Integrating and Connecting Care
A. Ryan et al. (Eds.)

doi:10.3233/978-1-61499-783-2-14

Downtime in Digital Hospitals: An Analysis of Patterns and Causes Over 33 Months

Jessica CHEN[a], Ying WANG[b] and Farah MAGRABI[b,1]
[a] *Graduate School of Biomedical Engineering, University of New South Wales, Sydney, Australia*
[b] *Centre for Health Informatics, Australian Institute of Health Innovation, Faculty of Medicine and Health Sciences, Macquarie University, Australia*

Abstract. The use of health information technology (IT) is increasing around the world. However, as complex IT systems are implemented, new types of errors are introduced. These can disrupt workflow and care delivery, and even lead to patient harm. The purpose of this paper is to examine the patterns and causes of IT system downtime in a hospital setting. We examined all the downtime events that were recorded by a hospital IT department from February 2010 to October 2012. On average downtime disrupted care delivery for 49 hours per year with 51% of total downtime between 9 am and 5 pm. These results show that there is a need for safer design and implementation of IT systems. Further studies are required to measure the effects of downtime on care delivery and patient outcomes in digital hospitals.

Keywords. Health information technology, patient safety, downtime, outage

Introduction

The use of information technology (IT) or digital health can improve healthcare quality and patient safety [1] [2]. However, rapid adoption of complex IT systems can lead to incidents of patient harm as new types of errors are introduced [3] [4]. A retrospective analysis of safety events in England from 2005-2011, found that IT does create potentially hazardous circumstances that can lead to patient harm or death [5]. *Downtime* amongst these safety events was significantly more likely to disrupt care delivery and took longer to resolve than events created by the failure to use IT appropriately or by the misuse of IT. A *downtime is a period of time when IT systems are not available or only partially available* [6]. Downtime in hospitals can cause major disruptions in workflow delaying or interrupting patient care, and increases the likelihood of patient harm [6] [7].

There is no active surveillance of the frequency and scope of downtime currently experienced by hospitals in Australia or elsewhere in the world. In a 2014 survey of US healthcare organisations, 70% (n=59) of respondents reported at least one unplanned downtime lasting 8 or more hours in the previous 3 years [8]. However, few studies have sought to characterise actual patterns of downtime in healthcare. The only study

[1] Corresponding Author.

measuring downtime, done in 2003, was restricted to a hospital emergency department, and detected 77 events ranging from a few minutes to 16 hours over a 4-month period [9]. Thus, we set out to examine the patterns and causes of downtime in a hospital setting.

1. Method

The study was conducted in a 350-bed metropolitan teaching hospital in Australia. The hospital has a mature electronic medical record (EMR) which is integrated with laboratory and pharmacy systems. We analysed the log of 129 downtime events that were recorded by the hospital IT department from February 2010 to October 2012 (see Table 1). One event with a faulty date was removed leaving 128 events. Descriptive analyses were undertaken for all events to examine patterns including the distribution of downtime by the time of the day, day of the week, detection and areas affected.

Table 1. Example of event in downtime log captured by the hospital IT department.

Element of report	Example
ID; Start; End	97; 3:30 am; 7:30 am
Details; Details 2	svpwgssvc0302; All departments
Description	Switch died at around 3:30am according to alert
Resolution	Went on site at around 7:30am and replaced switch
Comments	Switch blew 3:30 and needed replacing, done at 7:30 am
Relevant; Date	Yes; 26/10/2011
Restored; Status	26/10/2011; complete
System ID	01CG216299; pwgssvc0302

The causes of downtime were examined by analysing the descriptions of events. Using all 18 events from 2011 we identified keywords and tabulated definitions for major categories of equipment and problems e.g. switch, router and bug. Patterns of these keywords were determined by the frequency of their occurrences. This step was repeated for the remaining events to identify and record new keywords. Based on the frequency of these keywords and the current literature on IT safety [11], keywords were grouped into four main categories of downtime events: network down, power outage, software and other [12] [13]. To test and measure the reliability of this classification, an inter-rater reliability analysis using the kappa statistic was performed [14] [15]. A second investigator was trained using a random set of 8 events and the reliability was tested using a separate set of 26 events that were also randomly selected. The inter-rater reliability was κ =0.69, 95% CI 0.43 to 0.95. Analyses were undertaken in Microsoft Excel and Access with SQL queries.

