Password compliance for PACS work stations: Implications for emergency-driven medical environments

T B Mahlaola, M Tech (Radiography); **B van Dyk**, M Tech (Radiography)

Department of Medical Imaging and Radiation Sciences, Faculty of Health Sciences, University of Johannesburg, South Africa

Background. The effectiveness of password usage in data security remains an area of high scrutiny. Literature findings do not inspire confidence in the use of passwords. Human factors such as the acceptance of and compliance with minimum standards of data security are considered significant determinants of effective data-security practices. However, human and technical factors alone do not provide solutions if they exclude the context in which the technology is applied.

Objectives. To reflect on the outcome of a dissertation which argues that the minimum standards of effective password use prescribed by the information security sector are not suitable to the emergency-driven medical environment, and that their application as required by law raises new and unforeseen ethical dilemmas.

Method. A close-ended questionnaire, the Picture Archiving and Communication System Confidentiality Scale (PAC-CS) was used to collect quantitative data from 115 health professionals employed in both a private radiology and a hospital setting. The PACS-CS sought to explore the extent of compliance with accepted minimum standards of effective password usage.

Results. The percentage compliance with minimum standards was calculated. A significant statistical difference (p<0.05) between the expected and observed data-security practices was recorded.

Conclusion. The study interrogates the suitability of adherence to minimum standards of effective password usage in an emergency-driven medical environment and calls for much-needed debate in this area.

S Afr J Bioethics Law 2017;10(2):62-66. DOI:10.7196/SAJBL.2017.v10i2.600

The effectiveness of password usage in data security has been heavily criticised. A variety of assumptions regarding password usage have been made, depending on the focus of the literature. From a technical perspective, passwords are considered ineffective in restricting access only to individuals with authorised and legitimate access to data.[1] Engineers suspect that human factors play a significant role in determining the effectiveness of technical safeguards, so that human beings are deemed the weakest link in data security.[2] It remains unclear whether the use of passwords is effective in safeguarding electronic data.

Literature findings do not inspire confidence in the usage of passwords for data security. Several quotes taken from various points in time attest to this fact, for example: 'Boot passwords, put your computer under lock and key';[3] 'Goodbye passwords, you aren't a good defense'[4] and more recently, 'Forget passwords – use your face instead.'[5]

There is extensive literature focusing on the effectiveness and suitability of password usage in preventing confidentiality breaches within environments such as computer security. The researchers have no knowledge of similar studies relating to the suitability of password usage within the medical environment. The aim of this article is to bring to the fore factors unique to the medical environment that argue against the direct 'copy and paste' adoption of the minimum standards for effective password usage from computer security into the medical environment.

Background

The use of passwords is ineffective in restricting access only to individuals who are authorised to access data. This popular and easy means of controlling access to data may, in fact, provide the easiest way to breach confidentiality. Information technologists insist that with proper management, passwords are an effective means of protecting the security of data. Measures include, but are not limited to, the use of strong passwords, having individual rather than shared passwords and changing passwords on a regular basis.[6]

Compliance with the minimum standards for effective password usage requires knowledge of and to some extent expertise in data security on the part of the healthcare provider.[7] However, the responsibility to comply cannot be placed solely on the healthcare provider. Standards for effective password usage should be well accepted and applied by all users of the technology. At times, factors unique to the medical field may influence the acceptance of security measures. For instance, in a medical emergency, there may be a legitimate need to circumvent the minimum standards of effective password usage in order to save a life.[2,8] It is for this reason that the contributions of both human and technical factors in normative research are noteworthy, but will never be adequate if the context in which technology is applied remains excluded.

This paper draws on the assumption that the situated use of technology creates challenges to the inscribed ethics of technology use, resulting in the emergence of new ethical dilemmas. Based on this assumption, we argue that the proper management of passwords as described in the environment of computer security is not suitable to the emergency-driven medical environment. In this paper, we reflect on the research outcome of the first author's dissertation in putting this argument forward.[9]

Methods

Picture Archiving and Communication System (PACS; RamSoft, USA) is a digital storage system designed to address the limitations of film and paper records. The conventional storage system imposed disadvantages that became an impediment to the continuity of patient care, because the records could be easily misplaced and therefore difficult to retrieve, resulting in delayed medical treatment.[10] PACS is inherently a radiology archiving system that may be extended to various other sections within a hospital. It allows for remote and instant access to radiology data by a multidisciplinary complement of health professionals (HPs) who are based in different locations within a hospital setting, so that the data of the same patient may be accessed simultaneously by different HPs.[11] PACS has contributed to improved patient care by increasing efficiency and the accessibility of data, and has led to fewer delays in the clinical management of patients.[11] The electronic nature of PACS makes it possible for patients' data to be accessed, duplicated and exported without the patient's knowledge and consent.[12] The use of passwords aids in restricting access to PACS data, to minimise the risk of breaching patient confidentiality.

