J Digit Imaging (2015) 28:481–491
DOI 10.1007/s10278-014-9746-4

Business Model for the Security of a Large-Scale PACS, Compliance with ISO/27002:2013 Standard

Josefina Gutiérrez-Martínez · Marco Antonio Núñez-Gaona · Heriberto Aguirre-Meneses

Published online: 30 January 2015

Abstract Data security is a critical issue in an organization; a proper information security management (ISM) is an ongoing process that seeks to build and maintain programs, policies, and controls for protecting information. A hospital is one of the most complex organizations, where patient information has not only legal and economic implications but, more importantly, an impact on the patient's health. Imaging studies include medical images, patient identification data, and proprietary information of the study; these data are contained in the storage device of a PACS. This system must preserve the confidentiality, integrity, and availability of patient information. There are techniques such as firewalls, encryption, and data encapsulation that contribute to the protection of information. In addition, the Digital Imaging and Communications in Medicine (DICOM) standard and the requirements of the Health Insurance Portability and Accountability Act (HIPAA) regulations are also used to protect the patient clinical data. However, these techniques are not systematically applied to the picture and archiving and communication system (PACS) in most cases and are not sufficient to ensure the integrity of the images and associated data during transmission. The ISO/IEC 27001:2013 standard has been developed to improve the ISM. Currently, health institutions lack effective ISM processes that enable reliable interorganizational activities. In this paper, we present a business model that accomplishes the controls of ISO/IEC 27002:2013 standard and criteria of security and privacy from DICOM and HIPAA to improve the ISM of a large-scale PACS. The methodology associated with the model can monitor the flow of data in a PACS, facilitating the detection of unauthorized access to images and other abnormal activities.

Keywords Availability · BPMN · DICOM · HIPAA · Integrity

J. Gutiérrez-Martínez (✉) · M. A. Núñez-Gaona · H. Aguirre-Meneses
Subdirección de Investigación Tecnológica, Instituto Nacional de Rehabilitación, Av. México Xochimilco 289, Col. Arenal de Guadalupe Tlalpan, 14389 México, D. F., Mexico
e-mail: gtzmtzjos@gmail.com

J. Gutiérrez-Martínez · M. A. Núñez-Gaona · H. Aguirre-Meneses
Departamento de Desarrollo Tecnológico, Instituto Nacional de Rehabilitación, Av. México Xochimilco 289, Col. Arenal de Guadalupe Tlalpan, 14389 México, D. F., Mexico

Background

A PACS (picture and archiving and communication system) [1] is a complex system for transferring, storing, and displaying medical images; it is composed of a great number of autonomous and heterogeneous components interconnected by means of a high-performance network, including database servers. Today, PACS has become very important in effective management of imaging departments in hospitals where there are a large production of medical images.

Actually, most PACS are in compliance with the DICOM (Digital Imaging and Communications in Medicine) standard [2]. This standard, released by ACR (American College of Radiology) and NEMA (National Electrical Manufacturers Association), is a protocol defined into 20 parts to exchange medical images and associated information between two systems or AE (Application Entities). It includes the file format definition for network communication TCP/IP (transmission control protocol/Internet protocol). DICOM enables the integration of the various medical image data acquisition devices, such as scanners, servers, workstations, printers, storage, and viewers, as well as, network hardware from multiple manufacturers.

PACS should work with any radiology information system (RIS) [1] to exchange patient data (demographic and clinical information). An integrated setting, all-in-one operation,

depends critically on maintaining data integrity and continuous communication between the RIS and the PACS. It is crucial for PACS to comply with interoperability, complexity management, knowledge management, and safety of the information. Also, a disaster recovery plan must be implemented in order to minimize downtime, operator errors, and avoid loss of images, reports, and patient data.

Data security is a critical issue, not only when digital images and personal patient information are stored in a backup archive system but also during the transmission of these data through public networks. Media security refers to the protection of stored data, secure destruction of computer storage media, or media scanning for viruses. The robust privacy and security practices implemented in health information system (HIS), electronic medical record and RIS, have become increasingly relevant in patient care settings [3]. This protection must be characterized in terms of privacy, authenticity, and integrity of the data [4]. Privacy refers to the control of unauthorized access and use of disclosure of personal information. Authenticity means validating the source of a message, that is, a properly identified sender transmitted it. Integrity refers to the assurance that the data has not been modified accidentally or deliberately in transit, by replacement, insertion, or deletion [5].

Techniques of data protection—such as network firewalls, data encryption, data embedding including intrusion detection, public evasion [6, 7], or public-key cryptography system to create digital signature or watermarking [8]—have been designed to assure data security in terms of confidentiality, authenticity, and integrity. Although these techniques are commonly used in fields like the financial, banking, and military industry, they have not been systematically applied in medical imaging systems as PACS [9]. Digital image archives require a disaster recovery plan based on the institutional workflow and imaging volumes, as the metro-cluster failover design reported by Mansoori et al., with more robust duplication, much better uptime, and shorter scheduled upgrades [10]. Meanwhile, Qi Liang et al. (2012) presented an enhancement to the dynamic identity password-based authentication scheme proposed by Chen et al. It achieves user anonymity and intractability configuration, as well as mutual authentication between the user and the server, and can tolerate multiple attacks [11].

Despite the fact that these practices have been used in the last two decades, these methods have not been able to guarantee the image/data integrity during data transmission. Information security in healthcare systems must include not only the protection of patient information against unauthorized access use, modification, and disclosure but also fast recovery during system downtime and assurance of data integrity and patient privacy [12].

