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
Available online xxx

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

limited knowledge are thus presumed to result from ignorance (Sarkar, 2010: 115). The adoption of technology in healthcare requires HPs to learn job-specific skills in terms of the latest technology that could be imparted through training (Shange, 2014). Thus, to protect confidentiality in the technology age requires a seamless integration of education in medical ethics and training on the ethical usage of information technology (Kwon & Johnson, 2013).

The medical world is concerned with saving lives which requires efficiency in decision-making and quick execution of tasks. The efficiency required in a medical emergency introduces time pressures leading to a stressful working environment for HPs and increasing the risk of committing errors (Adams, 2012). Human errors could arise due to the need to circumvent security measures to save the life of the patient (Bernat, 2013). A medical emergency could thus create an ethical dilemma that forces HPs to focus on saving lives and neglect the protection of patient confidentiality.

The medical environment is also centred on team work which creates a culture of trust and support among HPs (Brody & Doukas, 2014). Considering that HPs are bound by oath to protect patient confidentiality (Gautberg & Batalden, 2014), there may be the assumption that all HPs are ethical beings and thus respect patient confidentiality at all times. It is therefore often unclear whether the culture of trust in fact encourages poor supervision of HPs in protecting confidentiality.

The challenge facing the protection of confidentiality is not limited to pinpointing the implications of human error but also to identifying the reasons for the breaches and the nature of these breaches. Patients may be comforted by the knowledge that intentional breaches are in the minority, and that most breaches committed by HPs are non-intentional threats (Liginlal et al., 2012). It was anticipated that this study might provide insight into the nature of breaches involving PACS data. This insight could inform future practice in terms of handling confidential information when using PACS.

3. Materials and methods

3.1. *Materials*

The study was conducted on health professionals with access to health records stored in PACS during the course of their work.

3.2. *Setting*

An invitation to participate in the study was extended to six private hospitals affiliated to different healthcare facility groups and located within the city of Johannesburg. For this study a 75% refusal rate to participate was observed. The sensitivity of the topic was a concern for two hospitals, while a further two hospitals did not respond to the study invitation. One hospital and its radiology department gave permission and was termed "research setting 1". A radiology department in a different hospital consented to participate in the study, although the hospital itself failed to respond to the invitation. The independent radiology department was termed "research setting 2". The study population was thus sampled from research settings 1 and 2.

Setting 2 comprised only the radiology population (N = 19); two of which were radiologists plus 17 radiographers. Setting 1 comprised a complement of the radiology and non-radiology population groups (N = 210). The non-radiology population in setting 1 included 80 medical doctors, including medical specialists, and 100 nursing staff (registered nurses, intensive care nurses, assistant nurses, caregivers and student nurses). The radiology group in setting 1 included 10 radiographers, 4 radiography students and 16 radiologists (5 of whom were locum radiologists).

It was predetermined by the statistician that a sample size of 100 participants was necessary to achieve statistically meaningful results. The study sample was acquired through non-probability quota sampling (Daniel, 2012). A sample size (n = 115) was derived from the two research settings, setting 2 provided a sample size of 17 (n = 17) and setting 1 a sample size of 98 (n = 98). A detailed breakdown of the study sample is provided in Table 1. The study sample was divided into two groups (radiology and non-radiology groups) based on their reasons for accessing PACS data. The radiology group included HPs that accessed PACS as part of their routine activity (radiologists, radiographers, student radiographers) while the non-radiology group included HPs that accessed PACS as part of patient clinical management (nurses, doctors, medical specialists). Assistant nurses, caregivers and student nurses in setting 1 were excluded because they were prohibited by the hospital from accessing PACS. Therefore, only registered nurses and intensive care nurses were included.

3.3. *Design*

A correlational study design was employed to collect quantitative data.

3.4. *Procedure*

A self-designed questionnaire, the Picture Archiving and Communication-Confidentiality Scale (PAC-CS), was used. The questionnaire design was informed by the ISO 17799 model from which the constructs, the choice of questions and their quantification were derived and adapted. The ISO 17799

Table 1 – Breakdown of study sample.

