIT is not infallible and is subject to disruptions and downtimes that may threaten the continuity of operations [3] and cause adverse patient care outcomes, both of which can lead to financial and operational difficulties for healthcare organizations [4].

Over the last several years, there have been several highly publicized, widespread (i.e., affecting multiple facilities simultaneously), extended (i.e., lasting greater than 12 h) EHRs downtimes in the USA and Canada [5–12]. EHRs downtimes have also been reported in China [13]. However, there is little published description of practices that institutions are using to maintain the safety and effectiveness of continuous healthcare delivery while EHRs are unavailable. Our study goal was to describe EHRs downtime practices across a variety of healthcare institutions and identify practices that could be useful for planning for and dealing with EHRs unavailability. By describing and highlighting important elements of contingency plans across a variety of EHRs-enabled healthcare systems, our goal was to provide healthcare organizations with more comprehensive information to prepare for the risks of potential operational disruptions and avoid harm to patients.

2. Methods

2.1. *Survey development*

Before survey development, we reviewed the existing literature and did not find any previous survey that systematically described or assessed EHRs downtime practices within healthcare organizations. Therefore, we developed a survey for the purposes of the present study. The conceptual foundation for the survey was Sittig and Singh's eight-dimension sociotechnical model of safe and effective HIT use. Although not specific to EHRs downtime, this model describes the complex interactions within eight components or "dimensions" of a HIT system and/or process [14]. These include hardware and software; clinical content; user interface; people; workflow and communications; organizational policies, procedures, and the physical environment; external rules, regulations, and pressures; and system measurement and monitoring. By applying these dimensions to downtime processes, we developed survey items that addressed multiple, interrelated aspects of downtime preparedness and processes.

Following review of published articles describing noted EHRs downtimes along with articles describing best practices for contingency planning, we conducted fact-finding interviews (April–September 2011) at three large academic institutions and two community hospitals to elicit policies, procedures, and practices related to EHRs downtimes. Interview participants included IT personnel and hospital administrators. These interviews revealed a large degree of heterogeneity between institutions in policies, procedures, and practices and informed the development of items related to each dimension of our sociotechnical conceptual model. For example, in the "people" dimension, representatives from all institutions mentioned the need to train key personnel on appropriate downtime procedures, although there were significant differences in the type and extent of training offered. In addition to interviews, we observed a planned downtime (November 2011) at one of the academic hospitals to enable a better understanding of practices related to the "workflow and communication" dimension. Thus, a combination of data from interviews, our observations of a planned downtime, and a pre-publication copy of the American Health Lawyers Association (AHLA) Emergency Preparedness Checklist [15], developed by a team of lawyers with extensive experience in managing the aftermath of unexpected EHRs downtimes, provided information required to create items for our EHRs downtime survey. These data also provided us with a conceptual basis to discover potentially useful practices for EHRs contingency planning. Early drafts of the survey were pilot tested with five subjects, not involved in the original survey development, who had extensive experience working in EHRs-enabled healthcare organizations. Several questions and many of the response options were modified in response to their feedback. The final version of the survey consisted of 96 multiple choice and free text items where respondents could describe their institutions' policies, procedures and practices during scheduled or unscheduled downtimes (see Appendix A).

2.2. *Survey administration*

We administered an online version of the downtime survey through a web-based questionnaire hosting service (https://www.SurveyMonkey.com). Following approval by our local institutional review board (December 2011), the survey was distributed to the Scottsdale Institute's member email distribution list in February 2012 [16]. At the time of the survey, the Scottsdale Institute consisted of 59 member organizations focused on improving their organization's HIT practices. The Scottsdale Institute reported that their members have a mean, Health Information and Management Systems Society (HIMSS) Electronic Medical Record Adoption Model (EMRAM) score of 4.6. In addition, 75% of these members reported a score of 4 or greater. Healthcare organizations with HIMSS EMRAM scores of 4 or greater are using computerized physician order entry with clinical decision support, have implemented the major ancillary systems (i.e., pharmacy, laboratory, and radiology), have a clinical data repository for results review, and have an electronic medication administration record. These organizations are likely at much greater risk in the event of system unavailability for any reason [17]. Members included institutional leaders (e.g., chief executive officers, chief information officers, and chief financial officers) and HIT experts from large healthcare organizations across the USA. Participants were asked to base their responses on the current EHRs downtime practices of their respective organizations. One email reminder was sent to prospective participants after 2 weeks, and the survey was closed after one month.