Three international organizations have issued guidelines, mandates, and standards for image/data security. The ACR/NEMA has defined DICOM standards for equipment specifications, quality improvement, licensure, staff credentialing, and liability. Part 15 of the DICOM standard (PS 3.15) specifies security profiles for communication and digital signature, and technical means for AEs [2]. The Health Insurance Portability and Accountability Act (HIPAA) [13]—the law 104-191 published in 1996—was officially instituted until 2003. It mandated healthcare providers to be HIPAA compliant by April 2005. The goal of HIPAA is to set and enforce the standards to protect patient privacy and security of health data. The third organization is the Society for Imaging Informatics in Medicine, which has issued a primer on security issues in digital medical enterprise.

A PACS security server (based on digital signed and enveloped for mammogram and MR images for HIPAA supporting information) was proposed to assure data integrity, authenticity, and confidentiality when image recovery cannot be confined within a private local area network (LAN) protected by a firewall [9]. The limitation of this solution is its slowness and intensive process demanding CPU (i.e., an image of digital mammogram is recovered in 40 s). There is a HIPAA compliant auditing system [14] generated for automatically monitoring the EMR's data flow and detecting unauthorized access that uses intrusion detection technology; however, this system is not specifically designed to be compatible with a particular PACS. Authorized DICOM digital signatures have been designed and implemented for electronic health record systems [15], but today, there are PACS, RIS, or inclusive HIS with no watermark or digital signature [8].

A few aspects of HIPAA security and DICOM compliance have been implemented in PACS but most lack audit mechanisms. Most PACS have not fulfilled the security specifications like DICOM supplement 41 or DICOM supplement 86 [2]. The paper presented by Oh et al. is amongst a few where watermarking technique was used as authenticity and integrity mechanism for medical images [16].

The rest of security measures, such as embedding auditing logs into information systems are as important as the safe storage and communication authentication. Effective security management for PACS that build confidence in interorganizational activities is still lacking. The ISO/IEC 2700 series refers to code of practice for ISM. It includes the ISO/IEC 27001:2013 standard, "established guidelines and general principles for initiating, implementing, maintaining, and improving information security management (ISM) within an organization" [17].

The National Institute of Rehabilitation (INR) is a medical research institution in Mexico City comprised of four units: orthopedic, rehabilitation, human

communication area, and burn center. Our PACS design started in 2004 and completed its integration throughout the hospital until 2008. INR actually provides more than 95,000 imaging studies (CT, computed tomography; MR, magnetic resonance; DR, digital radiology; CR, computer radiology; US, ultrasound; MN, medicine nuclear) annually, distributed from multiple central locations by means of an architecture that allows viewing the images anywhere (medical offices, emergency room, operating rooms, intensive care), anytime (24 h 365 days a year), and by any authorized user (as many as 245 concurrent users).

In this paper, we focus on implementing the Business Model for PACS Information Security (BMPIS) compliant with ISO/IEC 27002:2013 controls for auditing proposes. This proposal aims to ensure the integrity, privacy, and authenticity of the medical images on a highly available PACS based on the security criteria of DICOM and HIPAA standards. This model was implemented in the PACS-INR.

Method

Digital Image Security Process

According to systems theory, a system is an organized collection of parts (or subsystems) that are highly integrated to accomplish an overall goal. A system essentially consists of objects (physical or logical), attributes that describe the objects, relationships among the objects, and the environment in which the system is contained. The system has several inputs, which undergo certain processes to produce reliable outputs, which together accomplish the overall desired goal of the system.

In this context, mechanisms to maintain safe PACS transactions as well as the underlying infrastructure and information are outlined in the business model for the security of medical imaging information shown in Fig. 1. This model—based on systems theory—is part of the strategic plan for the ISM. The INR has established policies for information security that are compatible with the DICOM and HIPAA security/privacy requirements, procedures, and guidelines.

The security framework corresponds to 114 controls defined in ISO/IEC 27002:2013, part 15 of DICOM standard, privacy/security HIPAA regulations, and INR policies. The 114 ISO 27002:2013 controls are classified in four categories of services:

1. Policies and regulations of the organization
2. Authentication, which includes AE and user identification
3. Access control, which includes data confidentiality and privacy regulations
4. Data integrity, which includes asset management to prevent unauthorized disclosure, destruction, removal, or modification of information.

These four categories of services include three criteria; the first is the compliance with standards, the second are the indicators, and the third is the end-user perception, as described below.

