INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS 83 (2014) 122–130

journal homepage: www.ijmijournal.com

Characteristics of health IT outage and suggested risk management strategies: An analysis of historical incident reports in China

Jianbo Lei[a,b,*], *Pengcheng Guan*[a], *Kaihua Gao*[a], *Xueqin Lu*[a], *Yunan Chen*[c], *Yuefeng Li*[d], *Qun Meng*[d], *Jiajie Zhang*[b], *Dean F. Sittig*[b], *Kai Zheng*[e,f]

[a] *Center for Medical Informatics, Peking University, Beijing, China*
[b] *School of Biomedical Informatics, University of Texas Health Sciences Center at Houston, Houston, TX, USA*
[c] *Donald Bren School of Information and Computer Sciences, University of California, Irvine, CA, USA*
[d] *Center for Statistics and Informatics, Ministry of Health, China*
[e] *School of Public Health Department of Health Management and Policy, University of Michigan, Ann Arbor, MI, USA*
[f] *School of Information, University of Michigan, Ann Arbor, MI, USA*

ARTICLE INFO

Article history:
Received 28 January 2013
Received in revised form
12 October 2013
Accepted 14 October 2013

Keywords:
Health information system
Electronic health records
Patient safety
Accident prevention
Failure prediction
Failure recovery, maintenance and self-repair
Safety critical systems

ABSTRACT

Background: The healthcare industry has become increasingly dependent on using information technology (IT) to manage its daily operations. Unexpected downtime of health IT systems could therefore wreak havoc and result in catastrophic consequences. Little is known, however, regarding the nature of failures of health IT.

Objective: To analyze historical health IT outage incidents as a means to better understand health IT vulnerabilities and inform more effective prevention and emergency response strategies.

Methods: We studied news articles and incident reports publicly available on the internet describing health IT outage events that occurred in China. The data were qualitatively analyzed using a deductive grounded theory approach based on a synthesized IT risk model developed in the domain of information systems.

Results: A total of 116 distinct health IT incidents were identified. A majority of them (69.8%) occurred in the morning; over 50% caused disruptions to the patient registration and payment collection functions of the affected healthcare facilities. The outpatient practices in tertiary hospitals seem to be particularly vulnerable to IT failures. Software defects and overcapacity issues, followed by malfunctioning hardware, were among the principal causes.

Conclusions: Unexpected health IT downtime occurs more and more often with the widespread adoption of electronic systems in healthcare. Risk identification and risk assessments are essential steps to developing preventive measures. Equally important is institutionalization of contingency plans as our data show that not all failures of health IT can be predicted and thus effectively prevented. The results of this study also suggest significant future work is needed to systematize the reporting of health IT outage incidents in order to promote transparency and accountability.

* *Corresponding author at*: Center for Medical Informatics, Peking University, 38 Xueyuan Rd, Haidian District, Beijing 100191, China. Tel.: +86 10 8280 5901; fax: +86 10 8280 5900.
E-mail address: jblei@hsc.pku.edu.cn (J. Lei).
1386-5056/$ – see front matter © 2013 Elsevier Ireland Ltd. All rights reserved.
http://dx.doi.org/10.1016/j.ijmedinf.2013.10.006

1. Introduction

The widespread adoption of health information technology (IT) has been taking place in most industrialized countries as well as some developing countries such as China [1–3]. As a result, healthcare provider institutions around the world have become increasingly dependent on using IT to manage their patient care delivery and hospital/clinic operation processes. These include time-sensitive and mission-critical processes in settings such as emergency rooms and surgical and intensive-care units.

Health IT that provides computerized decision-support functionalities has also become an indispensable tool aiding clinicians in their medical practice. For example, clinicians are more and more reliant on using order-sets stored in computerized prescriber order entry (CPOE) systems for complex medication prescriptions or procedure orders [4,5]. They may not necessarily know, or remember, what constitutes an order-set. Such overdependence on technology could over time 'deskill' healthcare workers, and create chaos when health IT systems become unexpectedly unavailable [4–6].