Sample	Frequency	Percent
Study sample		
Doctor	7	6
Radiologist	9	8
Radiographer	41	35
Nurse	53	46
Student radiographers	4	3
Paramedics	2	2
Incomplete questionnaire	−1	
Total	115	100
Sample groups based on reasons for PACS access		
Radiology sample	53	46
Non-radiology sample	62	54
Total	115	100

model is used in IT to benchmark an organisation's level of compliance with international standards of data security and was therefore deemed suitable for the PAC-CS design (Karabacak & Sogukpinar, 2006). The PAC-CS comprised close-ended questions aimed at determining the participants' pre-existing knowledge about the PACS data protection features, knowledge on their organisation's data protection policy and the participants' attitudes towards confidentiality breaches. A pilot study was conducted prior to the data collection. Since hand-delivery is associated with a greater response rate compared to mailed questionnaires (Nimon, Zientek, & Henson, 2012), the PAC-CS questionnaire was hand-delivered and self-administered to the participants over a period of three months.

3.5. *Analysis*

To eliminate bias, responses were captured and analysed by an independent statistician by means of the Statistical Package for the Social Sciences (SPSS) 16. The process of data analysis was organised into three phases. In the first phase, the researcher used guidelines by the US Health Insurance Portability and Accountability Act (HIPAA) of 1996 to establish benchmarks for best practice. A 90% benchmark was set for minimum recommended compliance and 10% for intolerable levels of non-compliance. The researcher believed that the use of international standards was justified because (i) the researcher could not locate any guidelines applicable in South Africa that were *specific to PACS technology*; (ii) the HIPAA legislation has been consulted to inform the security needs of the PACS (Cao, Huang, & Zhou, 2003: 185) and (iii) the PAC-CS was designed using a model for compliance based on international standards.

In the second phase the documented breaches were quantified using weight values derived from the ISO7799 model. The numerical data was then expressed in terms of frequency counts. Statistical significance ($p < 0.05$) was calculated using the one-sample Chi-square test for non-parametric data, the choice of which was informed by the lack of randomisation, sample size and type of the data collected. While the cross-tabulations determined the degree of statistical significance, the phi coefficient helped to determine the extent of the correlation, the strength of which was determined by the Pearson Chi-square test. In the third phase the reasons for breach incidences were determined and classified using Sarkar's analysis of insider threats (2010).

4. Ethical considerations

Prior to the enquiry, ethical clearance was obtained from the ethics committees of the two research settings as well as from the University of Johannesburg, the Faculty of Health Sciences Higher Degrees and Ethics Committees (ethical clearance codes HDC67/02-2011 and AEC70/02-2011).

4.1. *Potential benefits and hazards*

The covering letter attached to the PAC-CS questionnaire set out the study details for the participants. The information contained in the covering letter included an explanation of the nature of the study, the study rationale, objectives, risks, benefits and the right to withdraw without any repercussions. Participation was voluntary and the participants did not derive any personal benefits through participation. The questionnaire did not require the inclusion of personal information and thus the participants' anonymity was ensured. The responses were kept in a locked cabinet under constant camera surveillance and could only be accessed by the researcher. In this way the data in the questionnaires was kept confidential.

4.2. *Recruitment procedure*

Non-probability quota sampling was deemed suitable for achieving the predetermined sample size and permit comparison of the subgroups of the population as per the study's inclusion criteria (Daniel, 2012).

For research setting 1, participants were recruited from those sections of the hospital that had active PACS systems; these included casualty, emergency room, doctors' consulting rooms and intensive care units. At the time of the study, the medical wards in the hospital were not linked to the radiology PACS and were thus excluded. The researcher approached HPs in the radiology and non-radiology domains who fitted the study's inclusion criteria and were willing to participate. Data was collected twice daily to access both day and night shift workers. The researcher had no control over the recruitment for research setting 2 as the practice manager offered to distribute the questionnaire personally.

4.3. *Informed consent*

Informed consent was ensured by allowing participants to ask questions relating to the study. Verbal consent was obtained and implied through the completion of the questionnaire.

4.4. *Data protection*

The completed questionnaires were deposited in a sealed box.

4.5. *Reliability*

The findings of any study would be worthless unless the findings were deemed accurate (valid) and reproducible (reliable). In this study, the integrity of the PAC-CS was examined during a pilot test by peers that represented the sample (Nimon et al., 2012). Although the PAC-CS is not amenable to the Cronbach's test for reliability, its design is consistent with the ISO 17799 model used to collect data on information security. Moreover, the study findings were consistent with the increasing confidentiality breaches documented in the US.