I. Standard compliance

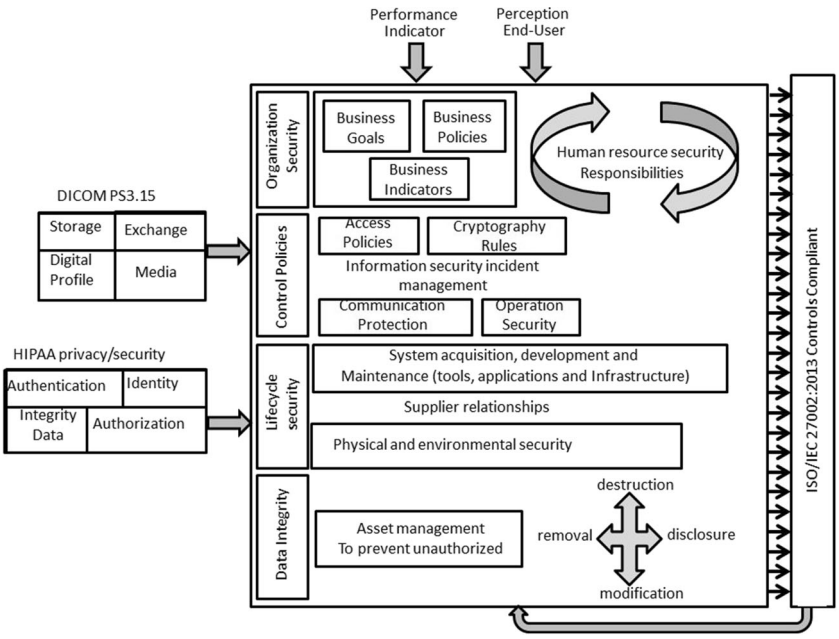

Fig. 1 Business Model for PACS Information Security (BMPIS) applied to PACS-INR, proposed to meet the ISO/IEC 27002:2013 controls

I.a This should be considered a security DICOM four profiles (PS 3.15 standard)

(1) Profile secure use, which includes online electronic storage

(2) Profile secure transport connection, which negotiates and establishes secure data exchange on the network

(3) Profile digital signature

(4) Profile media security

I.b HIPPA compliance

Privacy and security measures must include authentication, authorization, identity management, data integrity, and data securing both static and in transit.

II. Usage of security indicators

In the discipline of information security from the viewpoint of a comprehensive assessment, yet there are no standardized indicators for PACS. Indicators are proposed for each organization. In order to help getting the safety indicators, we identified four keys elements: privacy, integrity, authenticity, and availability.

III Perception by the end-user

Questionnaires and surveys focused on the perception about system security are developed and applied to the end-users.

Results

The PACS-INR is used to show the Business Model for PACS Information Security (BMPIS) proposed in this paper. This model considers three aspects; the first is the analysis of functionality of the system, the second includes standards and policies of the organization and, finally, the third refers to guidelines for implementation of security rules.

System Analysis (PACS-INR Functionality)

The PACS-INR platform is based on a three-tier architecture (implemented in Java platform). This architecture decouples the client tier, the application logic tier, and the data management tier. Liability and functions of each layer are described below:

Client Tier This layer contains all the medical imaging modalities (CT, MR, NM, DR, US) that need to be stored, queried, and retrieved in DICOM format. The DICOM medical image viewer is also part of this layer, which is an AE developed to display and process the medical images.

Business Logic Tier This layer is responsible for managing all transactions in DICOM format to support concurrent clients. Metadata that include patient data, study data, series data, and image data are extracted from DICOM images. Only the metadata and pointers to each image are stored into Oracle database. DICOM images are saved in file systems called direct attached storage (DAS), which is managed by DiskXtender EMC^2 component. VNX5300 EMC^2 device is used as DAS for the PACS-INR. The DICOM images are migrated to a container of fixed-storage called content addressed storage (CAS) to ensure security, availability, and integrity of information. Centera G4 EMC^2 device is used as CAS for the PACS-INR.

Data Management Tier This is the physical layer, which stores all DICOM images generated in the modalities mentioned above. The set of distributed components CAS/DAS EMC^2 technology is used to ensure data integrity during image lifecycle management. This technology provides fast access to fixed content and offers high availability online.

Figure 2 describes the overview of the PACS-INR architecture. StartUML (Open Source) was used to model the software architecture, including the layers (client tier, business, or application logic tier and data management tier) and the communication protocols (DICOM and DISKXTENDER).

Regulatory Compliance with Standards and Policies

As already mentioned above, data security and continuous access are critical issues that must be characterized in terms of availability, privacy, authenticity, and integrity of the data. Table 1 describes the security and privacy ISO/IEC 27002:2003 controls, while Tables 2, 3, and 4 show DICOM and HIPAA security requirements as well as the organization policies for the PACS-INR.

The Information Security Management (ISM) for a medical imaging systems (PACS) must include not only the protection of patient information against unauthorized disclosure, modification, and holdback but also guarantee timely access during consultation, fast recovery during downtime of the system, and the assurance of data integrity and privacy of the patient.

Popular commercial PACS use common Information Technology (IT) controls, or proprietary technology;