2.3. *Survey data analysis*

Survey responses were downloaded from the web-based survey administration tool and were analyzed using Microsoft Excel (Microsoft Corporation, Redmond, WA). We generated descriptive statistics to summarize the characteristics of respondents and their responses. Free text responses were reviewed to identify common themes and provide context for specific items.

3. Results

We received survey responses from representatives of 50 of the 59 (84%) institutional members of the Scottsdale Institute (i.e., unit of analysis was the institutional member), although not all respondents answered all questions on the survey. Respondents were either chief information officers or other personnel directly responsible for maintaining the organization's HIT infrastructure. Most (96%) represented non-profit organizations, and 80% were affiliated with large (>600 bed) hospital systems. Nearly all respondents had experience with downtime events, with 95% reporting at least one unplanned downtime (of any length) in the last 3 years and 70% reporting at least one unplanned downtime greater than 8 h in the last 3 years. Three respondents reported that one or more patients were injured as a result of either a planned or unplanned downtime.

We organized survey responses according to several key hardware infrastructure components (see Table 1) and point-of-care components (see Table 2) involved in either preparing for or dealing with a downtime event. Tables 1 and 2 list for each item the percentage of positive responses (i.e., the proportion of institutional respondents who reported having the components in place), along with the corresponding sociotechnical dimension from our conceptual model. Of note, we included follow-up items to determine not only the availability of certain "backup systems" but also more detailed information about how these systems were tested and used (see Table 1). For example, all respondents reported having uninterruptable power supplies (UPS), but only 50% reported that they tested them on a monthly basis. Similarly, 96% reported having a back-up generator, but only 79% tested their generators on a monthly basis, and only 79% had more than 2 days of fuel available to keep it running.

Table 2 lists respondents' endorsement of various point-of-care system components to ensure that staff can continue to access critical information and perform needed clinical functions during planned and unplanned downtimes. Overall, about three-fourths of organizations reported having a central or hospital-wide, read-only, back-up system, and a similar proportion reported having clinic-level, read-only, back-up systems. The large majority backed up their data at least hourly. However, far fewer organizations – only a third – tested their read-only backup systems at least monthly. Other practices related to backup systems were endorsed more variably.

All respondents reported that they maintained a daily backup copy of their patient data in a secure off-site location, although less than half reported that their data was complete and encrypted, and relatively few (15%) attempted to restore their backups on a quarterly basis. In fact, two organizations reported that they had never tested their backup. All organizations trained their staff on how to handle either a planned or unplanned downtime, but less than a third (28%) had yearly, unannounced downtime drills on any shift. Sites that performed these drills followed up with clinicians to identify areas for improvement.

4. Discussion

We surveyed representatives of large integrated healthcare systems that were members of a professional organization created to share EHRs-related practices. The vast majority of these organizations were advanced EHRs users as indicated by their mean HIMSS EMRAM score of 4.6. Almost all of our respondent organizations had experienced an unplanned downtime, and most had experienced an unplanned downtime exceeding 8 h in the last 3 years. Three organizations reported patient injury had resulted from these events.

While many EHRs downtimes could be uneventful, the risk of patient injury remains. Downtime events could result in patient harm due to delays in test performance, delivery of abnormal test results, or in the administration of time-critical medications. In a subsequent on-line survey of the American Society for Healthcare Risk Management (ASHRM) and the American Health Lawyers Association (AHLA) on frequency and types of various EHR-related serious safety events, we also found downtime to be a significant issue [18]. Respondents from these organizations confirmed the findings from the Scottsdale Institute and reported similar rates and severities of events related to downtime. These data sources suggest that the risk of major system outages is likely more common and hazardous than most organizations currently plan for. For example, while all of the organizations surveyed had an off-site backup copy of their data, not all had implemented key care continuity infrastructure such as uninterruptable power supplies, backup generators, redundant paths to the Internet, and paper-based backup ordering and documentation procedures. Only three-quarters had some sort of read-only backup system capability either at the organization or clinical unit level. In light of the high rates of downtimes, potential severity of these events and potential for patient harm, it is incumbent on all organizations to take the necessary precautions required to mitigate the effects of inevitable downtime events.

