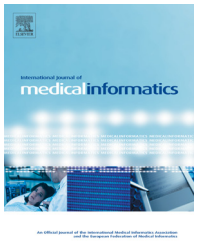
INTERNATIONAL JOURNAL OF MEDICAL INFORMATICS 84 (2015) 454–467

journal homepage: www.ijmijournal.com



Analysis of health professional security behaviors in a real clinical setting: An empirical study

José Luis Fernández-Alemán[a,*], *Ana Sánchez-Henarejos*[a], *Ambrosio Toval*[a], *Ana Belén Sánchez-García*[b], *Isabel Hernández-Hernández*[b], *Luis Fernandez-Luque*[c]

[a] *Faculty of Computer Science, Department of Informatics and System, University of Murcia, Spain*
[b] *Reina Sofia University Hospital, Murcia, Spain*
[c] *Northern Research Institute, Tromsø, Norway*

ARTICLE INFO

Article history:
Received in revised form
13 January 2015
Accepted 14 January 2015

Keywords:
Privacy
Security
Health personnel
Surveys
Personal health information

ABSTRACT

Objective: The objective of this paper is to evaluate the security behavior of healthcare professionals in a real clinical setting.
Method: Standards, guidelines and recommendations on security and privacy best practices for staff personnel were identified using a systematic literature review. After a revision process, a questionnaire consisting of 27 questions was created and responded to by 180 health professionals from a public hospital.
Results: Weak passwords were reported by 62.2% of the respondents, 31.7% were unaware of the organization's procedures for discarding confidential information, and 19.4% did not carry out these procedures. Half of the respondents (51.7%) did not take measures to ensure that the personal health information on the computer monitor could not be seen by unauthorized individuals, and 57.8% were unaware of the procedure established to report a security violation. The correlation between the number of years in the position and good security practices was not significant (Pearson's $r = 0.085$, $P = 0.254$). Age was weakly correlated with good security practices (Pearson's $r = -0.169$, $P = 0.028$). A Mann–Whitney test showed no significant difference between the respondents' security behavior as regards gender ($U = 2536$, $P = 0.792$, $n = 178$). The results of the study suggest that more efforts are required to improve security education for health personnel.
Conclusions: It was found that both preventive and corrective actions are needed to prevent health staff from causing security incidents. Healthcare organizations should: identify the types of information that require protection, clearly communicate the penalties that will be imposed, promote security training courses, and define what the organization considers improper behavior to be and communicate this to all personnel.

* *Corresponding author at*: Faculty of Computer Science, Campus of Espinardo, Murcia, Spain. Tel.: +34 868 884621; fax: +34 868 884151.
E-mail addresses: aleman@um.es (J.L. Fernández-Alemán), anasanchez@um.es (A. Sánchez-Henarejos), atoval@um.es (A. Toval), absg2@um.es (A.B. Sánchez-García), isabelhdezhdez@yahoo.es (I. Hernández-Hernández), luis.luque@norut.no (L. Fernandez-Luque).

http://dx.doi.org/10.1016/j.ijmedinf.2015.01.010
1386-5056/

1. Introduction

Health organization security threats can be categorized into five levels, in increasing order of sophistication [1,2]: accidental disclosure, insider curiosity, data breach by insider, data breach by outsider with physical intrusion, and unauthorized intrusion on the network system. According to the 2012 European Network and Information Security Agency report [3], the number of data breaches detected in healthcare organizations has increased over the last few years. More than 9 out of 10 breaches would have been prevented if organizations had followed information security best practices. Forty one percent of the health record breaches in Europe are the result of the negligence of employees, who shamelessly flaunt their invisibility and treat sensitive data as invaluable commodities [4]. A similar situation appears in the USA healthcare industry. According to the results of the Ponemon Institute's Third Annual Benchmark Study on Patient Privacy & Data Security published in December 2012 [5], employee mistakes or unintentional actions continues to be at the root of 42% of breaches. The majority of human error-related privacy breach incidents are mistakes during the information processing stage [6]. Major threats to patient privacy stem from insiders since they are legally privileged as regards accessing patient information [2]. A total of 192 data breaches owing to insiders' intentional or unintentional actions, including those of doctors and administrative personnel in medical centers, were made public in the Privacy Rights Clearinghouse from 2005 to 2013 [7]. These breaches compromised the confidential health information of more than half a million patients.