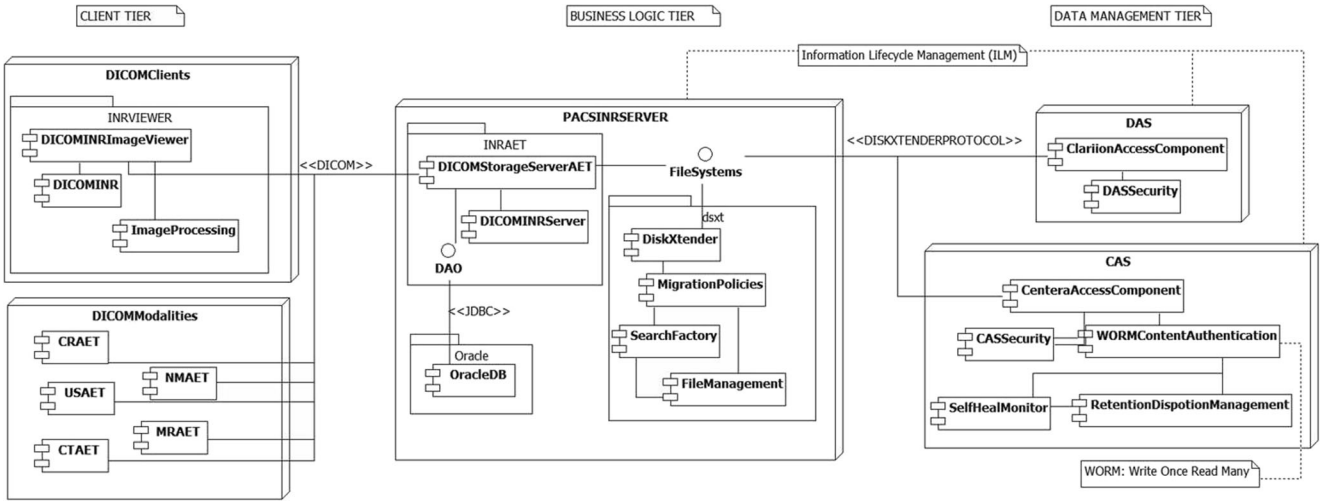

Fig. 2 Overview of the PACS-INR architecture using starUML. The client layer includes DICOM viewer as modalities (DR, US, CT, MR, NM). PACS server integrates the application logic tier, and the last layer is the physical container of the DICOM images

some of the most used are shown in Table 5. All regulatory conditions, standard requirements, and IT controls are interrelated to protect the information, as shown in Fig. 3.

Table 6 shows the comparison of security management, standard compliant, and disaster recovery tools among PACS in production, all of them are based on DICOM standard and IT.

Table 1 Reference control objectives and controls of ISO/IEC 27002:2013 [17]

Category	Control	Objective
Policies and regulations of the organization	5. Information security policies	Direction accordance with business requirements, laws, and regulations.
	6. Organization of information security	To control the implementation and operation of information security.
	7. Human resource security	To protect the organization's interests ensuring that employees are aware of their information security responsibilities.
Privacy	8. Asset management	To ensure that information has an appropriate level of protection. To prevent unauthorized disclosure, modification, removal, or destruction of information stored on media.
	9. Access control	To ensure authorized user access for safeguarding their authentication information.
Integrity	10. Cryptography	To protect the confidentiality, authenticity, and/or integrity of information.
	11. Physical and environmental security	To prevent loss, damage, theft, or compromise of assets and interruption to the organization's operations.
	12. Operations security	To ensure correct and secure operations of information processing facilities and to protect against loss of data.
	13. Communications security	To ensure the protection of information transferred in networks and its supporting information processing facilities.
	14. System acquisition, development, and maintenance	To ensure that information security is designed and implemented across the entire lifecycle of information systems.
	15. Supplier relationships	To ensure protection of information that is accessible by suppliers.
Authenticity	16. Information security incident management	To ensure a consistent and effective approach to the management of information security incidents, including communication on security events and weaknesses.
Policies and regulations of the organization	17. Information security aspects of business continuity management	Continuity in information security management should be integrated into the master plan of the organization.

Table 2 HIPAA control codes used for compliance with ISO/IEC 27002:2013 [17]

Control code	Security issue	Implementation
HIPAA-1	Authenticity	PACS-INR will be analyzed to implement the single sign-on (SSO) for authentication. Users may be able to access multiple applications after validating their signature the first time
HIPAA-2	Privacy	PACS-INR supports OAuth for authorization, which is an open standard that allows resource owners to share their private resources stored on one site with another site without handing out the credentials
HIPAA-3	Privacy	PACS-INR will use federated identity management (FidM), identifying persons and maintaining associated identity attributes for the users across multiple organizations
HIPAA-4	Integrity	PACS-INR adopts 256-bit Advanced Encryption Standard (AES-256), which is a data encryption standard e stablished by NIST. All data/image are first encrypted using AES-256 standard
HIPAA-5	Integrity	All transmission of data is protected with HTTP over secure socket layer encryption technology
HIPAA-6	Integrity	PACS-INR will adopt a key patient dynamic management changing the key patient with a configured frequency. Also, all the keys are encrypted and stored in a remote data storage, which is separate and distinct from the actual data store
HIPAA-7	Authenticity	PACS-INR will use message authentication codes (MAC) to detect both accidental and deliberate modifications in the data. Computation of MAC involves the use of a secret key that is known only to the party that generates the MAC and the intended recipient and the data on which the MAC is computed

Guidelines for Implementing the Security Rules in the PACS-INR According to the ISO/IEC 27002:2013 Standard

Indicators

An integrated setting, all-in-one operation, depends critically on maintaining data integrity and continuous access. In this context, eight indicators are proposed for evaluating the security and availability of medical images in the PACS-INR. Each of these indicators has one or more associated items related to ISO/IEC 27002:2013 standard controls. The names, definition, and measure are shown in Table 5.

End-user perception is as important as the security of the media. The organization shall propose mechanisms to assess user confidence (radiologist and physician) in the system; i.e., access time for consultation, quality of the image, recovery during system downtime, and right image for the right patient. To do this, we implemented surveys to detect anomalies, misidentifications, or even lack of training and usability guidelines.

Table 3 DICOM control codes used for compliance with ISO/IEC 27002:2013 [17]

Control code	Security issue	Implementation
DICOM-1	Authenticity	Secure use profiles include online electronic storage
DICOM-2	Integrity	Secure transport connection profiles to negotiate and establish the secure data exchange over a network
DICOM-3	Privacy	Digital signature profiles
DICOM-4	Integrity	Media security profiles

Physicians were asked to complete a brief and anonymous questionnaire that examined their awareness of the flow of the patient medical imaging information, as well as their perceptions of privacy and trust in relation to how their information is managed.