The original research aimed to determine the extent to which the practices of HPs complied with patient-confidentiality principles when using PACS. The study invitation was initially extended to six hospitals in Johannesburg. However, owing to a 75% refusal rate among this group, the eventual study sample was drawn instead from a private hospital and radiology setting affiliated to different healthcare-facility groups located in Johannesburg instead. The selection criteria included HPs who were willing to participate and were using PACS as either part of routine activity or as a means of delivering patient care. The study sample comprised a multidisciplinary complement of HP such as radiologists, radiographers, student radiographers, doctors, medical specialists and nurses.

Prior to data collection, ethical clearance was obtained from the research settings as well as the research committee of the University of Johannesburg (ref. no. HDC67/02-2011), South Africa (SA). Data were collected from various sections within the hospital, namely radiology, emergency, casualty, theatre, intensive-care units including coronary care, acute care, respiratory, trauma intensive care, neurology and surgical-care units. Data were collected over a period of 3 months using a self-designed questionnaire, the Picture Archiving and Communication Confidentiality Scale (PAC-CS). Consent was obtained verbally, and implied through the completion of the PAC-CS. Informed consent was ensured by allowing participants to ask questions relating to the study, and the data were anonymised. Access to study data was restricted to the researchers.

The PAC-CS design was informed by the content of the ISO/IEC 17799:2005)[13] standard, from which the constructs, the choice of questions and the quantification were derived and adapted. The ISO/IEC 17799:2005 is a model used in information technology to benchmark an organisation's compliance with international standards of data security. The consistency of the PACS-CS design with the ISO 17799 model helped to establish its content validity and reliability. A sample size of 115 participants was achieved through the hand-delivery of PAC-CS using a non-probability quota-sampling technique.[14]

A quantitative, correlational design was deemed suitable for determining the extent of compliance of the situated practices of effective password usage by HPs with minimum standards for effective password usage. The lack of guidelines pertaining to PACS by the Health Professions Council of SA (HPCSA) at the time of this study led to the use of the Health Insurance Portability and Accountability (HIPAA)'s security rule of 1996 as an alternative model for compliance with data-security rules.[15,16] The HIPAA security rule is a detailed outline of the national standards and steps necessary to protect electronic health information from inadvertent disclosures through breaches of security. The choice of this US legislation was informed by its reputation as one of the best regulatory rules pertaining to electronic data security, embedded in the fact that it is continually updated in line with technological advances, and most importantly, addresses the security needs of PACS technology explicitly.[16]

The participant responses were analysed by an independent statistician using the Statistical Package for Social Sciences (SPSS, USA) version 16. The quantified responses were expressed in terms of frequency counts and compliance percentage. A 90% benchmark was set for minimum compliance with technical safeguards, whereas a 10% benchmark indicated an intolerable level of non-compliance. Statistical significance (p>0.05) was calculated using the one-sample χ^2 test for non-parametric data, the choice of which was informed by the lack of randomisation, the sample size and the type of data collected.[14] While the cross-tabulations were used to determine the degree of statistical significance, the phi coefficient helped to calculate the extent of the correlation, the strength of which was determined by the Pearson χ^2 test.

Section A of the PAC-CS focused on the compliance of technical and physical safeguards with international standards. The responses to the close-ended questions regarding technical safeguards in terms of password usage, namely the type of passwords and the frequency of password changes, will be presented.

Results

The study results were evaluated in line with the following definition: the situated practices for effective password usage of HP are conceptually defined as the complete range of functions, activities, roles, responsibilities and decision-making capabilities in which individuals are competent, educated and authorised to perform within a specified work environment in complying with the minimum standards of effective password usage. In Table 1 and Fig. 1, the study questions and the corresponding responses that relate to the effectiveness of passwords when using PACS technology are summarised.

According to Table 1, 102 participants (90% of the sample) were expected (EN) to use individual passwords to access PACS. Only 27% of the participants complied with the use of individual passwords, while the remainder, 78%, used shared departmental codes instead. A further 23% of participants accessed PACS without requiring a password, and only 2% changed their PACS passwords on a monthly basis. Moreover, a mere 3% of the PACS workstations remained active for less than a minute. In determining the extent of the non-usage of passwords, cross-tabulations between the radiology and non-radiology groups were conducted. Fig. 1 demonstrates that staff members in radiology departments accessed the PACS workstations without the use of an access code to a greater extent than their non-radiology counterparts.