4.6. *Validity*

Content validity of the PAC-CS was achieved by aligning the constructs and questions in the questionnaire with those of the ISO 17799 model. Useful inferences could thus be drawn from the questionnaire responses (Cahit, 2015). The relevance of the PAC-CS to the research domain was assessed during the

pilot test. The reviewers paid attention to the wording of the questions to ensure that the questions were expressed clearly and without ambiguity.

5. Results and findings

Based on the data analysis, the following was found.

Objective 1: To examine participants' knowledge of PACS data protection features, their pre-existing knowledge of data protection policy and their attitudes towards confidentiality breaches.

It is a legal requirement of the HIPAA of 1996 to de-identify medical data. In this study, 58% of the participants were able to download data from PACS but 72% of the participants were unable to de-identify data downloaded from PACS (Table 2).

Clear policy and guidelines tend to improve ethical responses to security issues even in the case of individuals with lower ethical attitudes. The answers of the participants revealed that 62% of participants were poorly informed about their organisation's policy on data security (Table 2).

It is known that patients suspect that HPs may be breaching the confidentiality of their medical records (Akyüz & Erdermir, 2013), it is thus crucial to determine the HPs commitment towards the protection of confidentiality and their attitude towards breaches in order to prevent such breaches. Table 3 indicates that, of the confidentiality breaches (15%) witnessed by fellow HPs, 48% were reported to the authorities.

Objective 2: To examine the nature and classification of breaches committed when using PACS.

It is considered an abuse of the PACS to browse the work list without an intended purpose (Nicholson, 2008). By browsing the PACS without a reason, HPs may access data of patients not assigned to them and thus breach confidentiality (Matlakala & Mokoena, 2011). In this study, 7% of participants admitted to browsing the PACS work list for no valid purpose; and 67% of the participants accessed data of patients not assigned to their care (Table 4).

Provided that confidentiality is maintained, it is permissible to use PACS data for non-medical purposes such as research, auditing and teaching (Nicholson, 2008). In this study the non-medical uses of PACS data included teaching (59%), research (31%), auditing (4%), and assignments (2%) (Table 3). It is unclear whether confidentiality was maintained during the non-medical uses of data considering that 72% of the participants were unable to de-identify data downloaded from PACS.

A further 28% admitted to sharing embarrassing patient data with colleagues, friends and family members. Some of the patients' data was transferred using social medial such as blackberry messenger (BBM)-6% and Facebook (2%) (Table 5). Yet, fewer than 10% of the participants admitted to breaching patient confidentiality when using PACS (Table 3).

The results of the cross-tabulation indicated a statistical significance between the expected and observed confidentiality practices of participants and also between the adequacy of system knowledge and policy awareness. Participants in setting 2 were poorly informed about their organisation's policy on electronic data security (Fig. 1), while radiology PACS users tended to share embarrassing patient data with colleagues, friends and family members (Fig. 2).

Table 2 – Summary of participant's ability to download data from the PACS and awareness of organisational policy on data protection.

Ability to download data from PACS				
Benchmark	Response	EN	ON:N = 112	C
No = 90%	Yes	11 (10%)	65 (58%)	17%*
	No	101 (90%)	47 (42%)	
Ability of PACS to de-identify patients' data				
Benchmark	Response	EN	ON:N = 64	C
Yes = 90%	Yes	58 (90%)	16 (28%)	28%*
	No	6 (10%)	48 (72%)	
Awareness of organisation's data policy pertaining to electronic data				
Benchmark	Response	EN	ON:N = 114	C
Yes = 90%	Yes	103 (90%)	39 (38%)	38%*
	No	11 (10%)	75 (62%)	

Values are given as N expressed in frequency counts.
B, set benchmark (indicated by the percentage next to the desired response)
EN, Expected N.
ON, Observed N.
C, Extent of compliance.
*p = 0.00; **p < 0.05; ***p > 0.05.

Table 3 – Summary of participant's attitude towards confidentiality breach.

