# SAFETY ASPECTS IN SHARED MEDICAL IT ENVIRONMENT

**Igor Dugonjić[1], Mihajlo Travar[2], Gordan Bajić[1]**

*[1]Pan-European University "Apeiron", Banja Luka, BiH*

*[2]University of Business Studies, Banja Luka, BiH*

**Critical Review**

DOI: **10.7251/JIT1802086D** UDC: **001.3:61]:615.849**

**Abstract:** Regional PACS and other shared medical systems are primary intended for sharing medical images. In these systems, the number of users is significantly increased in relation to local systems, and the fact is that the public network is very frequently used for data transfer. As medical data are very sensitive, such situation creates considerable risk regarding privacy, integrity and right to access to these data. This paper includes the most frequent risks and methods to solve these issues as well as recommendations for safe use of cloud computing systems in order to implement these systems.

**Keywords:** PACS, DICOM, IHE.

## INTRODUCTION

In the era of fast changes and increasingly less time necessary to put an innovation in use, there is a great urge to accomplish as much as possible with the minimum of effort and tools. It is common for radiology wards in hospitals to possess and use a central information system such as Picture Archiving and Communication System (PACS), Radiology Information System (RIS) and the like.

While Electronic Medical Record (EMR) is able to coordinate handling with medical content (medical image with meta-data) which come from different viewers, EMR users must face the work with different viewers from different wards [17]. Due to this fact, it is easy to predict users' dissatisfaction because of the need to work in several different applications that are basically intended for the same job [13][5]. This why there is also a problem on the level of a health institution due to allocation of funds for maintenance of several small or medium archives.

The logical solution to this problem is the centralisation of the medical data archiving system on the regional or national level rather than local level only. Such organisation can improve the level of health services in human resources, education, and R&D, develop better and more comprehensive patient monitoring systems and possibility of improving new healthcare services.

The use of PACS creates a data sharing mechanism. These data may be delivered to a regional PACS client or any XDS client (document user). Apart from advantages such system can offer, it also poses certain risks. The growth of a system to the regional level significantly increases the risk of its users, which also leads to significant increase in safety risks. Therefore, it is necessary to analyse the risks and develop mechanisms to enhance medical image security.

## SECURITY CONSIDERATION

The Royal College of Radiologist (RCR) prescribes standards for patient confidentiality, and RIS and PACS [11]. Confidentiality is one of the basic patient-physician relationship principles. However, attention should be paid in introducing modern technologies since this relationship may include other participants as well. Pursuant to Data Protec-

tion Act (1998) [3], the Human Rights Act (1998) [8] and National Health Service Act (NHS) (2006) [10], RCR defines the following key identification data on patients: patient's name, address, full post code, date of birth, pictures, photographs, videos, audio tapes, NHS number, local patient identifiable codes and anything else that maybe used to identify a patient directly or indirectly, for example rare diseases, drug treatments etc.

Although PACS brings many possibilities to improve radiological practice on one hand, there is a significant risk to patient confidentiality on the other. This risk may occur in case of improper use of PACS. Some of these examples are searching images and results by medical staff not involved in a patient's care as well as searching images and results by individuals unauthorized for the access to such medical archives [11].

The 1996 Health Insurance Portability and Accountability Act (HIPAA) requires, among other things, the protection from unauthorized access to patient data [7]. Medical images obtained from CR, CT, MRI, US etc. cannot be used without other information such as description of diagnosis, possible reference to the history of disease, previous treatments and other information on the patient. This complex set of information on the patient is highly sensitive. This is why a high level of security is required for the data handled by regional PACS.

Training has always been one of the most important parts in radiology. Images adequate for training or research need to be created as anonymous i.e. personal data on patient and other information that may indicate the patient's identity during sending to the regional PACS that is used for training and research need to be replaced with fictitious data.

Besides economic advantages, the service quality such as greater availability, high reliability and scalability is the main incitement to use cloud computing. However, in case of outsourcing i.e. clinical data transfer to the cloud, health institutions face many challenges that should be taken into consideration in the preparation phase of integration. Namely, privacy and confidentiality of data in the cloud is the main obstacle for cloud to be widely accepted due to the risk of compromised user's data confidentiality when the data are transferred to cloud.

## Privacy Protection and Regulation of Right to Access

Data need to be protected at three different levels, as follows: a) data transferred in the public network, b) data stored on the regional PACS server and c) user's access to these data.

Health institutions not covered by own optical network are oriented to public networks, which is much more economical but requires the use of data protection cryptography.