Furthermore, while the vast majority of institutions had the proper system components in place, far fewer were using them completely or correctly. For example, 80% of organizations had a warm-site backup (i.e., a remote site with pre-configured hardware and network connectivity on which an organization's application software and data can be quickly loaded), but less than a third tested it at least quarterly. Similar findings were seen for other practices such as testing backup generators and encrypting backup databases. Even fewer organizations had routine measurement and monitoring systems in place to enable continuous surveillance of the infrastructure required to maintain the organization's EHRs and ensure continuity of care. For example, only 60% of organizations had a computer-generated EHRs interface error transaction log, and only half of those that did, reported that greater than

Table 1 – Overview of infrastructure for backup systems (positive responses calculated based on the percent of Scottsdale Institute members responding positively to each survey item).

Dimension	Item	Positive response
Hardware/software	*Have an uninterruptable power supply (UPS)*	100%
Workflow	Test UPS at least monthly	50%
Hardware/software	*Have a back-up generator dedicated to HIT infrastructure*	96%
Workflow	Test generator at least monthly	79%
Hardware/software	Greater than 2 days of fuel	79%
Hardware/software	Greater than 75% of power replaced by generator	68%
Hardware/software	*Have a warm site*[a] *back up*	80%
Workflow	Warm-site available in 8 h or less	78%
Workflow	Test warm site at least quarterly	31%
Workflow	Warm-site has come online	70%
Workflow	Warm-site has come online because of an emergency	33%
Workflow	Switched over to warm site before 4 h	50%
Hardware/software	*Redundant path to the internet at organizational level*	92%
Internal policy/procedure	Different internet provider as their redundant path	68%
Hardware/software	*Have an EHRs interface transaction error log*	60%
Internal policy/procedure	Greater than 75% errors investigated and fixed	50%

[a] Remote site with pre-configured hardware and network connectivity on which an organization's application software and data can be quickly loaded.

Table 2 – Overview of point-of-care components during downtimes (positive responses calculated based on the percent of Scottsdale Institute members responding positively to each survey item).

Dimension	Item	Positive response
	Practices related to downtime, read-only EHR	
Hardware/software	*Have a network-accessible, hospital-wide read-only back-up*	77%
Workflow	Backup data updated at least every hour	85%
Workflow	Test central read-only back-up system at least monthly	33%
User interface	Downtime, read-only version of EHRs is clearly marked	62%
User interface	Downtime, read-only EHRs disabled during normal operation	45%
Hardware/software	*Have a local, clinic-level read-only back-up system*	75%
Workflow	Update data in clinic-level read-only back-up system at least hourly	90%
Internal policy/procedure	Clinicians activate clinic-level read only back-up system	50%
External rules and regulations	Read only clinic-level back-up system generic password protected	52%
Workflow	Test clinic-level read-only back-up system at least monthly	33%
Hardware/software	Clinic-level read-only back-up system connected to UPS	94%
	Practices related to data backup	
Content	*Back up patient data in a secure, off-site location*	100%
Content	Data at off-site location is complete and encrypted	48%
Workflow	Back-up their data to an off-site location daily	100%
Workflow	Organization conducts at least quarterly tests to ensure data can be reloaded	15%
Content	Back-up includes complete, up to date copy of all data used to configure system	96%
Workflow	Organization backs up data before every upgrade	100%
Personnel	*Organization trains staff on what to do in planned and unplanned downtime*	100%
Workflow	*Have a yearly unannounced downtime drill*	28%
Monitoring and surveillance	Follow up on drills looking for opportunities for improvement	100%
Internal policy/procedure	*Have a written downtime policy and procedure*	94%
Workflow	Review and update downtime policy at least every 2 years	41%
Workflow	Planned downtime communication strategy via email	81%
Workflow	Unplanned downtime communication strategy via email	59%
Workflow	Out of band downtime communication strategy (pager, overhead, people)	92%
	Availability of paper forms before downtime	
User interface	Order and document medications	88%
User interface	Order and document laboratory tests and results	92%
User interface	Order and document radiology tests and results	92%
User interface	Document RN observations and care delivered	83%
User interface	Document MD observations and plans	79%
Workflow	Enough paper on hand to last >48 h	43%
Personnel	Staff trained in use of paper forms	92%

75% of the errors identified were investigated and fixed. Our findings thus suggest the need for increasing the resilience of the existing hardware and software infrastructure as well as streamlining policies, procedures, and people required to implement, test, and maintain these systems [19] in order to achieve the promise of transforming our healthcare delivery system through state-of-the-art health information technology.