Although the reliability of computing hardware has significantly improved over the past several decades, the complexity of software has escalated. This is especially true in healthcare [7,8]. At the same time, many provider institutions must adopt tens, if not hundreds, of different IT applications supplied by different vendors. These systems are often interdependent on one another in order to provide a full spectrum of services. In such highly complex environments, system failures are inevitable. It is therefore believed that the occurrence of health IT outage at any given healthcare institution is no longer a matter of whether, but when [7,8]. Many factors may be responsible for health IT failures such as capacity overrun, hardware malfunction, software defects, human errors, computer virus/hacker attack, and natural disasters [9].

Analyzing historical outage incidents can be a valuable means to better understand health IT vulnerabilities and subsequently inform more effective prevention and emergency response strategies. It has been shown that most existing IT risk analysis techniques are grounded in the classical probability theory, which postulates that the past is an indication of the future [10,11]. No prior systematic research has been conducted to examine the health IT outage events reported in public mainstream news outlets, however. We performed a careful PubMed search using many keywords and combinations of keywords in an attempt to identify relevant studies. We also searched in Wanfang (wanfangdata.com.cn), China National Knowledge Infrastructure (cnki.net), and VIP Journal Integration Platform (cqvip.com), the three most popularly used scientific literature databases indexing research papers published in Chinese journals. The searches either yielded no results, or the articles retrieved were related but not closely relevant [e.g., 12,13]. The list of keywords we used is provided in Appendix 1.

In this study, we conducted a qualitative analysis to summarize, thematize, and make inferences of health IT outage events that occurred in China. The analysis was based on news articles and incident reports publicly available on the internet. Even though less developed compared to many western countries, nearly 50% of hospitals and ambulatory care practices in China have by now adopted the basic forms of electronic health records (EHR) systems, practice management systems (often referred to as Hospital Information System in China, or HIS), picture archiving and communication system (PACS), and CPOE [3,14]. While not all results from this China study are generalizable to other countries, we believe certain insights may have broad implications because the fundamental architecture of health IT, thus its vulnerabilities, is more or less the same. These include vulnerable hardware components, capacity constraints, complex messaging and interoperability mechanisms, human errors, threats from the internet, and natural disasters.

2. Methods

2.1. Data collection

To obtain news articles and publicly available incident reports describing health IT outage events in China, we performed a comprehensive internet search using two popularly used web search engines: Baidu (baidu.com) and Google (google.com). Baidu is the dominant search engine in the Chinese web controlling approximately 78.3% of the market share [15]. Worldwide, it is among the top five most frequently visited websites according to Alexa Internet [16].

To facilitate the search, we compiled a list of keywords and combinations of the keywords and their varied forms of spellings, which we believe is reasonably inclusive. The list is provided in Appendix 2. Two graduate students specialized in health informatics (KG and XL) conducted the search and independently evaluated the records returned by the two search engines. Another graduate student research assistant, also trained in health informatics (PG), audited a random set of the results. Discrepancies and disagreements were resolved through group discussions among the investigator team.

2.2. Data analysis

To analyze the content of the articles and reports retrieved, we applied a deductive grounded theory approach [17] leveraging a synthesized IT risk conceptual framework proposed by Sherer and Alter [18]. Based on a systematic review of 46 research papers published in the area of information systems, Sherer and Alter found that most prior conceptualizations of IT risk focus on negative outcomes and their constructs generally fall into the following three categories: risk components, risk factors, and probability of negative outcomes [18].

We first coded the data based on this conceptual framework, referred to as the Synthesized IT Risk Model in the remaining parts of this paper. Then, we examined the recurring themes that emerged from the data to understand common causes of health IT outage and common risk management strategies used to prevent or minimize the adverse impact of the failures. We also recorded and analyzed metadata associated with the reported health IT outage events whenever available, such as date and time when an event occurred, general characteristics of the healthcare setting (e.g., location and hospital type), and scope of the impact.