The PACS must always be monitored in real time to ensure high levels of security for confidential enterprise assets and to take measures to detect anomalies, attacks, and other vulnerabilities that can cause harm to the information. Weekly monitoring of continuous operation of the PACS-INR is performed to detect downtime events.

Business Process Model and Notation (BPMN)

Besides techniques, rules and plans of data protection; indicators should be integrated into the ongoing ISM of the organization (Table 7). For this, purpose, a strategy workflow based on BPMN [18] methodology was implemented.

Table 4 INR control codes used for compliance with ISO/IEC 27002:2013 [17] for

Control code	Security issue	Implementation
INR-1	Privacy	Access controls policies, including user profiles
INR-2	Integrity	Preventive, detective, and corrective controls are implemented to prevent a hazard event, identify an incident in progress, or limit any damage
INR-3	Availability	Medical images available online, medium-term, and long-term storage
INR-4	Availability	Downtime controls are implemented to prevent disruptions due to power outages, hardware failures, and system upgrades.

Table 5 Informatics technology controls used in popular commercial PACS products

Control code	Security issue	Implementation
IT-1	Authenticity	IIS (Microsoft Internet Information Services) [21] for FTP, SMTP, HTTP, HTTPS services
IT-2	Integrity	AON (Access Over Network) ensures the reliability when images compression is performed [21]
IT-3	Privacy	PCI/DSS (payment card industry/data security standard), requirement 3.4, relates to the encryption and key management user [22]
IT-4	Integrity	EMC^2-RSA (EMC^2—propietary technology) information management platform for alert against baseline anomalies, alert on unusual privileged user activity, maintain digital chain of custody with unaltered log data for data retention and forensic requirements [23]
IT-5	Availability	HSM (Hierarchical Storage Manager—proprietary technology) is used for image archival, copies, and backups to multiple tiers of storage and creates a redundant archive copy for complete archive backup and disaster recovery [21]

Figure 4 shows a multi-level view (using BizAgi [19] Process Modeler software—Open Source) of the systems involved in the digital image security process (DISP) at INR and how they interact with each other.

Desktop Support

Desktop support is implemented to provide attention to end-user reports and, thus, track and document incidents related to imaging studies access in PACS-INR. The software OsTicket (Open Source) was used to allow auto-generation of a unique identification code (report code) that sends an automatic response to the user, including self-help for FAQs, provides alerts, notices, and record of incidents. In Fig. 5, the mechanism of self-reported using OsTicket is shown.

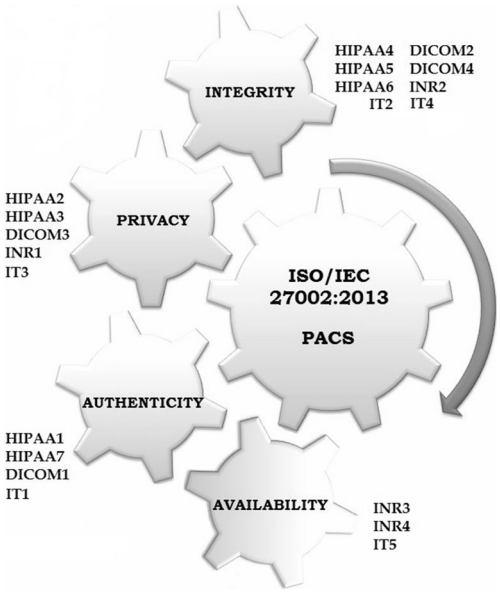

Fig. 3 Scheme of interrelationship between integrity, privacy, authenticity, and availability of data in a PACS; supported over ISO/IEC 27002:2013 controls, in compliance with DICOM/HIPAA standards, IT controls, and INR policies

Discussion

PACS security checks that conform to the ISO/IEC 27002:2013 standard depend on mechanisms to authenticate users and maintain the integrity and privacy of the image and also of the policies and regulations of the organization. User authorization can be controlled through strong passwords conveying a high degree of safety for the protection of information, while several factors such as physical access restrictions, security schemes in storage technology, and transmission systems by controlled network help maintain the integrity and privacy of medical imaging.

HIPAA requirements (authenticity, data integrity, access control, identity) help protect patient privacy and medical image security. Similarly, security profiles, according part 15 of DICOM, define a framework for the protection of DICOM files for media interchange by means of an encapsulation with a cryptographic envelope.

One cannot just implement the image security using HIPAA and DICOM and assume that PACS system is secure. These standards do not include image data security rules before or after the transition. It is crucial to follow the digital image security process (DISP).

The ISO/IEC 27002:2013 standard includes not only security access controls and data integrity via hardware and software but also the policies and regulations of the organization (see Table 1). This standard does not require that all controls must be implemented. Each organization can select those necessary to maintain system security.

The Business Model for PACS Information Security (BMPIS) presented in this paper includes an ISM to keep track of access to information through the identification of the person that accessed the data, the date and time when data was accessed, the type of access (create, read, modify, delete), the access status (success or failure), and the identification of the data.