Admission of confidentiality breach when using PACS				
Benchmark	Response	EN	ON:N = 114	C
Yes = 10%	Yes	11 (10%)	10 (9%)	90%***
	No	103 (90%)	104 (91%)	
Incidences where colleagues were witnessed using PACS data for reasons other than medical purposes				
Benchmark	Response	EN	ON:N = 115	C
Yes = 10%	Yes	12 (10%)	17 (15%)	70%*
	No	103 (90%)	98 (85%)	
Incidences where intentional confidentiality breach was reported to authorities				
Benchmark	Response	EN	ON:N = 21	C
Yes = 90%	Yes	19 (90%)	10 (48%)	52%*
	No	2 (10%)	11 (52%)	

Values are given as N expressed in frequency counts.
B, set benchmark (indicated by the percentage next to the desired response)
EN, Expected N.
ON, Observed N.
C, Extent of compliance.
*p = 0.00; **p < 0.05; ***p > 0.05.

6. Discussion

It was found that most of the breach incidences (66%) in the study were as a result of ignorance. In this study, two factors

Table 4 – Summary of participant's ability to download data for purposes other than medical purposes.

Download of data from patients not under one's care					NB
Benchmark	Response	EN	ON:N = 113	C	
Yes = 10%	Yes	11 (10%)	76 (67%)	14%*	Accidental
	No	102 (90%)	37 (33%)		
Browsing the PACS work list for no valid purpose					
Benchmark	Response	EN	ON:N = 114	C	
No = 90%	Yes	11 (10%)	8 (7%)	97%***	Ignorance
	No	103 (90%)	106 (93%)		
Use of patients' data and images for non-medical purposes					
Benchmark	Response	EN	ON:N = 114	C	
Yes = 10%	Yes	11 (10%)	52 (46%)	21%***	Ignorance
	No	103 (90%)	62 (54%)		
Sharing embarrassing patient data for entertainment purposes					
Benchmark	Response	EN	ON:N = 112	C	
Yes = 10%	Yes	11 (10%)	32 (28%)	34%*	Intentional
	No	101 (90%)	82 (72%)		

Values are given as N expressed in frequency counts.
B, set benchmark (indicated by the percentage next to the desired Response).
EN, Expected N.
ON, Observed N.
C, Extent of compliance.
*p = 0.00; **p < 0.05; ***p > 0.05.
NB, Nature of breach.

Table 5 – Summary of methods used for data sharing and the various uses of the downloaded data.

Use of data and images for purposes other than patient management			
Benchmark	Response	ON:N = 81	NB
0%	Teaching	48 (59%)	Ignorance
	Research	25 (31%)	Ignorance
	Auditing	3 (4%)	Ignorance
	Assignments	1 (2%)	Ignorance
	Other (Entertainment)	3 (4%)	Intentional
	Other (Social networks)	1 (2%)	Intentional
Methods of data sharing N = 48			
Benchmark	Response	ON:N = 48	NC
0%	Telling	17 (35%)	Ignorance
	Images	25 (52%)	Ignorance
	Reports	1 (2%)	Ignorance
	BBM	3 (6%)	Intentional
	Email	1 (2%)	Ignorance
	Facebook	1 (2%)	Intentional

Values are given as N expressed in frequency counts.
B, set benchmark (indicated by the percentage next to the desired response)
EN, Expected N.
ON, Observed N.
C, Extent of compliance.
NB, Nature of breach.

contributing to confidentiality breaches were identified, namely a lack of knowledge regarding data protection policy and the ease of access to electronic data.

Although access to patient data is crucial for the advancement of the health profession through processes of teaching and research, patients believe that their data is used solely for medical care (Knapp van Bogaert & Ogunbanyo, 2014). To balance this conflict, the National Health Act of 2003 (Act 61) allows for patient data to be used for research provided that consent is obtained prior to the use and that the data be anonymised. The electronic nature of PACS allows for easy access to patient data and a flawless download without

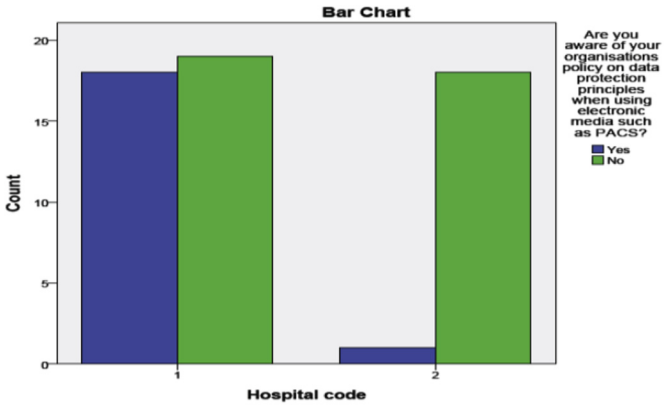

Fig. 1 – Policy awareness setting one versus setting two.1. Research setting 1. 2. Research setting 2.Fig. 1 demonstrates the cross-tabulation outcome between research setting one and two. Based on the above the participants in research setting two were less informed about their organisation's policy on electronic data security. Mahlaola (2013).

