J Digit Imaging (2013) 26:1040–1044
DOI 10.1007/s10278-013-9618-3

# The Information Security Needs in Radiological Information Systems—an Insight on State Hospitals of Iran, 2012

**Akram Farhadi · Maryam Ahmadi**

Published online: 13 July 2013


**Abstract** Picture Archiving and Communications System (PACS) was originally developed for radiology services over 20 years ago to capture medical images electronically. Medical diagnosis methods are based on images such as clinical radiographs, ultrasounds, CT scans, MRIs, or other imaging modalities. Information obtained from these images is correlated with patient information. So with regards to the important role of PACS in hospitals, we aimed to evaluate the PACS and survey the information security needed in the Radiological Information system. First, we surveyed the different aspects of PACS that should be in any health organizations based on Department of Health standards and prepared checklists for assessing the PACS in different hospitals. Second, we surveyed the security controls that should be implemented in PACS. Checklists reliability is affirmed by professors of Tehran Science University. Then, the final data are inputted in SPSS software and analyzed. The results indicate that PACS in hospitals can transfer patient demographic information but they do not show route of information. These systems are not open source. They don't use XML-based standard and HL7 standard for exchanging the data. They do not use DS digital signature. They use passwords and the user can correct or change the medical information. PACS can detect alternation rendered. The survey of results demonstrates that PACS in all hospitals has the same features. These systems have the patient demographic data but they do not have suitable flexibility to interface network or taking reports. For the privacy of PACS in all hospitals, there were passwords for users and the system could show the changes that have been made; but there was no water making or digital signature for the users.

**Keywords** Picture Archiving and Communications System · Radiological Information System · Information Security

A. Farhadi (✉)
Tehran University of Medical Science, Tehran, Iran
e-mail: Akram_farhadi@yahoo.com

A. Farhadi
e-mail: A-farhadi@tums.ac.ir

M. Ahmadi
Health Information Management, Tehran University of Medical Science, Tehran, Iran
e-mail: m_ahmadi@tums.ac.ir

## Introduction

The overlapping need of medical images and patient record data in electronic format improves the accuracy and efficiency of patient management. With the development and implementation of different separate systems for image management and for other medical data, it is often very difficult to provide an integrated presentation of a single EMR that links to all sources of data for a given patient. It is also not unusual in large medical institutions to implement different Picture Archiving and Communications System (PACS) archives in deferent departments or sections. The compliance of cardiology, nuclear medicine, and radiology systems with standards such as the Digital Imaging and Communications in Medicine (DICOM) standard ensures that image data can be exchanged and retrieved from different systems into a single point of review [1]. (Roger Bauman, et al. suggested PACS for the first time. They used this term in hospitals but the application of this term changed during the years. PACS was originally used for allowing a better communication between radiologists and clinicians in film-based media, but 20 years ago, its services changed to capture medical images electronically so the usage of PACS increased in that term. They could decrease the cost of medical images by changing it to electrically images) [2]. Medical diagnosis methods are based on images such as clinical radiographs, ultrasounds, computed tomography (CT) scans, magnetic resonance imaging (MRI),

or other imaging modalities. Information obtained from these images are correlated with patient information such as study type, patient name or id, personal data, date, hospital ID, machine ID, diagnostic findings, prescriptions, and so forth [3]. In Iran, there were different radiological information systems (RIS) that were not integrated and they were imperfect. We have done this research to determine the defects of PACS and RIS in Iran.

## Literature Review

Since the paper would be evaluating the PACS and the security control implemented, it is imperative to conduct a comprehensive literature review from two angles i.e., to see the advancement, adoption of PACS itself, and the security consideration in PACS.

Since medical information systems consist of images and of their interpretations by the radiologists, a reporting system is required when PACS is introduced into hospital. This facilitates linkage of the reports with patient image data [4]. Nowadays, PACS make a connection between images and their uses; both images and their data are important and they are complementary to each other. The data of images would be more helpful if it could be organized in appropriate way. This data should be organized and managed based on standard criteria. Other information such as disease reports has to be established and an access mechanism has to allow combinations of information to make a better diagnosis. Complete and accurate data of images can help clinicians to use them in more applicable ways [5].