2. Results

Downtime Patterns: Of the 128 events analysed, all but one were unplanned (n=127). The start and end times were available for 41 events. The total downtime associated with these 41 events was 147 hours and 22 minutes over the 33-month period (Table 2). Analysis of temporal patterns showed that 51% of total downtime was between 9 am and 5 pm; 90% in 2010, 24% in 2011, and 11% in 2012 (Figure 1). We found that downtime was unevenly distributed over the week with 68% of downtime occurring on weekdays. In 2010, 85% of downtime occurred on weekdays, 94% in 2011, and 31% in 2012. In 2012, 69% of downtime was on a Saturday.

Causes of Downtime: Based on the frequencies of keywords in 128 events, causes of downtime were grouped together to form four main categories (Table 3).

Table 2. Descriptive statistics summary for 41 (32%) events with start and end times.

Year	Annual Downtime (hh:mm)	Mean (hh:mm)	Confidence Interval (95%) (±hh:mm)	Median (hh:mm)	Range (hh:mm)	Number of events
2010	71:39	03:34	03:23	01:22	21:25	20
2011	16:31	03:28	01:16	01:44	15:05	11
2012	59:12	05:55	04:24	02:19	26:40	10
Total	**147: 22**					**41**

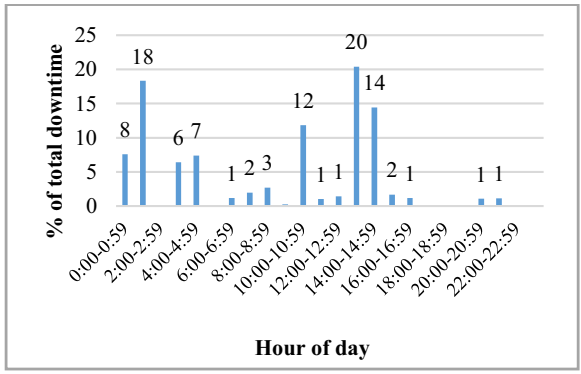

Figure 1. Downtime events by hour of day over the 3-year period (n=41).

Table 3. Frequency of keywords.

Network Down	Frequency	Power Outage	Frequency	Software	Frequency	Other	Frequency
network	34	power	32	software	4	air	4
concentrator	2	link	22	script	7	cbord	2
router	28	supply	7	firewall	23	card	8
server	93			<EMR>*	35		
service	35			<prescribing software>*	14		
servicing	2			bug	9		
switch	62			virus	4		
transmitter	3			security	7		
reconfigured	4			application	20		
Total	263		61		103		14

*clinical software package de-identified

Network Down: Computer network related issues were the most common cause accounting for 77% of all events (n=98); 69% in 2010 (n=55), 89% in 2011 (n=16) and 90% in 2012 (n=27); all of these were unplanned. Further analysis of these events revealed that 61 (55%) were server-related (74% in 2010 (n=41), 56% in 2011 (n=9) and 37% in 2012 (n=10).

Power Outages: All power outages were unplanned and accounted for 8% all events, 6% in 2010 (n=5), 11% in 2011 (n=2), 10% in 2012 (n=3). Causes of power outages ranged from human error (e.g. a patient accidentally turning off a circuit breaker) to external networks and links (e.g. <power company> outage). A backup supply failure was also logged and was considered as a power outage.

Software Related Downtime: Software issues accounted for 13% of events overall. In 2010, 21% were software-related (n=17). One of these events was due to a planned software upgrade in 2010. However, there were no software or application failures in 2011 and 2012. Other software related events were also due to security reasons where there were firewall failures, computer viruses and bugs in software programs.

Other Events: There were some events that could not be categorised in either network down, power outage or software. These events relating to air-conditioning or card system functionality made up 2% of those analysed, 4% in 2010 (n=3) and none in 2011 and 2012.