4.1. *Need for best practices to avoid EHR-related disruptions and downtimes*

A recent USA Institute of Medicine report recommends that healthcare organizations have contingency plans in place to avoid if possible and, if not, to mitigate any potential issues related to planned and unplanned EHRs downtimes [20]. While there are several USA federal regulations (e.g., HIPAA Security Rule 45 CFR Sec. 164.x) and compliance standards (e.g., USA Center for Medicare and Medicaid (CMS) Services' Hospital Conditions of Participation [21] and The USA Joint Commission) that cover legal aspects of EHR-related disruptions and downtimes [22], to our knowledge a list of best practices for managing these disruptions that focus on patient safety does not exist in the USA or abroad.

While both CMS and the Joint Commission recognize safety issues posed by EHRs downtimes and the loss of continuous access to patient information, healthcare providers are generally expected to establish their own record maintenance and security systems to ensure that the EHRs meets their requirements and is reliably available when needed. Literature related to downtime preparedness emphasizes the need to have an EHRs disaster plan that is tested, accessible, and regularly audited [23], including provisions for assessing employees' knowledge of downtime practices (e.g., testing an organization's plan in a "fire drill"-type scenario) [24]. Experiences along the USA's gulf coast during hurricanes Katrina (August 2005) [25] and Ike (September 2009) [26] as well as along the New York/New Jersey coast during hurricane Sandy (October 2012) [27] illustrated the necessity for such contingency plans, providing useful insights regarding needs for internal communications and widespread clinician access to patient information [28]. Some guidance is available from the American Health Lawyer's Association's (AHLA) Emergency Preparedness, Response and Recovery Checklist, which provides a few items to help healthcare organizations prepare their EHRs services for emergencies [15] Although many professionals have shown the need for planning and some have suggested a limited number of best practices or tips, there is no comprehensive guidance to inform the development of EHRs-specific downtime best practices. Thus, institutions might have a highly variable spectrum of contingency planning practices, and it is unknown to what extent any of the practices are implemented or used. Therefore, while the evidence in this area is still emerging, there is a pressing need to develop appropriate downtime procedures to minimize risks to patients [29].

The USA HIPAA Security Rule, which applies to healthcare providers as "covered entities" and to their "business associates" (which includes EHRs vendors), is the USA federal law that most explicitly addresses contingency planning related to electronic health records. Its general requirements include ensuring the "availability" of all electronic protected health information, as well as its confidentiality and integrity, USA Security Rule 45 CFR Sec. 164.306(a)(1), and protecting against reasonably anticipated threats or hazards to the security or integrity of such information, USA Security Rule 45 CFR Sec. 164.306(a)(2). This standard has implementation specifications on data backup plans, disaster recovery plans, emergency mode operation plans, testing and revision procedures, applications and data criticality analysis. These provisions of the HIPAA Security Rule overlap with and reinforce the practices we identified in our survey on avoiding and mitigating downtimes.

4.2. *Developing potentially useful practices to avoid EHR-related disruptions and downtimes*

Our survey findings from the work with the Scottsdale Institute suggested the need for best practices to avoid EHRs downtimes. It also suggested what some of those practices might be. We used the findings from our survey to inform work on a separate project, funded by the Department of Health and Human Services (DHHS) Office of the National Coordinator for Health Information Technology (ONC) to develop self-assessment guides in 9 areas, including contingency planning, to optimize the safety and safe use of EHR. These guides are called the Safety Assurance Factors for EHRs Resilience (SAFER) Guides (Available at: http://www.healthit.gov/safer/) and the recommended practices in these guides are centered on six key principles: data availability, data quality and integrity, data confidentiality, complete and correct EHRs system use, system usability, and system surveillance and monitoring [30]. The Contingency Planning SAFER Guide ("Downtime Guide") was developed based upon prior research, including the survey described above, expert input, and field research, including site visits to 9 healthcare organizations ranging in size from large, multi-site, integrated health care organizations to single physician practices [31]. Interview data from key representatives provided additional context to develop our list of recommended practices on contingency planning (see online appendix).