PACS-INR is a large-scale system that runs in a private LAN; it is DICOM and HIPAA compliant. It provides a security framework and data redundancy for real-time backup

Table 6 Comparison of security management among different PACS products

Brand	Product	Security management	Standard compliant	Disaster recovery tools
INR	PACS-INR	EMC^2-WORM (Write Once Read Many), AEs encryption	DICOM, HTTPS, HIPAA	EMC^2-Redundant Array of Independent Nodes—RAIN [23]
General Electric	Centricity PACS-IW	EMC^2-RSA in Vision [23]	DICOM, HIPAA, PCI DSS [22]	EMC^2 Recover Point/Cluster Enabler (CE) and VMware
AGFA	IMPAX	ISMS—information security management system [24]	DICOM, HIMSS, MDS2 ISO 27001 certified	NA
Philips	IntelliSpace PACS	IntelliSpace iVault [25]	DICOM, HIPAA	Philips' Disaster Recovery Data Centers
Siemens	Syngo	ISA—Siemens healthcare's image sharing and archiving service [26]	DICOM, HIPAA	NA
Fuji	Synapse	NA	DICOM, HTTP	HSM—Hierarchical Storage Manager [21]

of the information contained in the storage system (CAS/DAS EMC^2 architecture) with two linked servers located in two distant places (more than 100 m). This storage system had a disaster and data protection solution that operated in a failover support mode: the fault-tolerant PACS-INR server [20].

At present, a secure transport of image, allows the PACS-INR negotiates and establish secure data exchange between AEs through a private LAN. A controlled password is used to authorize access and retrieval of image by the end-user (physician and technician). The data storage unified architecture along with EMC^2 storage technology offers the capability for data protection—Write Once Read Many (WORM)—using the encryption algorithm (future-proof HMAC-SHA-512 bit hashes) to safeguard DICOM files for media exchange via an encapsulation method [20].

We perform a weekly monitoring of hardware and software to prevent loss, damage, or, even worse, data modification. In addition, we have implemented a disaster recovery plan for the PACS-INR in order to minimize downtime, misidentification of image/patient, operator errors, and loss of images.

Table 7 Data protection, information privacy, and security indicators for PACS-INR

Indicator	Definition	Measure
Accessibility	Information, system, and components must be accessed only for identifiable, known, and authorized users by password that meets policies and standard	Percentage (%) of components (remote access points and servers) with password
Safety storage	Restricted data must be encrypted using strong, public cryptographic algorithms, in such a way as to make images unreadable by anyone except those possessing special key	(Number of storages components with cryptography algorithm/total number of storage components of PACS)∗100
Identification and authentication	All users and medical imaging equipment are validated in accordance with information security policy	(Number of valid transactions/total number of transactions)∗100
Vulnerability	To document, track, and report an adverse event in the PACS, network, and visualization workstation	(Number of incidents reported on time/total number of reported incidents)∗100
Reliability	To verify that the image is not changed during transfer	(Number of misidentified images/total number of images)∗100
Contingency	Establish, maintain, and implement redundancy backup to ensure the availability and protection of information (images)	(Number of redundancy backup working/number of redundancy backup implemented)∗100
Continuity	Determining tolerable downtime and idle time	(Total time – down time)/total time
Timeliness	The response time—how quickly a system is able to provide users with the output they require	The length of time between submission of an input transaction to the system and receipt of the first character of the output