Table 1. Summary of effective password usage

Benchmark	Response	Expected, *n* (%)	Observed, *n* (%)	Extent of compliance*
Do you have a unique PACS access code? (*N*=113)				
Yes=90%	Yes	102 (90%)	31 (27%)	27%
	No	11 (10%)	82 (73%)	
Does your department have a PACS access code which everybody uses? (*N*=114)				
No=90%	Yes	11 (10%)	89 (78%)	22%
	No	103 (90%)	25 (22%)	
Can you access data from the PACS without using an access code? (*N*=110)				
No=90%	Yes	11 (10%)	25 (23%)	77%
	No	99 (90%)	85 (77%)	
Approximately how long does the PACS work station remain active? (*N*=113)				
<1 min	<1 min	102 (90%)	3 (3%)	3%
90%	1 min	8 (7%)	4 (4%)	
	>1 min	2 (2%)	44 (39%)	
	All the time	1 (1%)	62 (54%)	

*p=0.000

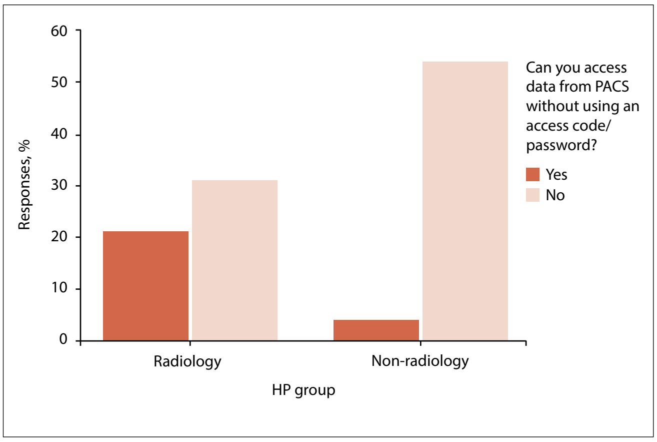

*Fig. 1. Cross-tabulations on effective password usage between radiology and non-radiology Picture Archiving and Communication System (PACS) users. A significant difference was indicated (*p<0.05*) between the observed practices and the expected password requirements. (HP = health professional).*

Discussion

PACS workstations are purposefully designed to provide instant access to data. By design, PACS is inherently a password-driven technology. The password requirement serves: (*i*) as a means of restricting access to data only to authorised PACS users; and (*ii*) to authenticate the person accessing the data. The password-driven nature of PACS in itself is a form of an inscribed ethic designed to protect the confidentiality of patient data stored in the PACS. In protecting confidentiality, patients' privacy is secured, and the intrinsic value of patients as human beings is recognised. Not all types of passwords are considered effective in delivering the ethics inscribed in PACS technology. The minimum standards for effective password usage necessitate that passwords are long and contain a variety of characters that would not be easy to crack.[6] As a gold standard, individual passwords rather than shared passwords are recommended, and these need to be changed frequently. The benefit of effective access restriction is the protection of patient confidentiality, which HPs are obligated to uphold. In the original study, the motivations informing the choice of passwords for the various departments within a hospital setting could not be ascertained. This paper draws on other literature findings to explore possible reasons for poor compliance with the minimum standards of effective passwords, specifically for emergency departments.

The study outcomes vary from 27% of participants using individual passwords, to 78% who used shared departmental passwords. In cases where the automatic log-off was disabled, participants accessed PACS without requiring passwords, and this accounted for 23% of the results. The multidisciplinary nature of the study participants introduces a range of functions, activities, roles and responsibilities that should be considered within a specified work environment when explaining the inconsistency in the types of passwords used. It appears that some sections within the hospital setting used passwords that were unique to each department and shared by all members within that particular section, accounting for the 78% use of shared departmental passwords. It could not be ascertained whether the choice of departmental passwords complied with the requirement for hard-to-crack passwords. It may be postulated that the departmental password should be easy to remember, and have predictable features that are not consistent with hard-to-crack passwords.

Perhaps the staffing issues unique to the medical setting provide compelling reasons for the use of departmental passwords. For instance, nursing departments employ a significant number of temporary staff, while casualty officers and some specialist doctors, such as traumatologists, work on an on-call basis whereby they may rotate within the public and private sectors. Setting up an individual password for each of the temporary and rotational staff may be a costly, time-consuming and futile exercise when a staff member may be employed only for one day. It may not be possible to set up passwords for an urgent replacement organised at the last minute to replace a staff member who called in sick for duty.