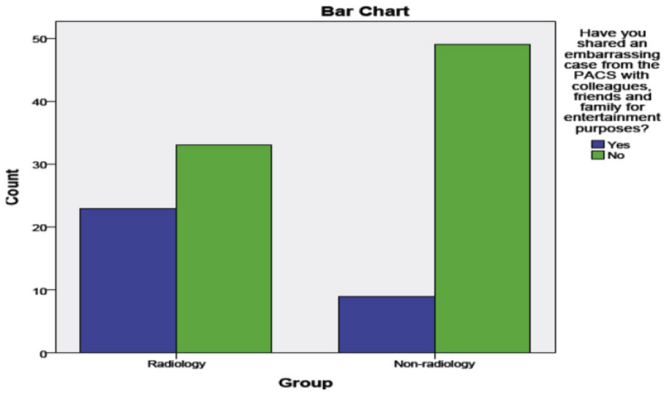

Fig. 2 – Sharing of embarrassing patient data Radiology versus Non-radiology group.The cross-tabulation results between research setting one and two are revealed in Fig.2 above. As demonstrated the radiology PACS users had the propensity to share embarrassing patient data for entertainment purposes as compared to the non-radiology users. Mahlaola (2013).

the patients' knowledge and permission (Benatar, 2010). One could thus argue that the attainment of patient consent by HPs may be considered an unnecessary requirement. In this study, it is unclear whether patients consented to the non-medical use of their data. It is therefore possible that the basic requirement of confidentiality, where the owners of data should be informed of the data-sharing process, was breached (Arora, Yttri, & Nilsen, 2014).

One breach involving participants who accessed data of patients not assigned to their care could not be classified due to a lack of clarity. Data exchange among HPs who share a common patient is permissible (Muhlen & Ohno-Machado, 2012). In the absence of clarity, ignorance was deemed the most logical explanation of data breaches.

Of concern are the incidents in which information was shared via BBM or Facebook and thus assumed to be intentional. One could argue that data shared via BBM is limited to a particular audience compared to Facebook that allows access to a wider audience. The internet does not guarantee against unauthorised viewing and the use of personal information (Moore, 2012). Therefore, BBM and Facebook are equally vulnerable to internet hacking. Patients use the Internet to research their medical conditions and are thus more likely to uncover the breach of their confidentiality by HPs (Griffith, 2012). The discovery of breaches by patients could destroy the mutual trust in the doctor–patient privilege. Thus to evade embarrassment caused by possible confidentiality breaches, patients may avoid seeking medical treatment altogether (Kuo, Ma, & Alexander, 2014).

Sharing of embarrassing patient data with colleagues, friends and family members is not a unique act. Similar behaviour was observed in US clinicians who shared embarrassing medical photographs on social media (Muhlen & Ohno-Machado, 2012). The expansion of Facebook from being a social tool to a platform for addressing professional discourse has been blamed for these breaches of confidentiality (Oxley, 2014; Power, 2015). When intentional breaches are conducted by health professionals, concerns about the

integrity of those authorised to access sensitive information (Wallace, 2015) and the adequacy of the teaching and enforcement of medical ethics comes to the fore.

Clear policy guidelines can improve ethical responses to security issues, even in the case of individuals with lower ethical attitudes. This study revealed that 62% of the participants were ill-informed about their organisation's policy on data security. At the time of the study, the United Kingdom had the Data Protection Act of 1998 in place while the United States (US) had the HIPAA of 1996 in place. South Africa was at the time in the process of enacting the Protection of Personal Information Bill (POPI). "Apart from the Constitution itself, there is no legislation which deals specifically and fully with information protection" (South Africa Law Reform, 2005, p. 9). Contrast to the Promotion of Access to Information Act 2 of 2000 and the Electronic Communications and Transaction Act 25 of 2002; it was anticipated that the POPI Act of 2013 would be the first such legislation to adequately address the issue of data protection with the advent of IT. The researcher could not locate any local regulations relating specifically to the ethical usage of PACS, and both the Health Professions Council of South Africa (HPCSA) and the South African Nursing Council (SANC) did not appear to have regulations in this regard. This lack of policy is not uncommon considering that the law often lags behind in keeping pace with the advances in IT (Polito, 2012).