The evaluation period is weekly

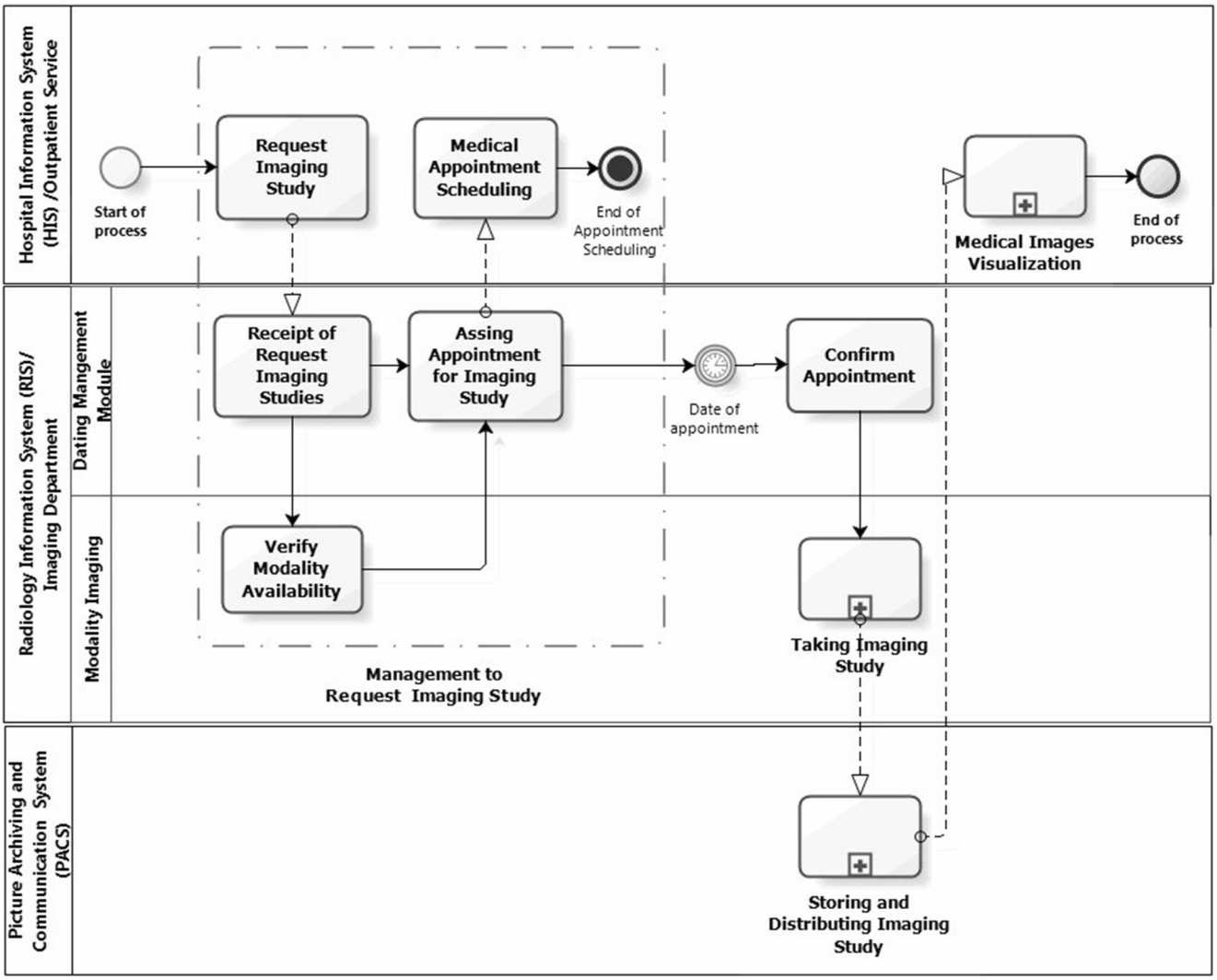

Fig. 4 Digital image security process using BPMN (generated by Norma Navor)

A PACS committee has been formed to ensure and follow the quality of the digital imaging security process, for maintaining data security, interoperability with RIS and HIS, and disaster recovery plan. The INR's head, biomedical engineers, physicians, and informatics staff compose this committee. This team is responsible for determining criteria controls, defining access policies based on user profile, liability of the actors (designer, architect, and physician), classification of information, records of incidents, updates, and storage policies.

Currently, we have established the methodology for implementing the controls of ISO/IEC 27002:2013 for PACS-INR. We defined security policies for system and users, the responsibilities of each authorized person, verification mechanisms to protect confidentiality, authenticity, and integrity of information through indicators along its life cycle.

In the future, the PACS-INR will be used outside the institution; therefore, the mechanisms of authenticity and integrity of the data together with control unauthorized access by firewall will be implemented to provide web or teleradiology services.

Conclusion

Many of the DICOM/HIPAA controls described in this paper have not been implemented in popular commercial PACS products yet. While information technology provides useful tools for the protection of information, technology itself is not the solution.

To protect medical information, the national health services and hospitals need to establish PACS that are compatible not only with DICOM/HIPAA requirements but also with IT controls, standards, procedures, and guidelines. The controls listed in the tables describe in this paper are declarative in manner but in no way limited; each organization sets its own policies and regulations.

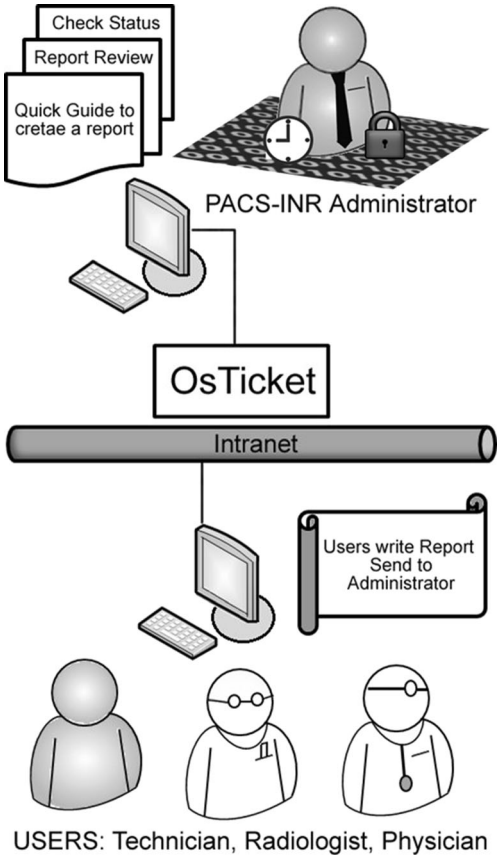

Fig. 5 Mechanism of self-reported of incidents using OsTicket

The exact role of an ISM is not yet clearly defined in many organizations. ISO/IEC 27002:2013 controls that comply with HIPAA and DICOM standards can be used to help ensure the safety and integrity of medical images. It is also essential that a workflow analysis for digital imaging security process be done. Actual PACS implementations that fulfill the BMPIS requirements for audit purposes are still lacking.

The implementation of the Business Model for PACS Information Security (BMPIS) based on ISO/IEC 27002:2013 and DICOM/HIPAA standards is to

1. Reducing risk—using a structured methodology and globally recognized information that identifies and mitigates the threats.
2. Protecting confidential information—for threats such as loss of data and violation of privacy, and thus recover more quickly from such attacks. It is also for the detection of authorized users who misuse their privileges (like navigating through all records of patients) and intruders trying to enter to system with malicious intentions.
3. Preventing harm to the patient—detecting corrupted and unreadable data, leading to errors that endanger patient safety or decrease the quality of care. These unintended consequences also may impact on patient health and can have serious legal implications.
4. Implementing business continuity plans—to ensure that its operations are not interrupted in the event of natural or man-made disasters.

