Available online at www.sciencedirect.com

ScienceDirect

journal homepage: http://ees.elsevier.com/hsag/default.asp

Full Length Articles

Reasons for Picture Archiving and Communication System (PACS) data security breaches: Intentional versus non-intentional breaches

Tintswalo Brenda Mahlaola[*], *Barbara van Dyk*

Department of Medical Imaging and Radiation Sciences, Faculty of Health Sciences, University of Johannesburg, P.O. Box 17011, Doornfontein, 2000, South Africa

ARTICLE INFO

Article history:
Received 14 July 2015
Accepted 11 April 2016

Keywords:
Intentional breaches
Patient confidentiality violation
PACS
Unintentional breaches

ABSTRACT

Background: The Picture Archiving and Communication System (PACS) has led to an increase in breached health records and violation of patient confidentiality. The South African constitution makes provision for human dignity and privacy, virtues which confidentiality seeks to preserve. Confidentiality thus constitutes a human right which is challenged by the use of technology.

Humans, as managers of information technology, constitute the weakest link in safeguarding confidentiality. Nonetheless, it is argued that most security breaches are non-intentionally committed by well-meaning employees during routine activities.

Objective: The purpose of this article is to explore the nature of and reasons for confidentiality breaches by PACS users in a South African context.

Methods: A closed-ended questionnaire was used to collect quantitative data from 115 health professionals employed in a private hospital setting, including its radiology department and a second independent radiology department. The questionnaire sought to explore the attitudes of participants towards confidentiality breeches and reasons for such behaviour.

Results: Breach incidences were expressed as percentage compliance and classified according to the nature and reasons provided by Sarkar's breach classification. Cross tabulations indicated a statistical significance ($p < 0.00$) between the expected and observed confidentiality practices of participants and also the adequacy of training, system knowledge and policy awareness.

Conclusion: Our study supports previous findings that, in the absence of guidelines, most security breaches were non-intentional acts committed due to ignorance. Of concern are incidents in which sensitive information was intentionally shared via social media.

* *Corresponding author*. Tel.: +27 0115596421 (w); fax: +27 0769394254 (c).
E-mail addresses: brendam@uj.ac.za (T.B. Mahlaola), bvandyk@uj.ac.za (B. van Dyk).

Peer review under responsibility of Johannesburg University.
http://dx.doi.org/10.1016/j.hsag.2016.04.003

1. Introduction

1.1. Background and problem statement

Patients suspect that health professionals (HPs) may be abusing their privileges of authorised access to medical records (Akyüz & Erdermir, 2013). Of particular concern are the intentional confidentiality breaches due to acts of indiscretion (Knapp van Bogaert & Ogunbanyo, 2014). One example of indiscretion in the United Kingdom (UK) was reported where HPs shared sensitive data of patients stored in the Picture Archiving and Communication System (PACS) for entertainment purposes ("*Lack of confidentiality*", 2004). According to the literature, the use of information technology (IT) introduces new risks of compromising confidential data to an extent not possible with paper records (Griffith, 2015).

In the past, the breach of confidentiality involved access to paper and film records, which were often stored in a central location making it difficult to compromise the principles of confidentiality. Despite this benefit, the paper system imposed disadvantages that became an impediment to the continuity of patient care because the records could be easily misplaced and thus difficult to retrieve resulting in delayed medical treatment (Beach & Oates, 2014). To address this limitation, advances in IT led to the development of a digital storage modality for radiology data (radiographs and reports) known as PACS.

Although PACS is inherently a radiology archiving system, it can be used in various other sections within a hospital. PACS allows for the remote and instant access to radiology data by a multidisciplinary complement of HPs who are based in different locations within a hospital setting, and thus data of the same patient may be accessed simultaneously by different HPs (Bolan, 2013). PACS has contributed to improved patient care by increasing efficiency and accessibility to data and has led to fewer delays in the clinical management of patients (Bolan, 2013). A possible disadvantage of PACS is that the patients' data is archived on the internet and it is thus possible for unauthorised people to gain access to the data, for instance by internet hackers. It is also possible for data to be duplicated and exported without the patient's knowledge and consent (Benatar, 2010).

The number of breached electronic health records in the United States (US) increased to 137% between 2012 and 2013 (Collier, 2012). These breaches highlight how confidentiality is at an increased level of threat as a result of using IT. There is evidence to indicate that most security breaches are non-intentional threats caused by employees when conducting routine work activities (Barlow, 2015). In South Africa there is no documented data on the types of breaches that have occurred as a result of using PACS technology.

South Africa could prevent the increase in breach incidences as reported in the US if the reasons for breaches and the types of breaches were known. Knowledge of the types of breaches could contribute towards the formulation of guidelines that would ensure that the doctor–patient relationship would not be jeopardised by the use of IT.

1.2. Purpose and objectives

The aim of this study was to test the hypothesis that the nature of most security breaches committed by HPs authorised to use PACS is non-intentional. The objective of this quantitative, correlational study conducted on HPs at two private hospital settings in Johannesburg was to examine the following:

- Participants' pre-existing knowledge of data protection policy, knowledge of PACS data protection features and their attitudes towards breaches of confidentiality.
- The nature and classification of breaches committed when using PACS.

1.3. Definition of key terms

In this study two major categories of breaches, namely intentional and non-intentional, were considered. The non-intentional breaches were further classified into accidental breaches and breaches resulting from ignorance and were defined as follows:

- *Accidental breaches* – these are violations resulting from inadequate system knowledge and stress (Sarkar, 2010, p. 115).
- Breaches arising from *ignorance* – these are violations caused by a lack of training and awareness of policy (Sarkar, 2010, p. 166).
- *Intentional breaches* – these refer to violations emanating from deliberate ignorance of rules and data theft (Sarkar, 2010, p. 166).

2. Theory

People constitute the weakest link in the safeguarding of confidentiality (Princely, 2012). It was found that in the United States human error is the leading cause of data breaches in the banking and IT sectors (Liginlal, Sim, Khansa, & Fearn, 2012). Some breaches may be intentional due to the deliberate intent to ignore policy. Reports on cybersecurity relating to the corporate and law industries indicate that while some disgruntled employees deliberately steal data with a motive for revenge against the institution (Simshaw, 2015), some breach confidentiality to satisfy their curiosity or for personal financial gain (Griffith, 2015). The underlying causes for human error as a precursor to breaches, according to Liginlal et al. (2012), are inadequate knowledge of security policy, a stressful environment with regard to time pressures and limitations in the system design.

Moreover, the law lags behind in keeping pace with the advances in IT (Polito, 2012). The purpose of legislation is to provide guidelines in terms of security policy while education is crucial in providing the required knowledge to enable adherence to policy (Kwon & Johnson, 2013). The gap in teaching may result in limited knowledge specific to the confidentiality of electronic data in terms of medical ethics, human rights and patients' rights. Breaches committed due to