Unlike general wards and intensive-care units where nurses, referring doctors and radiographers could all access PACS, the radiology department is mainly accessed by radiology staff, making it susceptible to practices of accessing PACS without requiring a password. This practice may be endorsed by the culture of trust that dominates medical environments, in which HPs are considered to be ethical beings who respect confidentiality and therefore require minimal supervision.[7] Emergency and theatre departments may be a further example of environments where passwords are not utilised. In contrast, doctors' consulting rooms may be suitable for the use of individual passwords, accounting for the 27% reported in this study. The advantage of using individual passwords is that improper conduct relating to data security may be traced back to the offender. Audit trails are mandatory by law, as otherwise, how would violations of confidentiality be punished?

In a medical emergency, a patient's life may be threatened by the sudden and unexpected development of a health condition. High unpredictability and the requirement for expedited service delivery are characteristic of a medical emergency department. The need for efficiency raises challenges that require a balance between the right to life, efficiency and the protection of human dignity. The right to life and the right to dignity are enshrined in sections 10 and 11 of the SA Constitution, respectively.[17] Section 2.3(a) of the Patient's Rights Charter states that everyone has the right to receive timely emergency care.[18]

Members of the emergency team never know what to expect at any given point in time, resulting in feelings of anxiety.[19] When attending to multiple patients at the same time, overcrowding, high noise levels and fatigue may result in interruptions of the thinking and decision-making process.[20] These factors are cited in the literature as the leading cause of errors in diagnosis associated with clinical emergencies.[21] The need for efficiency in emergency departments induces stress in members of the emergency team. Individuals are likely to forget passwords that are long and contain a variety of characters, especially when working under stressful conditions.[6,22,23] Perhaps considerations regarding the right to life and timely access to emergency care inform some of the practices that result in the accessing of the PACS without requiring a password. Similar reasons may account for the 54% of PACS workstations that were not capable of automatic log-off, causing them to remain active all the time.

Conclusion

This paper highlights the dilemma in emergency departments between the need for efficient patient treatment and respect for patient ethical rights. In a medical environment dominated by a culture of trust, human dignity may not be the primary concern, especially when competing with the supreme right to life. However, just because HPs are inclined to trust one another, based on the assumption that HPs are ethical beings who respect patient confidentiality, this does not mean that all HPs are trustworthy. There may be occasions when patients suspect that HPs may abuse their privileges of access to medical records.[24]

The protection of patient data requires the fulfilment of diligent security measures, including the use of effective passwords and automatic computer log-off. These measures may be time-consuming, and therefore not suitable for the levels of efficiency needed in emergency departments. The use of effective passwords is necessary to protect human dignity, the provision of which is enshrined in section 14(d) of the SA Constitution.[17] Yet, practices that are compliant with the minimum standards of effective passwords stand to threaten the supreme human right to life.

In a medical emergency, seconds count. Computers take ~60 seconds to initialise and authenticate the user, excluding the additional time needed to process an image or to call up patient data.[25] Depending on the type of medical emergency, 60 seconds could mean the difference between organ impairment and death. Eliminating the time for computer initialisation and authentication could go a long way towards saving lives. At the time of this report, there were no data to suggest that lives have been lost as a result of computer initialisation and authentication. However, the lack of data does not mean that incidents have not occurred or will not occur in the future.

It remains unclear whether compliance with the minimum standards for effective password usage is suitable to emergency departments. This article may have contributed to normative ethics in asking the question as to whether medical emergency departments ought to be an exception to the minimum standards of effective password usage. The reasons for non-compliance presented in this article are mere suggestions drawn from the literature. Future research is needed, firstly, to determine reasons for non-compliance specific to the use of PACS in an emergency department; and secondly, to determine alternative security measures that would aid in preserving patient confidentiality in such departments.

Acknowledgements. This article presents the findings of a Master's dissertation obtained through the University of Johannesburg. Both authors greatly appreciate the permission granted by the research settings and the contribution of the participants.

Author contributions. TBM and BvD worked jointly in preparing and approving the article for submission. In her capacity as the primary researcher, TBM contributed to project design and data collection. BvD was the study supervisor, and made enormous contributions to the conceptual framework and editing of the manuscript.

Funding. None.

Conflicts of interest. None.