4.3. *Use of contingency planning SAFER guide as a resource to plan for downtimes*

In the SAFER Guide, we provide examples of activities that institutions could perform in order to operationalize good clinical practices and, where possible, cited additional literature to support our recommendations. As highlighted in some of the open-ended comments from our survey, we acknowledge that many of the recommended practices are not entirely under the control of the healthcare organization. Often EHRs developers must create new, or modify existing functionality, to enable organizations to configure their products to fully implement a practice. For example, when the EHRs is down and EHRs users must rely on the "read only" back-up, EHRs developers often control whether the user interface of the read-only system is clearly distinguishable from that of the "live" system (recommendation #9). This is not a feature that is easily "configurable" by the EHRs implementation team within the healthcare organization.

The Contingency Planning SAFER Guide acknowledges overlap with the HIPAA Security Rule requirements on contingency planning, and encourages healthcare providers and their business associates to use the SAFER Guides in conjunction with required compliance with the Security Rule. The Contingency Planning SAFER Guide includes references to provisions of HIPAA that are implicated by the recommended practices. Following the recommended practices in the SAFER Guide could help with compliance with the HIPAA Security Rule, but the HIPAA Security Rule is broader than the recommendations in the Contingency Planning SAFER Guide.

In the future, healthcare organizations of all sizes could use contingency planning guides, such as the ones we developed, to help them assess their readiness for the inevitable system outages and identify areas for improvement. Over time and in organizations at different points in their development of an EHR-enabled healthcare system, we anticipate that these guides will need to be modified. Finally, as we learn more about the impact of EHRs on patient safety, we expect that the standards that these recommendations reflect, will progressively become more stringent.

5. Study limitations

The major limitation of the survey was that respondents were from a relatively small number of USA-based, large, integrated, hospital-centric, healthcare delivery systems with significant experience in implementation, use, and ongoing optimization of their HIT and EHRs infrastructures. There were no small, self-contained ambulatory medical practices involved. We do not know how the survey findings on compliance with the practices identified in the survey would differ if the respondents were ambulatory practices. In addition, the goal of the survey was to explore the breadth of the current status of organizations with regards to contingency planning and suggest a minimum set of requirements. However, it may be difficult to get people responsible for purchasing, installing, and maintaining these systems to agree to anything more stringent [19]. Finally, with regard to the development of the "best practices," it is possible that new technologies, for example, tapeless backup systems that enable backups to be completed much faster and promise faster restore times [32], could make specific recommendations obsolete, although the underlying principles on which they are based will remain valid.

6. Conclusion

Extended EHR-related downtimes occurred in the majority of organizations surveyed. Most institutions had only partially implemented comprehensive contingency plans to maintain safe and effective healthcare during unexpected EHRs downtimes. Preparing for these unexpected downtimes should be a part of every EHR-enabled healthcare organization's overall patient safety strategy. The best practices identified in this survey and in the SAFER Guide on Contingency Planning could help the EHR-enabled healthcare system prepare for continuity of operations to ensure safe and effective healthcare.

Summary points

What was already known on the topic

- Reliable health information technology (HIT) in general, and electronic records (EHRs) in particular are essential to a high-performing healthcare system.
- When the availability of EHRs are disrupted, alternative methods must be used to maintain the continuity of healthcare.

What this study added to our knowledge

- Unexpected downtimes related to EHRs appear to be fairly common among healthcare institutions.
- Most institutions have only partially implemented comprehensive contingency plans to maintain safe and effective healthcare during unexpected EHR downtimes.

Funding statement

Dr. Singh is partially supported by the Houston VA Health Services Research & Development Center of Innovation (CIN 13–413). The funders had no role in the design and conduct of the study; collection, management, analysis, and interpretation of the data; and preparation, review, or approval of the manuscript; and decision to submit the manuscript for publication.