PACS is designed to communicate among people in the primary care of patients. One of the most important components of PACS such as image distribution provides the images and accurate information for health care providers. Usage of PACS affects the time and quality of care and help clinicians to make decisions in a shorter time [2]. The PACS should be integrated in the hospital information system (HIS) and several modalities of different vendors should be attached to it. Three critical factors influence the success of PACS installation such as: the support of the workflow, the interface of the RIS to the modalities, and the security policy to allow hospital-wide access to the images and results in the PACS. The PACS is an add-on to the RI driven by the RIS as the master [6]. The information asset of PACS is the image and patient demographic data that come from the imaging modalities such as CT, MRI, ultrasound, digital subtraction angiogram, digital subtraction imaging, computed radiography, direct radiography, and the PACS broker [7]. Individual radiology should have the information of registration, acquired information, interpretation of data, information of image management, radiology management, the report of the case and its transcriptions, and the radiology-scope research. It should also include the viewpoints of different radiology staff such as: radiologists, referring clinicians, radiology administrators, and radiology researchers. This individual radiology could help radiologists to get the required information and make a decision in an applicable way [8].

Connection of PACS to other systems such as radiological information system or health information system requires the linking of medical images with other patient data thus it should have the necessary data: information of past medical history, laboratory data, and reports on the previous images through RIS or HIS for physicians to make a correct diagnosis based on complete information. Without this information, PACS would have limited diagnostic utility [4]. The integration of the various digital subsystems in a hospital is a prerequisite for a routine clinical operation of PACS and associated systems. Close cooperation between PACS manufacturers and radiologists must be an integral part of PACS development, design and implementation, and particularly, in the task of integration of the systems to guarantee the practical orientation [9]. Comparing the HIS terminals and PACS image workstations, the requirements for PACS workstations are much more complicated than for HIS terminals because of image-display features while having to handle patient data, too. Therefore, PACS terminals can serve also as HIS terminals, provided that they are designed to have the roles described in the preceding section. Image displays controlled by a multi-purpose workstation are the future PACS components [10]. The advantages of PACS and similar systems are ease of access and immediate sharing of data and images that can result in better patient care. With an electronic system, images can be viewed trust-wide, on any terminal, at any time. From the initial impulse to download an image to actually looking at the image, it takes only a few seconds; if you remember the name, you can find the image [11].

Computer and information system security is currently an importation issue. With the proliferation of computers and computer networks into all aspects of business and daily life—financial, medical, education, government, and communications—all concern over secure file access and communications privacy is growing [12]. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) offered some general guidelines to enforce the protection of private medical information. One such guideline stated that patients have the right of accessing their medical records to understand and monitor their health status and the process of diagnosis and therapy [13]. HIPAA had increased the awareness of the security of PACS information. Staff should be informed about the ways of distribution of data and ways for limiting them. They should know more about the people that should know the information and some others that should not know about them. Yet, there are some ways

that access to data cannot be restrained because it is nearly impossible to predict who will legitimately need access to a particular patient's record. Among those systems, the RIS and PACS contain vast amounts of confidential information and are coming under increasing scrutiny by health care privacy officers. Web-based radiology image and report systems are often granted to hundreds or even thousands of clinicians. More of them can access the patient information in a short time but there should be limit access to a need-to-know basis. Also, the satisfaction of patients should be considered. Often, such restrictions cannot be adequately manipulated to restrain access [14].

Medical image security is an important issue when digital images and their pertinent patient information are transmitted across public networks [15]. In telemedicine and teleradiology, image data cannot be limited within a private local area network protected by a firewall. Therefore, the (digital envelop) DE-based security system proposed here offers the most useful security assurance of patient information privacy and image integrity [16]. The use of World Wide Web technologies in radiology is not new. These technologies have been used in radiology-teaching files to access information in multimedia-integrated PACS and for teleradiology purposes. Web technology has also been used to access the images stored in a DICOM archive in PACS environments [17]. Some information are valuable and should not be released for other organizations, therefore the people who have the responsibility of protecting them should be more careful and use confidential ways for transferring data. There should be an efficient scheme for storing the information that needs to be confidential. Also, there should be sufficient means for addressing the risks of disclosure. The storage and communication of information must involve an efficient scheme that will minimize the risk of disclosure and limits the access to the information [12]. Several security services are offered by a security service provider (SSP) in the form of web services. This SSP is independent and acts as a facilitator, it serves the security agents by means of providing directory, conflict resolution, and other services.

A monitor tool can be designed to monitor the pattern and make decisions whether it is an unauthorized data access for the abnormal pattern based on the role-based policy. Any pattern that violates the policy would automatically cause a warning or alert result [18]. Access to the PACS room can be possible by a smart card with an audit-trail system. The power supply in the PACS room can be a series of power points created from a complete set of three-phase essential power supply in the main supply [17].