The safety of data sent through public network may be ensured by using dedicated optical cables whenever possible, and by using encrypted tunnels with a high level of protection in all shared lines used in another network traffic. For this purpose, IPSEC tunneling (Internet Protocol Security tunelling) may be used, most frequently with Advanced Encryption Standard AES-256 encrypting algorithm. IPSEC is the most frequently used safety control on network layer for private data protection through public IP networks. Depending on how it is implemented and configured, IPSEC can provide any combination of the following protection types: Confidentiality, Integrity, Authentication, Replay Attack Protection, Traffic Analysis Protection, and Access Control [15]. The most frequent method of using IPSEC implementations is Virtual Private Network (VPN) service. VPN is a private network built on the already existing physical network, which can ensure a safe communication mechanism for data and information sent through the network.

The safety of data stored in a shared medical archive can be attained by using a hardware intended for this purpose as well as strict restriction of physical and network access to the equipment. One of the ways to implement the access control is to use two firewalls, one of which is controlled by the local health institution and its staff, and the other (external) firewall by the regional PACS engineering staff. This allows the regional PACS administrators to control the access to central resources, while the health institution network administrators can control the access to their network. This allows anybody to have the access to resources they are responsible for and which they control. This refers to both network connection variants i.e. those implemented with optical cables and those using IPSEC tunnel between the regional PACS server and local institution.

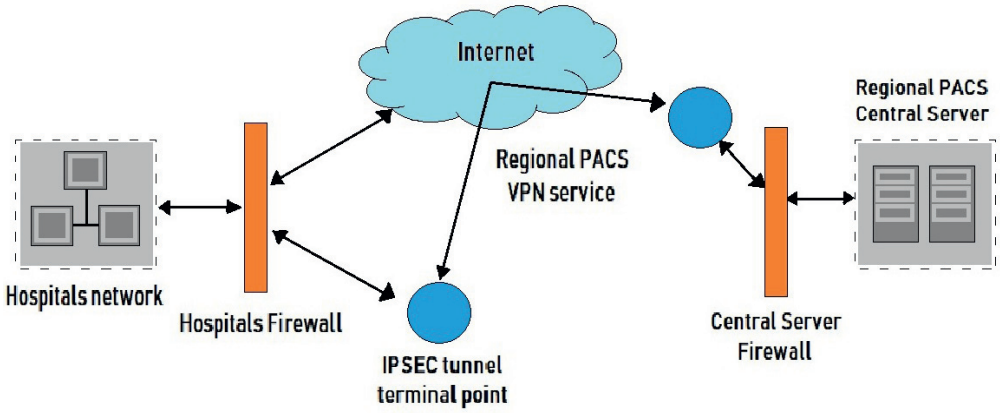


***Figure 1.*** *Health institutions interconnection model using IPSEC tunnel*

As with a local medical data exchange server, the regional system must have the access to data; however, generally in this case the data are in a remote location and need to be accessed through the public network. The aspect of data privacy protection from unauthorized reading and changing in the regional systems expands the requirements the local PACS needs to fulfil. Data security must primarily be protected from those who are not system users.

When the local PACS is integrated into the regional system, there is the risk of unauthorized reading of medical data. This risk is present primarily due to the fact that local centres need to be connected into a joint network. The right to access to the regional system must be reduced in relation to the access to the local PACS. This comes from the fact that system users, generally, should not have the same rights in a remote centre in comparison to a local centre.

The access to medical images and related data must be defined in line with users' rights. The situation in the regional PACS is more complicated when it comes to the local centre. The ownership structure of local centres is generally heterogeneous, and the right of access policy and users' privileges in the system must be in line with the specific needs and requirements. Table 1. shows an example of establishing the regional PACS users' rights.

Digital identity can be defined as a set of claims made by one digital subject about itself or another digital subject [2], while determining the digital identity is reduced to what the subject: is (fingerprint), knows (password), has (token), does (motor skills), where he/she is etc.

Organized pairs of username and password may be used to log into the local system. Although such authentication system carries certain risks, it may

***Table 1.*** *Example of establishing a regional PACS system user's rights*

| | | Local center | | Remote center | |
|---|---|---|---|---|---|
| | | **Radiographer** | **Radiologist** | **Radiologist** | **System Administrator** |
| Local center | Image saving | Yes | Yes | Yes | Yes |
| | Image describing | Yes | Yes | Yes | Yes |
| | Raport writing | - | Yes | Yes | - |
| | Raport reading | Yes | Yes | Yes | Yes |
| | Administration | - | - | - | Yes |
| Remote center | Image saving | - | - | - | Yes |
| | Image describing | - | - | Yes | Yes |
| | Raport writing | - | - | Yes | - |
| | Raport reading | - | - | Yes | Yes |
| | Administration | - | - | - | Yes |

yield satisfactory results in some specific cases. PACS users identity in more complex systems may be based on Public Key Infrastructure (PKI). In that case, it is expected that every user that uses more than one workstation or who shares a workstation with someone else must possess Dongle that generates a private key. The competent body prescribes an appropriate public key. The issue of medical specialists' electronic identity should be solved globally i.e. for the whole system [16].