The study found that the uncovered breach incidences were committed by participants with inadequate system knowledge and policy awareness while working in an environment characterised by a culture of trust and medical emergencies. The hurried nature associated with medical emergencies creates an environment where mistakes are easily made. During medical emergencies HPs may feel justified in circumventing security to save a patient's life. Moreover, it is a challenge to prevent unauthorised access from authorised users. The study context was thus taken into account during the classification of incidents. It was found that of the 15 documented breach incidences, 11 (66%) may have been as a result of ignorance, one (6%) may have been accidental, while four (26%) were deemed intentional (Table 4).

6.1. *Practical implications*

Policy awareness and knowledge is crucial in protecting patient confidentiality but is worthless unless put into practice. It is thus critical that systems be implemented that can monitor compliance with confidentiality principles among PACS users to prevent the breach of confidentiality.

7. Conclusions, limitations & recommendations for future research

7.1. *Conclusion*

Not only do patients often suspect that HPs abuse their privileges of access by breaching the confidentiality of their data, patients are also concerned about breaches arising from acts of indiscretion. The majority of breaches uncovered in this study were classified as non-intentional breaches. This study has provided some insight into the reasons for the breaches committed by PACS users in the two hospital settings.

It is impossible to design monitoring systems and guidelines to address the issues of confidentiality unless the breaches committed by PACS users are identified and classified. The findings of this study may be helpful in informing a framework for the classification of breaches committed by PACS users. Despite the concerns of patients regarding acts of indiscretion, the study findings indicate that 48% of the witnessed breaches were reported to authorities. This may be an indication of the HPs commitment to protect confidentiality.

7.2. *Limitations*

The study sample was not randomised hence, the study findings cannot be generalised to other settings.

7.3. *Recommendations*

Clear organisational policy and improved awareness of guidelines through user education and training could help improve ethical attitudes to security issues. It is suggested that the following interventions might be useful in this regard:

- The implementation of a system to monitor the technical and human aspects of breaches. Such a system needs to be designed through a collaborative input by hospital owners, HPs, IT and PACS vendors.
- Institutions of higher learning should incorporate a module on informatics in their health curriculum.

Acknowledgements

This article is a product of a master's dissertation approved by the University of Johannesburg entitled "*Compliance of health professionals with patient confidentiality when using PACS and RIS*". The permission granted by the research settings, the contribution of the participants and the supervisor's guidance are greatly appreciated. As the primary researcher, Ms Mahlaola was responsible for the project design and data collection which formed part of her master's dissertation. The study was supervised by Mrs van Dyk who made conceptual contributions and edited the manuscript. The article was jointly prepared and approved for submission by both authors.

REFERENCES

Adams, J. (2012). *Ethical problems in emergency medicine: A discussion-based review*. Oxford, UK: Wiley- Blackwell.

Akyüz, E., & Erdermir, F. (2013). Surgical patients' and nurses' opinions and expectations about privacy in care. *Nursing Ethics, 20*, 660–671. http://dx.doi.org/10.1177/0969733012468931.

Arora, S., Yttri, J., & Nilsen, W. (2014). Privacy and security in mobile health (mHealth) research. *Alcohol Research: Current Reviews, 36*(1), 143–150.