By today's data security standards, restricted algorithms provide woefully inadequate security. They are easy to break by experienced cryptanalysts and are not suitable for a large or changing group of users. The truth is that data compression, similar to restricted cryptographic algorithms, provides little protection once the compression algorithm used is known by the intruder. For high-security applications, all modern encryption algorithms use a key, which can take on one of many values (larger is better) [19]. The confidentiality and security of data handled by PACS must be considered carefully. Security issues relate to the protection of data handled by PACS against unauthorized access and malicious or accidental corruption and loss. Electronic security measures, such as issuing a password, prevent illegal access to medical information [4].

## Research Methodology

This research has been done in two steps:

First, we surveyed the different aspects of PACS that should be in any health organizations. This includes hardware, software, technology and IT, and communication of PACS [20]. For example, it should have new services (digital image filing and image management), nonphysical image transport (networking), the changing work environment (digital image workstations), and lastly, it should be integrated with health information system [5]. Data base management system (DBMS) of PACS has the following capabilities:

(1) It can be integrated with other PACS modules to connect with other systems and share the information
(2) It has heterogeneous software and hardware
(3) Users have efficient access to required data by this system
(4) It has an automatic database recovery and reduces the redundancy of data
(5) An open architecture-interface helps it to connect with other DBMS
(6) It is object oriented and uses advanced tools such as 3GL and 4GL [8]

For the second part of step one, we surveyed the security controls that should be implemented in PACS. We had specific questions with set answers to choose from and it was a pen and pencil-based research. This security controls include (a) security attack that should uses any action to protect the information owned by an organization. This makes sure that the information is saved and protected against unauthorized disclosure; (b) security mechanism includes any process that is designed to detect the risks and make them ineffective or recover the missed information, (c) Security service to provide authentication, access control, and data confidentiality and integrity. This service can control the disclosure of information and somewhere, limit it.

Authentication makes sure that the communicating entity is the one claimed and access control helps to prevention the unauthorized use of a resource. Staff would be sure about the information that they get from others and they can transfer it to others. Data confidentiality should use effective ways to

protect the data from unauthorized disclosure and data integrity assures the staff that the data received is exactly sent by an authorized entity. They do not hesitate about the reliability of data. Also, there should be no repudiation to protect against denial by one of the parties in a communication [15].

This extensive data-gathering activity is performed by searching articles, books, and web sites to get the information for developing the checklist, and then, two checklists was prepared; one for the evaluation of PACS and the other for the evaluation of the security of PACS. The population of the study was six large hospitals in Tehran. They had the largest number of patients and therefore, they were chosen. Researcher filled these checklists by observing the PACS systems and interviewing with PACS administrators. Then, the data is inputted in SPSS software and analyzed. The final data is shown as an average of data in the following table.

## Results

Large State hospitals of Tehran that had the largest number of patients were surveyed. Referring to Table 1, the results indicate that PACS in hospitals can transfer patient demographic information but they do not show the route of information. These systems are not open source. They don't use XML-based standard and HL7standard for exchanging the data. In Shariati and Rasoul hospital, PACS interface with network. None of them interfaces with HIS or RIS. They do not control the data automatically [1].

As Table 1 shows, PACS can reconstruct image for proper display. They don't use DS digital signature. They use passwords and the user can correct or change the medical information. PACS can detect alternation rendered. They can audit database for image related events. These systems show patient number, age, ID, sex and name but they cannot monitor PACS information.

## Conclusion

The survey of results demonstrates that PACS in all hospitals has the same features. These systems have the patient demographic data but they do not have suitable flexibility to interface network or taking reports. About the standards, they just have DICOM standards and other standards for security or connection to other systems were not in these systems.

For preparing The privacy of PACS in all hospitals, there were password for users and the system could shows the changes that has been done in the systems but there were no water making or digital signature for users. PACS systems were not filmless and patients could not access their information.

In Iran, hospitals do not have electronic health records (EHR) so they should have some important qualifications that are necessary for hospital systems such as PACS. These systems qualification are primary steps for applying the EHR. Hospitals should be careful about selecting the PACS that is made by companies. Hospitals should check the important features of PACS that they make themselves or take the company's necessary information needs to prepare the comprehensive systems.

This study shows the strengths and weaknesses of systems, system users can use the study results for developing their systems, and managers can use the study results for developing their standards in different systems such as PACS and RIS. Most users have enough information about the system. They are told that creating such facilities in the system is costly, and then, their managers do not collaborate with them to develop the systems based on standards.