When regional PACS is used for educational or scientific purposes, it is important to establish the coordination in marking medical images with fictitious data so that the patient's identity always remain hidden. On the other hand, students or researchers have the access not only to individual medical images but also to series of images for a more complex insight into the history of disease and applied treatments. It is very important to deny access to sensitive and confidential information on the patient. A frame structure for training consists of the case study object. Every such object is a hypertext object describing a specific medical case and directing to relevant, also anonymous medical images. The data for a real patient originating from different clinical centres must use the same fictitious identity. Such principle allows students a more complex insight into the history of disease. Using Web Access to DICOM Objects (WADO) service, web client may require the access to DICOM objects such as medical images or medical reports in a remote repository. One of important parameters supported by WADO service is data anonymisation. It enables removal of all identification patient's data from DICOM objects if those have not been previously removed [4].

The current state of cloud computing does not guarantee privacy and confidentiality of stored data due to possible publishing and unauthorized use of those data. World Privacy Forum (WPF) suggests several pieces of advice for cloud computer users: a) the terms of service provision need to be carefully considered prior to storing any information into cloud and, if the terms are inappropriate or unclear, another cloud provider should be taken into consideration. b) information stored in cloud are more available than those in a private computer, due to which sensitive information should not be transferred into the cloud. c) in case of data withdrawal by users, it is important that the cloud provider does not retain the right to those data. d) During a change in requirements for service provision, make sure the user is informed on it [6]. This clearly shows that there are great risks regarding data confidentiality in using of cloud service.

Even in case of data anonymisation it is possible that they can be illegally used or sold to a third party for statistical purpose. Therefore, cloud computing without additional systems of data privacy and confidentiality is inadequate for storing any kind of confidential information. It is often impossible to provide a system so that it can avoid information 'leak' or data mining performed to separate certain patterns from medical data. Apart from that, there are many unclear situations such us 'if provider goes bankrupt, what will happen to the data in cloud?' Furthermore, there is the issue of provider's headquarters, users' headquarters and server location not being in the same countries, each of them having different legislation: In case of a dispute, which law is applicable? Therefore, these situations should also be taken into account when creating a system working under cloud.

In order to combine two concepts - Cross Enterprise Document Sharing for Imaging **(**XDS-I) and public cloud - it is necessary to ensure the privacy and confidentiality of protected medical information (PHI) without removing the interoperability between XDS-I profile. The way the privacy and confidentiality, and at the same time interoperability in migration of two XDS-I profiles to cloud, are ensured is by applying some of protection procedures such as coding during storing and on-the-fly decoding, or middleware coding/decoding and XDS-I with privacy protection. XDS-I with privacy protection allows protection and interoperability on the architecture level because trends and actors would be the same as in XDS profile. The shortcoming of this is the lack of interoperability on the document level because such profile has not been planned by IHE yet [12].

## Digital Watermarking

DICOM is the standard for transmission and storage of medical images. All installed equipment in a shared system should be fully DICOM compatible. The main content of DICOM image is medical visu-

al information, while DICOM header also contains metadata. These very sensitive data should be adequately protected.

Digital watermarking offers a suitable technique to ensure the authenticity and copyrights of medical images. For watermarking to be useful, the process of adding watermark on a medical image should be done immediately after obtaining the image on modality.

In respect of the visibility, watermarks are classified into visible and hidden, while in terms of resistance, watermarks are classified into robust and fragile watermarks.

A visible watermark is easily visible with the naked eye. This watermark is inserted into an image to be almost impossible to separate it and get the original image. This method can be used to prevent illegal distribution of medical images.

There are much more methods of marking with invisible watermark than method of marking with visible watermark. Invisible watermarks are hidden within the content. They can be detected only with authorized programs. They are used for protection and copyright authentication, ownership confirmation and detection of unauthorized copying. Inserted watermarks are resistant to image processing.

Robust watermarks are resistant to attacks and can be used for copyright protection.

Fragile digital watermarks can be easily destroyed during each attempt of data manipulation and hence they are used to detect changes in digital content. They allow data authentication.

Depending on domain insertion they are classified into spatial, transform and parametric watermarks.