Barlow, R. D. (2015). Horizon-scanning around HIPAA, HITECH: how far will they protect healthcare data from insiders, outsiders? *Health Management Technology, 36*(6), 6–8.
Beach, J., & Oates, J. (2014). Maintaining best practice in record-keeping and documentation. *Nursing Standard, 28*(36), 45–50.
Benatar, D. (2010). Indiscretion and other threats to confidentiality. *SAJBL, 3*(2), 59–62.
Bernat, J. L. (2013). Ethical and quality pitfalls in health records. *Neurology, 80*(11), 1057–1061.
Bolan, C. (2013). A view of the future image exchange. *Applied Radiology, 42*(11), 32–37.
Brody, H., & Doukas, D. (2014). Professionalism: a framework to guide medical education. *Medical Education, 48*, 980–987. http://dx.doi.org/10.1111/medu.12520.
Cahit, K. (2015). Internal validity: a must in research designs. *Educational Research & Reviews, 10*(2), 111–118.
Cao, F., Huang, H. K., & Zhou, X. Q. (2003). Medical image security in a HIPAA mandated PACS environment. *Computerized Medical Imaging and Graphics, 27*(2–3), 185–196.
Collier, R. (2012). Medical privacy breaches rising. *Canadian Medical Association Journal, 184*(4), E215–E216.
Daniel, J. (2012). *Sampling essentials: Practical guidelines for making sampling choices*. Washington, DC: SAGE Publications.
Gautberg, E., & Batalden, M. (2014). The professional oath: pledge of allegiance or reflective practice? *Medical Education, 48*(1), 9–11.
Griffith, R. (2012). Duty of confidentiality and the use of social networking sites. *British Journal of Nursing, 21*, 988–989.
Griffith, R. (2015). Patient information: confidentiality and the electronic record. *British Journal of Nursing, 24*(17), 894–895.
Karabacak, B., & Sogukpinar, I. (2006). A quantitative method for ISO 17799 gap analysis. *Computers & Security, 25*, 413–419. http://dx.doi.org/10.1016/j.cose.206.05.001.
Knapp van Bogaert, K., & Ogunbanyo, G. A. (2014). Ethics in healthcare: confidentiality and information technologies. *Journal of South African Family Practice, 56*, S3–S5.
Kuo, K., Ma, C., & Alexander, J. W. (2014). How do patients respond to violation of the information privacy? *Health Information Management Journal, 23*(2), 23–33.
Kwon, J., & Johnson, M. E. (2013). Security practices and regulatory compliance in health care industry. *JAMIA, 20*, 44–51. http://dx.doi.org/10.1136/amiajni-2012-000906.
Lack of confidentiality with picture archiving and communication system (PACS). *Journal of the Royal Society of Medicine, 97*, (2004), 455.
Liginlal, D., Sim, I., Khansa, L., & Fearn, P. (2012). HIPAA privacy rule compliance: an interpretive study using Norman's action theory. *Computer Security, 31*, 206–220.
Matlakala, M. C., & Mokoena, J. D. (2011). Student nurses' views regarding disclosure of patients' confidential information. *Journal of South African Family Practice, 53*(5), 481–487.
Moore, S. C. (2012). Digital footprints on the internet. *International Journal of Childbirth Education, 27*, 86–91.
Muhlen, M., & Ohno-Machado, L. (2012). Reviewing social media use by clinicians. *Journal of American Medical Informatics Association, 19*(5), 777–781.
Nicholson, T. (2008). *Standards for patient confidentiality and PACS*. London: The Royal College of Radiologists.
Nimon, K., Zientek, N. K., & Henson, K. K. (2012). The assumption of a reliable instrument and other pitfalls to avoid when considering the reliability of data. *Frontiers in Psychology, 3*, 1–12. http://dx.doi.org/10.3389/fpsyg.2012.00102.
Oxley, A. (2014). *Security risks in social media technologies: Safe practices in public service applications*. Oxford: Chandos Publishing.
Polito, J. M. (2012). Ethical considerations in internet use of electronic protected health information. *Neurodiagnostic Journal, 52*(1), 34–41.
Power, A. (2015). Is Facebook an appropriate platform for professional discourse? *British Journal of Midwifery, 23*(2), 140–142.
Princely, I. (2012). Understanding information security systems policy compliance: an integration of the theory of planned behaviour and the protection motivation theory. *Computers & Security, 31*, 83–95.
Sarkar, K. R. (2010). Assessing insider threats to information security using technical, behavioural and organisational measures. *Information Security Technical Report, 15*, 112–133. http://dx.doi.org/10.1016/j.istr.2010.11.002.
Shange, N. A. (2014). Training evaluation: process, benefits and issues. *IFE Psychology, 22*(1), 50–58.
Simshaw, D. T. (2015). Legal ethics & data security: our individual and collective obligation to protect online data. *American Journal of Trial Advocacy, 38*(3), 549–574.
South Africa Law Reform Commission. (October 2005). Discussion paper 109. Project 124. Retrieved from www.justice.gov.za/salrc/dpapers/dp109.pdf.
Wallace, I. M. (2015). Is patient confidentiality compromised with the electronic health record? A position paper. *Computers, Informatics, Nursing, 32*(2), 58–62.