Author contributions

All authors made substantial contributions to the conception or design of the work; or the acquisition, analysis, or interpretation of data for the work; and drafting the work or revising it critically for important intellectual content; and final approval of the version to be published; and agreement to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

Conflict of interest

The authors have no conflicts of interest.

Acknowledgements

We thank Shelli Williamson, Executive Director of the Scottsdale Institute and Ricki Levitan for their help and support of our survey, as well as all the Scottsdale member organizations who participated in the survey.

Appendix A. Supplementary data

Supplementary material related to this article can be found, in the online version, at doi:10.1016/j.ijmedinf.2014.07.007.

REFERENCES

[1] Health and Human Services, Federal Register: HIPAA Administrative Simplification: Interim Final Rule, Department of Health and Human Services, October 2009, http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/enfifr.pdf (retrieved 14.12.11).

[2] A. Wright, S. Henkin, J. Feblowitz, A.B. McCoy, D.W. Bates, D.F. Sittig, Early results of the meaningful use program for electronic health records, N. Engl. J. Med. 368 (February (8)) (2013) 779–780, http://dx.doi.org/10.1056/NEJMc1213481.

[3] P. Kilbridge, Computer crash – lessons from a system failure, N. Engl. J. Med. 348 (March (10)) (2003) 881–882.

[4] D.F. Sittig, H. Singh, Legal ethical and financial dilemmas in electronic health record adoption and use, Pediatrics 127 (April (4)) (2011) e1042–e1047, http://dx.doi.org/10.1542/peds.2010-2184.

[5] J. Merrick, 'Serious' computer crash hits hospital trusts, Daily Mail (July 31, 2006) 3984, Available at: http://www.dailymail.co.uk/news/article-77/Serious-crash-hits-hospital-trusts.html

[6] L. Rosencrance, Problems abound for Kaiser e-health records management system: an internal report details hundreds of technical issues and outages, Computer World (November 13, 2006) 9005, Available at: http://www.computerworld.com/s/article/004/Problems_abound_for_Kaiser_e_health_records_management_system_

[7] B. Brewin, August VA systems outage crippled western hospitals, clinics, Government Executive (October 5, 2007), Available at: http://www.govexec.com/defense/2007/10/august-va-systems-outage-crippled-western-hospitals-clinics/9/2546

[8] NPR Staff, Anti-virus program update wreaks havoc with PCs, National Public Radio (April 21, 2010), Available at: http://www.npr.org/templates/story/story.php?storyId=126168997&sc=17&f=1001

[9] C. Terhune, Patient data outage exposes risks of electronic medical records, Los Angeles Times (August 3, 2012), Available at: http://articles.latimes.com/2012/aug/03/business/la-fi-hospital-data-outage-20120803

[10] K. Robertson, Sutter electronic records system crashed, Sacram. Bus. J. 27 (August 2013), Available at: http://www.bizjournals.com/sacramento/news//08/27/sutter-electronic-records-system-down.html?page=all 2013

[11] E. McCann, Network glitch brings down Epic EMR, Healthcare IT News (January 28, 2014), Available at: http://www.healthcareitnews.com/news/network-glitch-brings-down-epic-emr

[12] G. Slade, System failure has docs, patients upset, Medicine Hat News (June 10, 2014), Available at: http://medicinehatnews.com/news/local-news//06/10/system-failure-has-docs-patients-upset/2014

[13] J. Lei, P. Guan, K. Gao, X. Lu, Y. Chen, Y. Li, Q. Meng, J. Zhang, D.F. Sittig, K. Zheng, Characteristics of health IT outage and suggested risk management strategies: an analysis of historical incident reports in China, Int. J. Med. Inform. 83 (2) (February 2014) 122–130, http://dx.doi.org/10.1016/j.ijmedinf.2013.10.006.

[14] D.F. Sittig, H. Singh, A new sociotechnical model for studying health information technology in complex adaptive healthcare systems, Qual. Saf. Health Care (2010) i68–i74.