Areas Affected: We found that 74% of events (n=71) were reported to affect multiple areas of the hospital i.e. more than one ward, floor or building; 78% affected multiple areas in 2010 (n=47), 38% in 2011 (n=5) and 83% in 2012 (n=19).

Detection: Over the three years, detection of downtime was mostly by users of clinical IT systems (88%), 11% were detected by IT and 1% were detected by personnel outside the hospital (e.g. network provider). Users detected 93% (n=62), 60% (n=9) and 94% (n=17) in 2010, 2011 and 2012 respectively.

3. Discussion

IT plays a mission critical role in hospitals. Our dependence on clinical IT at the point of care has never been greater, and with that dependence come the serious consequences of downtime. Yet few studies have looked at the patterns and causes of downtime in hospitals. We found that the availability of IT was affected by 128 events. As a consequence IT systems under performed or were not accessible to clinicians for a total of 5.1 days over the 33-month period. On average, the hospital experienced 49 hours of disruption per year which is almost double the 25 hours of annual downtime typically experienced by organisations in other industries [16].

We found four distinct causes of downtime in hospitals. Although this data does not directly tell us about the impact of these events on clinical workflow and patient safety, inferences can be made from our previous work on a subset of these events. That study sought to measure the effects of downtime on pathology testing by examining events ranging from a few minutes to 5 hours over 11-months at the same hospital (February 2011 and January 2012) [6]. We found that 5 to 6-fold delays in reading test results occurred immediately after a downtime of 17 min during which clinicians could not logon to the results reporting system ($p<0.003$). These effects varied depending on the type of event, but the investigation was not able to uniformly measure this. In this study, the inability to access servers means that clinical users were not be able to access clinical information at the point of providing care to patients. As most downtime affected access to data, decision-making and treatment could have been delayed. Hence, we suggest that further investigation is required to measure the effects of downtime on care delivery and patient outcomes including by type of event e.g. power outage.

Network issues were most common, accounting for 69-90% of events. Most of these were server related involving printer networks, virtualisation services and access to database networks.

The impact of power outages on care delivery were not apparent from these data. However, what we do know is that power outages affect computer networks as they need to be rebooted, replaced or reconfigured. Reported reasons for power outages included power supply failures, standby power supply failures, external outages (e.g. <supplier> power outage) and human error (e.g. patient accidentally switching off the power). While contingency plans are critical to minimising the effects of such disruptions, we found that the standby power had failed on one occasion and was of a "serious nature". Hence it is essential to regularly test contingency plans [8].

The partial and total loss of functionality of software was also common in 2010 but by 2012, no software-related events were logged. This suggests that as these software applications were used, there have been improvements made in the software. Nevertheless, it is interesting to note that there was a planned downtime for a software upgrade to the EMR in February 2010. This software was found to have subsequent issues throughout 2010 but none were recorded in 2011 and 2012, suggesting that software issues were resolved causing no further disruptions.

Events that are not classified in either network down, power outages or software were only found in 2010. Examples of other downtime events include air-conditioning failure and a card system. This suggests that these issues may either be no longer logged by IT staff or resolved elsewhere. For the purposes of this study, events were assigned to a single category. As a consequence some events which involved both network and software issues led to disagreements amongst the two investigators who

coded the incidents. This showed the need to use two or more categories to accommodate such events with multiple causes.

Multiple areas of the hospital were affected in 2010 and 2012 by network issues (mostly servers) and power outages. This is perhaps due to the location and configuration of the computer network indicating a need to redesign the network, considering the workflow of each clinic, ward or building.

As expected, the majority (60-94%) of events were detected by users who noticed performance issues while using IT. Indeed it is possible that these events were not detected in a timely manner because clinicians are often unaware that part of a complex IT system is not functioning properly. For example, the laboratory system may be down, thus even though it appears their request for laboratory tests was sent, it is actually held in a queue awaiting processing by the receiving system whenever it becomes available. It is thus possible that care delivery was significantly disrupted before downtime was detected. Other events were detected by IT staff using a monitoring system. Such monitoring systems which are tightly coupled to the underlying hardware and software used by IT systems, have limited ability to detect complex problems that emerge from interactions among IT system components. Therefore, there is a need for more robust ways to detect and respond to downtime in a timely manner before it disrupts care delivery and harms patients.