In spatial domain technique, a digital watermark is inserted into positions of lower bits that are not very significant for image display so that the display quality is not impaired. Digital watermark insertion techniques are quite simple and are relatively efficient way to insert an invisible watermark inside an image. Unfortunately, spatial domain techniques are not very resistant to common forms of data manipulation. This method is mainly used to provide authenticity.

The parametric method is based on transforming the original image on the parametric level, where the original image is manipulated by changing its parameters such as illumination, contrast or even colour in case of colour medical images.

Transformational (frequency) domain is the way to insert a digital watermark inside an image that begins with transformation of the original image in a frequency domain. The most used mathematical transform in digital watermark protection methods are Discrete Fourier transform (DFT), Discrete cosine transform (DCT) and Discrete wavelet transform (DWT).When using these techniques, watermarks are not added to intensities of individual parts of an image but to transform ratios, and the image with a digital watermark is obtained by inverse transformation. Such techniques are far more efficient since they allow for the human visual system properties in determining the watermark position inside the image.

This method (Transformational)is the most suitable for medical imaging as it neither impairs the quality of the original image nor changes the image parameters such as i.e. contrast, illumination or bit depth [14]. This method belongs to highly resistant methods in terms of the use of filters and compression.

A valuation of the existing protection methods using a digital watermark in terms of their resistance to imprint and subsequent digitalisation process has shown that the highest potential is in methods that disperse (distribute) the energy of a digital watermark across the entire digital signal. Such approach is inherently resistant to degradation caused by the process of imprinting and subsequent digitalisation, which arises from the very properties of mathematical transform, which is the basis of the approach.

The use of such method is unsuitable since even the tiniest bit changes may render a proper diagnosis problematic. However, RONI (Region of Non Interest), a method that inserts a watermark into a part of medical image that is not used in diagnostics, may be a compromise solution. The solution is a compromise because it uses the positive aspect of watermarking. However, ROI (Region of Interest) remains unprotected i.e. without watermark.

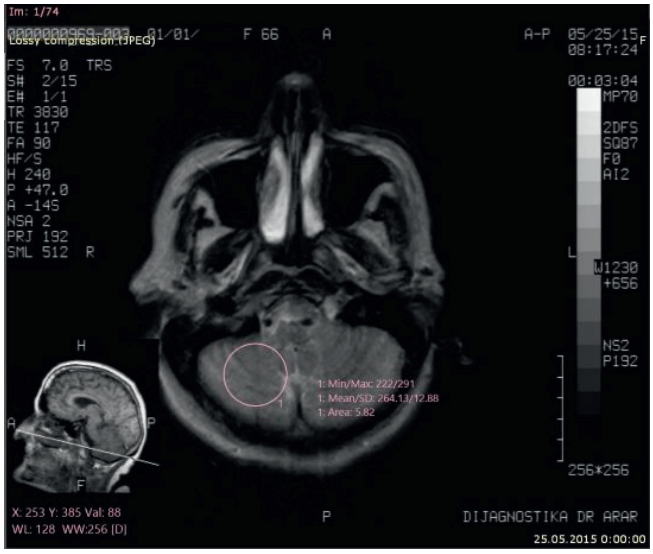


***Figure 2.*** *Manual circular ROI in MR image of head*

Watermarking can be very important in standard radiological practice and training of students and medical personnel staff since it can protect authenticity, proof of ownership and data immutability.

## Conclusion

For a shared regional medical system to be acceptable, it is necessary to pay attention to the rights and privileges of users and administrators on one hand, and confidentiality of patient medical data as well as information on health institutions themselves on the other. The issue of authentication is especially pronounced with mobile users who access the system from different locations or in case a single access point is used by several users. The need to protect medical data from unauthorized access is also pointed out, as well requirements for the use of regional PACS for educational and scientific purposes. Cloud computing is a technology that offers a simple way to allow PACS functionality and possibility of regional integration of local diagnostic centres. However, this technology carries certain risks related to data privacy. This paper deals with these risks and provides certain recommendations for their elimination. Besides, the paper examines the possibility of implementation of XDS-I infrastructure in cloud as well as medical image watermarking.