[15] E. Belmont, S. Chao, A.L. Chestler, S.J. Fox, M. Lamar, K.B. Rosati, E.F. Shay, D.F. Sittig, A.J. Valenti, Emergency Preparedness Checklist for Information Technology Infrastructure and Software Applications, American Health Lawyer's Association, Washington, DC, 2013, Available at: http://www.healthlawyers.org/hlresources/PI/InfoSeries/Documents/For%20the%20Healthcare%20Executive/EHR/Emergency%20Preparedness%20Checklist%20For%20Information%20Technology%20Infrastructure%20and%20Software%20Applications.pdf

[16] The Scottsdale Institute – The healthcare executive resource for information management. Available at: http://www.scottsdaleinstitute.org/

[17] D.F. Sittig, D.C. Classen, Monitoring and evaluating the use of electronic health records—Reply, J. Am. Med. Assoc. 303 (19) (2010) 1918–1919, http://dx.doi.org/10.1001/jama.2010 591.

[18] S. Menon, H. Singh, A.N.D. Meyer, E. Belmont, D.F. Sittig, Electronic health record-related safety concerns: a cross-sectional survey, J. Healthc. Risk Manag. 34 (1) (2014), http://dx.doi.org/10.1002/jhrm.21146.

[19] M.W. Smith, J.S. Ash, D.F. Sittig, H. Singh, Resilient practices in maintaining safety of health information technologies, J. Cogn. Eng. Decis. Mak. 8 (September (3)) (2014) 265–282, http://dx.doi.org/10.1177/1555343414534242.

[20] Institute of Medicine, Health IT and Patient Safety: Building Safer Systems for Better Care, Institute of Medicine, November 2011, http://www.iom.edu/Reports/2011/Health-IT-and-Patient-Safety-Building-Safer-Systems-for-Better-Care.aspx (retrieved 14.12.11).

[21] Center for Medicare and Medicaid Services, Conditions of Participation, U.S. Government Printing Office, June 1986, http://edocket.access.gpo.gov/cfr_2004/octqtr/pdf/42cfr482.24.pdf (retrieved 14.12.11).

[22] The Joint Commission, Comprehensive Accreditation Manual Oakbrook Terrace, The Joint Commission, Oak Brook, IL, 2011.

[23] P. Spath, Health information disaster planning 101, Hosp. Peer Rev. (2002) 112–114.

[24] N.C. Nelson, Downtime procedures for a clinical information system: a critical issue, J. Crit. Care (2007) 45–50.

[25] S. Fink, The deadly choices at memorial, The New York Times (August 25, 2009), Available at: http://www.nytimes.com/2009/08/30/magazine/30doctors.html?pagewanted=all

[26] Anonymous, Texas hospital leaders say Katrina's lessons helped them better prepare for Hurricane Ike, Health Facil. Manage. 22 (1) (2009) 5–7.

[27] F. Mogul, Four NYC hospitals still closed by hurricane sandy, Kaiser Health News (November 18, 2012), Available: http://www.kaiserhealthnews.org/stories//november/19/nyc-hospitals-still-closed-hurricane-sandy.aspx 2012

[28] K.H. Gamble, Weathering the Storm, Healthcare Informatics, November 2008, http://www.healthcare-informatics.com/ME2/dirmod.asp?sid=9B6FFC446FF7486981EA3C0C3CCE4943&nm=Articles%2FNews&type=Publishing&mod=Publications%3A%3AArticle&mid=8F3A7027421841978F18BE895F87F791&tier=4&id=96F1EDDC8CB24008870DBF8E7A0A5775 (retrieved 14.12.11).

[29] T.L. Hanuscak, S.L. Szeinbach, E. Seoane-Vazquez, B.J. Reichert, C.F. McCluskey, Evaluation of casues and frequency of medication errors during information technology downtime, Am. J. Health. Syst. Pharm. (2009) 1119–1124.

[30] D.F. Sittig, J.S. Ash, H. Singh, The SAFER guides: empowering organizations to improve the safety and effectiveness of electronic health records, Am J Managed Care 20 (5) (2014) 418–423.

[31] H. Singh, J.S. Ash, D.F. Sittig, Safety assurance factors for electronic health record resilience (SAFER): study protocol, BMC Med. Inform. Decis. Mak. 13 (April (1)) (2013) 46.

[32] J. Boucher, Ochsner health system transforms its backup and recovery with EMC, EMC Press Release (September 25, 2012), Available at: http://www.emc.com/about/news/press/2012/-04.htm 20120925