There are a few limitations in terms of the data we used. The events only included one planned downtime and represented those events that were detected and eventually resolved. This leaves out many other possible events that went undetected e.g. when systems underperformed. Also, not all data was specified. Important fields such as the start and end times were not available for 68% (n=86) of events. Therefore, total downtime is likely to be underestimated. Another limitation related to duration is that downtime was calculated from the point at which the event was detected. However, this may not accurately represent when the event occurred, thus potentially underestimating the total duration of downtime.

4. Conclusion

While IT has the potential to improve health care delivery, downtime can disrupt workflow and patient harm. We found that on average the hospital experienced 49 hours of disruption per year and most downtime was caused by computer network issues. Hence, there is a need for safer design and implementation of IT systems, particularly for network configurations and its usage. Further studies are required to measure the effects of downtime on care delivery and patient outcomes in digital hospitals.

References

[1] AK. Jha, D. Doolan, D. Grandt, T. Scott, DW. Bates, “The use of health information technology in seven nations,” Int. J. Med. Inform, vol. 77, no. 12, pp. 848-854, 2008.

[2] B. Chaudhry, J. Wang, S. Wu, et al, “Systematic review: impact of health information technology on quality,” Ann. Intern. Med., vol. 144, no. 10, pp. 742-752, 2006.

[3] E. Coiera, J. Aarts, C. Kulikowski, “The dangerous decade,” J Am Med Inform, vol. 19, no. 1, pp. 2-5, 2012.

[4] MO. Kim, E. Coiera, F. Magrabi, “Problems with health information technology and,” J Am Med Inform Assoc, vol. 24, no. 2, pp. 246-250, 2017.
[5] F. Magrabi, M. Baker, I. Sinha, et al., “Clinical safety of England’s national programme for IT: a retrospective analysis of all reported safety events 2005–2011,” Int. J. Med. Informatics, vol. 84, no. 3, p. 198–206, 2015.
[6] N. Nelson, “Downtime procedures for a clinical information system: a critical issue,” J Critical Care, vol. 22, no. 1, pp. 45-50, 2007.
[7] Y. Wang, E. Coiera, B. Gallego, OP. Concha, MS. Ong, G. Tsafnat, D. Roffe, G. Jones, F. Magrabi, “Measuring the effects of computer downtime on hospital pathology processes,” J. Biom. Inform, vol. 59, pp. 308-315, 2016.
[8] DF. Sittig, D. Gonzalez, H. Singh, “Contingency planning for electronic health record-based care continuity: A survey of recommended practices,” Int. J. Med. Informatics, vol. 83, no. 11, pp. 797,2014.
[9] N. Hoot, JC. Wright, D. Aronsky. “Factors Contributing to Computer System Downtime in the Emergency Department,” AMIA Annu Symp Proc. 2003; 2003: 866.
[10] MS. Ong, F. Magrabi, E. Coiera, “Syndromic surveillance for health information system failures: a feasibility study,” J Am Med Inform Assoc, vol. 20, no. 3, pp. 506-512, 2013.
[11] F. Magrabi, MS. Ong, W. Runciman, E. Coiera, “Using FDA reports to inform a classification for health information technology safety problems,” J Am Med Inform Assoc, vol. 19, no. 1, pp. 45, 2012.
[12] A. C. PRQC, “ATIS Telecom Glossary,” ATIS, [Online]. Available: http://www.atis.org/glossary/. [Accessed 30 January 2017].
[13] M. Rouse, “SearchNetworking,” TechTarget, [Online]. Available: http://searchnetworking.techtarget.com/definition/concentrator. [Accessed 30 January 2017].
[14] D. Altman, “Practical statistics for medical research,” London, Chapman & Hall/CRC, 1999, p. 611.
[15] B. Ciubotaru, GM. Muntean, Advanced network programming - principles and techniques: network application programming with Java, New York: Springer, 2013.
[16] Kovacs E. Downtime & data loss cost enterprises $1.7 trillion/year. Security Week 2014.