This methodology can generate HIPAA and DICOM compliant audit scheme of image data access for a specific patient on demand. It can also monitor the data flow of PACS facilitating the detection of unauthorized image access and other abnormal activities.

Regulatory compliance standards and policies such as ISO/IEC27002:2013, HIPAA, and DICOM is one of the greatest challenges faced by hospitals for establishing security processes in information systems such as PACS.

References

1. Huang, HK: PACS and Imaging Informatics. Basic Principles and Applications, New Jersey: Wiley Blackwell 2nd Edition, 2010
2. Pianykh, O: Digital Imaging and Communications in Medicine (DICOM) Cap 11. DICOM Media and Security, Springer 2nd Edition, 2012
3. Fernando J, Dawson L: The health information system security threat lifecycle: An informatics theory. Int J Med Inform 78:815–826, 2009
4. Lim, E: Data Security and Protection for Medical Images In: Biomedical Information Technology by Dagan Feng, Elsevier, 2008
5. Mouraditis H, Giorgini H, Manson G: Integrating Security and 85 Systems Engineering: Towards the modeling of secure information systems. Lect Notes Comput Sci. Adv Inform Syst Eng 2681:63–78, 2003
6. Alotaibi Y, Fei L: A novel framework to model a secure information systems. Int Conference Inf Comput Appl 24:84–89, 2012
7. Jadidoleslamy H: Weakness, vulnerabilities and elusion strategies against intrusion detection systems. Int J Comput Science & Engineering Survey 3(4):15–25, 2012
8. Farhadi A, Ahmadi M: The Information Security Needs in Radiological Information Systems—an Insight on State Hospitals of Iran, 2012 J Digit Imaging 26:1040–1044, 2013
9. Cao F, Huang HK, Zhou XQ: Medical image security in a HIPAA mandated PACS environment. Comput Med Imag Grap 27(2–3): 185–96, 2003
10. Mansoori B, Rosipko B, Erhard K, Sunshine J: Design and Implementation of Disaster Recovery and Business Continuity Solution for Radiology PACS. J Digit Imaging 27:19–25, 2014
11. Liang Q, Ma J, Ma Z, Li G: A Privacy Enhanced Authentication Scheme for Telecare Medical Information Systems. J Med Syst 37: 9897, 2013
12. Krens, R, Spruit, M, Urbanus, N: Evaluating Information Security Effectiveness with Health Professionals, Springer, 2013
13. Guidance on Risk Analysis Requirements under the HIPAA Security Rule. Available at http://www.hhs.gov/ocr/privacy/hipaa/administrative/securityrule/rafinalguidancepdf.pdf. Accessed 27 January 2015
14. Zhou Z, Liu B: HIPAA compliant auditing system for medical images. Comput Med Imag Grap 29:235–241, 2005
15. Lien CY, Yang TL, Hsiao CH, Kao T: Realizing Digital Signatures for Medical Imaging and Reporting in a PACS Environment. J Med Syst 37:9924, 2013

16. Oh G, Lee YB, Yeom S: Security Mechanism for Medical Image Information on PACS Using Invisible Watermark. Lect Notes Comput Sci 3402:315–324, 2005
17. ISO/IEC 27002:2013 Control objectives and controls IN: International Standard ISO/IEC27001:2013 Information technology - Security techniques - Information security management systems – Requirements. Second Edition 2013-10-01.
18. Allweyer T. BPMN 2.0 Introduction to the Standard for Business Process Modeling. Urheberrechtlich geschütztes Material 2nd Edition 2010.
19. BizAgi Process Modeler V.1.5.0.1. Available at http://www.bizagi.com. Accessed 20 January 2014.
20. Gutiérrez J, Núñez MA, Aguirre H, Delgado R: A software and hardware Architecture for a High-Availability PACS. J Digit Imaging 25(4):471–9, 2012
21. Fujifilm Medical Systems Synapse (Product Data). Available at http://www.fujifilmusa.com/shared/bin/server-interface.pdf. Accessed 20 October 2014.
22. Payment Card Industry Data Security Standard (PCI DSS). Available at https://www.pcisecuritystandards.org/documents/pci_dss_pa_dss_Feedback_Summary.pdf. Accessed 20 October 2014.
23. The EMC^2 Business Continuity Solution For GE HealthCare Centricity PACS-IW. Available at http://www.emc.com/collateral/software/solution-overview/h8680-ge-pacs.pdf. Accessed 20 October 2014.
24. Agfa HealthCare Global Policy (Information Security and Privacy). Available at http://www.agfahealthcare.com/he/global/en/binaries/Global_Policy-Information_ Security_and_Privacy_tcm541-91738.pdf. Accessed 20 October 2014.
25. IntelliSpace PACS iVault 4.4. Available at http://www.healthcare.philips.com/ main/products/healthcare_informatics/products/enterprise_imaging_informatics/isite_pacs/ivault/. Accessed 20 October 2014.
26. Image Sharing & Archiving. Available at http://usa.healthcare.siemens.com/ siemens_hwem-hwem_ssxa_websites-context-root/wcm/idc/groups/public/@us/@ healthit/documents/download/mdaw/mzi2/~edisp/final-isa_flyer-032012-00284737.pdf Accessed 20 October 2014.