Note that the average annual cost of data breaches to the USA healthcare industry is as high as $7 billion [5]. Employee mistakes and negligence therefore continue to be a huge issue, despite all the physical, administrative and technical safeguards, in addition to awareness efforts and training courses for health workers [8,9]. Healthcare-specific guidance on the selection and implementation of security controls for the protection of health information has been proposed [10], as has how these security controls are to be met [11]. However, little attention has been paid to the need to train staff in health information security [11,12].

Organizations routinely focus on primarily technical safeguards, while human error is overlooked as a major cause of privacy breaches [6]. Healthcare organizations do not generally employ security trained staff [13], which can create vulnerabilities as regards authorized access, data integrity and confidentiality. An insider has legitimate and often privileged access to facilities and information. Insider threats do not tend to be considered when planning the security strategy [13]. Not only malicious threats to information assets but also the accidental loss or release of information can have a negative impact on the security and privacy of Electronic Health Records (EHRs) [14]. In fact, most of the insider problems stem from ignorance rather than malicious motivation, but these accidental failures are equally dangerous and can have great impacts [14]. The lack of IT/HIT literacy may therefore represent an important threat [15].

Whilst healthcare organizations must focus on meeting legal requirements, staff security training shifts to the background [11], and the component of security is based on the individuals' ethical behavior which is underpinned by trust [13]. This situation leads to an increase in insider threats which, when combined with medical systems that are open to the Internet and the evolving nature of vulnerabilities [16], may lead to dangerous violations of personal health information privacy [17].

Education and awareness are the best non-technical measures with which to mitigate security and privacy threats in general, and insiders threats in particular [14]. According to the Health Insurance Portability and Accountability Act (HIPAA) [18], hospital workforces should be formally educated and trained at least once a year and when policies or procedures change. Empirical studies suggest that education can influence an organization's security performance [19]. Good training [20,21], awareness programs and the planning of a proper policy to fulfill security requirements are substantial to protect a healthcare organization from harm to patient privacy [11,21–24]. It is particularly important that health staff be trained in how to respond to security incidents. Clinicians usually find workplace privacy and security poorly implemented. Scheduling problems, difficulty in attending, irrelevant privacy and security training sessions are just some of the problems identified [21]. Research into checklists and other user aids require more attention if procedures ensuring that operators and supervisors are adequately trained to handle procedural errors during the information processing stage are to be identified [6].

This paper presents an empirical study of the security and privacy practices for healthcare professionals in a public hospital. Standards, guidelines and recommendations concerning security and privacy best practices for staff personnel have been identified. The contents selected from these documents have been refined and expressed in the form of a checklist for audit purposes. A questionnaire consisting of 27 questions was created and responded to by 180 workers from a public hospital. To the best of our knowledge no previous statistical studies have, to date, analyzed the security behavior of healthcare professionals in such a complete way in a real clinical setting. The results of this empirical study have been used to identify inadequate security practices in healthcare organizations, and to address future directions as regards improving the security education of health personnel.

The remainder of this paper is organized as follows. Section 2 provides an overview of related work and addresses the motivations behind this research. Section 3 describes the steps followed to identify the standards, guidelines and recommendations related to security and privacy best practices for staff personnel used in the preparation of the questionnaire. This section also presents the hypotheses guiding our research. Section 4 shows the results of the survey responded to by 180 participants, and statistically analyzes the data collected. Section 5 examines the causes and consequences of not following security and privacy best practices and compares the results obtained in our survey with those of other studies. Finally, Section 6 outlines some concluding remarks and discusses future work.