**Table 1** Evaluating the PACS in Hospitals of Iran

| | Shariati | Firuzgar | Emam | Farabi | Taleghani | Rasoul |
|---|---|---|---|---|---|---|
| Transferring patient demographic information | Yes | Yes | Yes | Yes | Yes | Yes |
| Being open source | Yes | Yes | Yes | Yes | Yes | Yes |
| Using of standards | Yes | Yes | Yes | Yes | Yes | Yes |
| Supported by IT | Yes | No | Yes | No | Yes | Yes |
| System controlling | No | No | No | No | No | No |
| System workstation abilities | Yes | Yes | Yes | No | Yes | No |
| Security of system | Yes | Yes | No | Yes | Yes | Yes |
| Auditing | Yes | Yes | Yes | Yes | Yes | Yes |
| Privacy of PACS | Yes | Yes | Yes | Yes | Yes | Yes |
| Auditing database for image related event | Yes | Yes | Yes | Yes | Yes | Yes |
| Patient table of system | Yes | Yes | Yes | Yes | Yes | Yes |
| Using of system for study | Yes | Yes | Yes | Yes | Yes | Yes |
| HIPAA-complaint audit trails | Yes | Yes | Yes | Yes | Yes | Yes |

**Acknowledgments** Tehran University of medical science funded this project.

## References


1. Ratib O, Swiernik M, Mccoy M: From PACS to integrated EMR. Comput Med Imaging Graph 27:207–215, 2003
2. Huang HK: Enterprise PACS and image distribution. Comput Med Imaging Graph 27:241–253, 2003
3. Rao NV, Kumari V: Watermarking in medical imaging for security and authentication. Inf Secur J 20:148–155, 2011
4. Kuroda C, Yoshioka H, Kadota T, Narumi Y, Okamoto H, Kumatani T, Hiruma O, Kumatani Y, Yoshida J: Small PACS for digital medical images-reliability and security in a clinical setting. Comput Methods Programs Biomed 43:101–106, 1994
5. Meyer-Ebrecht D: Picture archiving and communication systems (PACS) for medical application. Int J Bio-Med Comput 35:91–124, 1994
6. Schrader U, Kotter E, Pelikan E, Zaiss A, Timmermann U, Klar R: Critical success factors for a hospital-wide PACS. Proc AMIA Annu Fall Symp, 1997
7. Tong C, Fung KH, Huang H, Chan K: Implementation of ISO17799 and BS7799 in picture archiving and communication system: local experience in implementation of BS7799 standard. Int Congr Ser 1256:311–318, 2003
8. Taira R, Stewart B, Sinha U: PACS database architecture and design. Comput Med Imaging Graph 15(3):171–176, 1991
9. Mosser H, Urban M, Durr M, Ruger W, Hruby W: Integration of radiology and hospital information systems (RIS, HIS) with PACS: requirements of the radiologist. Eur J Radiol 16:69–73, 1992
10. Kimura M: PACS and patient data management systems. Comput Methods Programs Biomed 36(2-3):107–112, 1991. :2-3
11. Das-purkayastha P, Mcleod K, Canter R: Lack of confidentiality with picture archiving and communication system (PACS). J R Soc Med 97:455–458, 2004
12. Monk D, Canessa J, Canessa G. system and method of encryption for DICOM volumes. Patent Application Publication. Us 2010/0115288A1; 1–9
13. Huang L, Chu H, Lien C, Hasia C, Kao T: Privacy preservation and information security protection for patients' portable electronic health records. Comput Biol Med 39:743–750, 2009
14. Coleman R, Ralston M, Szafran A, Beaulieu D: Multidimensional analysis: a management tool for monitoring HIPAA compliance and departmental performance. J Digit Imaging 17(3):196–204, 2004
15. Rohini S, Bairagi V: Lossless medical image security. Int J Appl Eng Res, Dindigul 3(1):536–541, 2010
16. Cao F, Huang HK, Zhou XQ: Medical image security in a HIPAA mandated PACS environment. Comput Med Imaging Graph 27:185–196, 2003
17. Fernandez-bayo J, Babero O, Rubies C, Sentis M: Distributing medical images with internet technologies: a DICOM web server and a DICOM java viewer. RadioGraphics 20(2):581–590, 2000
18. Liu B, Zhou Z, Huang HKA: HIPPA-complaint architecture for securing clinical images. J Digit Imaging 19(2):172–180, 2006
19. Wong S: A cryptologic based trust center for medical images. J Am Med Inf Assoc, JAMA 6(3):410–421, 1996
20. Cohen M, Rumreich L, Garriot K, Jennings S: Planning for PACS: a comprehensive guide to nontechnical considerations. Am Coll Radiol 2:327–337, 2005