## References

[1] Avramović Ž. Zoran, Radojičić Z. Radomir, Mirković D. Saša,(2015) A new Approach to Computer Analysis of Queuing Systems Without Programming, JITA- Journal of Information Technology and Applications, JITA 5(2015) 1:25-32

[2] Cameron K., The laws of identity, Microsoft Corp.,https://msdn.microsoft.com/en-us/library/ms996456.aspx, (last accessed 27/10/17)

[3] Data Protection Act (1998), http://www.legislation.gov.uk/ukpga/1998/29/contents, (last accessed 27/11/17)

[4] Digital Imaging and Communications in Medicine (DICOM) Part 18: Web Access to DICOM Persistent Objects (WADO), National Electrical Manufacturers Association, USA 2011

[5] Fuller SS, Kethcall DS, Tarzy-Hornach P: Integrating knowledge resources at the point of care: opportunities for librarians, Bull Med LibrAssoc 87(4):393–403, 1999, Oct

[6] Gellman Robert ,WPF, Privacy in the Clouds: Risks to Privacy and Confidentiality from Cloud Computing, February 23, 2009

[7] HIPAA, Federal Register / Vol. 68, No. 34 / Thursday, February 20, 2003 / Rules and Regulations

[8] Human Rights Act (1998), http://www.legislation.gov.uk/ukpga/1998/42/contents, (last accessed 27/11/17)

[9] MaksimovićMirjana, Implementation of Fog computing in IoT-based healthcare system, (2017) JITA- Journal of Information Technology and Applications, JITA 7(2017) 2:100-107

[10] National Health Service Act(2006), http://www.legislation.gov.uk/ukpga/2006/41/contents (last accessed 27/11/17)

[11] RCR, https://www.rcr.ac.uk/publication/standards-patient-confidentiality-and-ris-and-pacs, (last accessed 27/11/17)

[12] Ribeiro S. Luís, Costa Carlos and Oliveira José Luís: Current Trends in Archiving and Transmission of Medical Images, Medical Imaging, InTech, 2011

[13] Richardson M, MIND scape and PubMed: Web sites that can change the way we work, AcadRadiol 5(7):519–520, 1998, Jul

[14] Rocek Ales, Medical image data security based on principles of digital watermarking methods, Advances in Data Networks, Communications, Computers and Materials ISBN:978-1-61804-118-0

[15] SheilaFrankel, Kent Karen , LewkowskiRyan , Orebaugh D. Angela , Ritchey W. Ronald:Guide to IPSEC VPNs: Recommendations of the National Institute of Standards and Technology Paperback – December 31, 2005

[16] SlavicekKarel, Javornik Michal, Dostal Otto: MeDiMed – Regional Center for Medicine Multimedia Data Exchange, WSEAS TRANSACTIONS on INFORMATION SCIENCE & APPLICATIONS ISSN: 1790-0832 Issue 4, Volume 5, 2008

[17] Stewart BK and Langer SG: Integration of DICOM images into an electronic medical record using thin viewing clients, Proc AMIA Symp 902-6,1998

Submitted: December 17, 2018
Accepted: December 22, 2018

## ABOUT THE AUTHORS

**Igor Dugonjić** earned his Master's degree in computer science at the Faculty of Electrical Engineering, University of Banja Luka. He is currently doing his PhD at Pan-European University 'APEIRON' in Banja Luka. Mr Dugonjić works as a medical equipment programming and maintenance engineer at the University Clinical Centre of Republika Srpska. He has written several scientific papers on medical ICT research.

**Mihajlo Travar** earned his PhD at the Faculty of Mechanical Engineering, University of Belgrade. He is a member of Regulatory Commission for Energy of Republika Srpska. Mr Travar is Associate Professor at the 'University of Business Studies' in Banja Luka, where he gives lectures on the following subjects: Databases, Software Engineering, CASE Tools, Design Engineering and ERP Systems. He has written more than forty scientific papers in ICT, mechanical engineering and business organisation.

**Gordan Bajić** earned his Doctor's degree in health sciences in the field of physiotherapy and work therapy at the Pan-European University "Apeiron", Banja Luka. Gordan Bajic is Assistant Professor of Health Sciences at the Pan-European University, Faculty of Health Sciences "Apeiron" and is vice-dean for teaching at the Faculty of Health Sciences, Pan-European University "Apeiron", Banja Luka. He is a member of many symposiums and has written many scientific papers in the field of medicine, physiotherapy, etc.

## FOR CITATION

Igor Dugonjić, Mihajlo Travar, Gordan Bajić, Safety Aspects In Shared Medical It Environment, *JITA – Journal of Information Technology and Applications*, PanEuropien University APEIRON, Banja Luka, Republika Srpska, Bosna i Hercegovina, JITA 8(2018) 2:86-92, (UDC: 001.3:61]:615.849), (DOI: 10.7251/JIT1802086D), Volume 8, Number 2, Banja Luka, june 2018 (45-96), ISSN 2232-9625 (print), ISSN 2233-0194 (online), UDC 004