1. Dayarathna R. The principle of security safeguards: Unauthorized activities. Comput Law Secur Rev 2009;25(2):165-172. https://doi.org/10.1016/j.clsr.2009.02.012
2. Princely I. Understanding information security systems policy compliance: An integration of the theory of planned behaviour and the protection motivation theory. Comput Secur 2012;31(1):83-95. https://doi.org/10.1016/j.cose.2011.10.007
3. Steers K. Boot passwords, put your PC under lock and key. PC World 2003;21(9):168.
4. Stross R. Goodbye passwords, you aren't a good defence. 8 October 2008. http://www.nytimes.com/2008/08/10/technology/10digi.html (accessed 27 May 2017).
5. Jeffersen G. Forget passwords – use your face instead [press release]. USA: USA Today Edition; 1 May 2015.
6. Payton L. Memory for passwords: The effect of varying number, type and composition. Psi Chi J Undergrad Res 2010;15(4):209-213.https://doi.org/10.24839/1089-4136.JN15.4.209
7. Williams PAH. In a 'trusting' environment, everyone is responsible for information security. Inf Sec Tech Rep 2008;13(4):207-215. https://doi.org/10.1016/j.istr.2008.10.009
8. Robinson R. Moral distress. Dimens Crit Care Nurs 2016;35(4):235-240. https://doi.org/10.1097/dcc.0000000000000185
9. Mahlaola TB. Compliance of health professionals with patient confidentiality when using PACS and RIS. PhD thesis. Johannesburg: University of Johannesburg, 2013. https://scholar.google.co.za/citations?user=SxxS8R4AAAAJ&hl=en
10. Beach J, Oates J. Maintaining best practice in recordkeeping and documentation. Nurs Stand 2014;28(36):45-50. https://doi.org/10.7748/ns2014.05.28.36.45.e8835
11. Bolan C. A view of the future image exchange. Appl Radiol 2013;42(11):32-37. http://appliedradiology.com/articles/technology-trends-a-view-of-the-future-image-exchange (accessed 24 October 2017).
12. Benatar D. Indiscretion and other threats to confidentiality. S Afr J Bioeth Law 2010;3(2):59-62. http://www.sajbl.org.za/index.php/sajbl/article/view/101/83 (accessed 24 Oct 2017).
13. International Organization for Standardization. Improved ISO/IEC 17799 makes information assets even more secure. https://www.iso.org/news/2005/06/Ref963.html (accessed 24 October 2017).
14. Daniel J. Sampling essentials: Practical Guidelines for Making Sampling Choices. Washington DC: SAGE Publications, 2012. https://doi.org/10.4135/9781452272047

15. Health Professions Council of South Africa. Confidentiality: Providing and Protecting Information. Booklet 11. http://www.hpcsa.co.za/Uploads/editor/UserFiles/downloads/conduct_ethics/rules/generic_ethical_rules/booklet_10_confidentiality_protecting_and_providing_information.pdf (accessed 2 October 2011).
16. Cao F, Huang HK, Zhou XQ. Medical image security in a HIPAA mandated PACS environment. Comput Med Imaging Graph 2003;27(2-3):185-196. https://doi.org/10.1016/s0895-6111(02)00073-3
17. Constitution of the Republic of South Africa, 1996.
18. Health Professions Council of South Africa. National Patients' Rights Charter. Booklet 3. http://www.hpcsa.co.za/downloads/conduct_ethics/rules/generic_ethical_rules/booklet_3_patients_rights_charter.pdf (accessed 10 July 2017).
19. Croskerry P, Cosby KS, Schenkel SM, Wears RL. Patient Safety in Emergency Medicine. Philadelphia: Wolters Kluwer Health, 2009.
20. Palmer LK. The relationship between stress, fatigue and cognitive functioning. Coll Stud J 2014;48(1):198-211. https://eric.ed.gov/?id=EJ1022296 (accessed 24 Oct 2017).
21. Luigi BP. Error risk in decision-making process. Emerg Care J 2014;10(1):37-40. https://doi.org/10.4081/ecj.2014.2119
22. Healy S, Tyrrel M. Stress in emergency departments: Experiences of nurses and doctors. Emerg Nurs 2011;19(4):31-37. https://doi.org/10.7748/en2011.07.19.4.31.c8611
23. Espana LY. Effects of password type and memory techniques on user password memory. Psi Chi J Psychol Res 2016;21(4)269-275. https://doi.org/10.24839/b21.4.269
24. Akyüz E, Erdermir F. Surgical patients' and nurses' opinions and expectations about privacy in care. Nursing Ethics 2013;20,(660)e671. https://doi.org/10.1177/0969733012468931
25. Ganthan NS, Rabiah A, Zuraini I. Security threats categories in healthcare information systems. Health Inform J 2010;16(3):201-209. https://doi.org/10.1177/1460458210377468

Accepted 17 October 2017.