We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

6,900
Open access books available

186,000
International authors and editors

200M
Downloads

Our authors are among the

154
Countries delivered to

TOP 1%
most cited scientists

12.2%
Contributors from top 500 universities

WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com

5

Current Trends in Archiving and Transmission of Medical Images

Luís S. Ribeiro, Carlos Costa and José Luís Oliveira
Universidade de Aveiro, IEETA
Portugal

1. Introduction

The traditional Picture Archiving and Communication System (PACS) model consists of one PACS serving one healthcare institution (i.e. hospital-centered). Typically, a healthcare institution does not possess all the modalities or experts to evaluate a patient. Therefore, patients tend to move across several healthcare institutions to undergo all the required exams or diagnosis. These high levels of patient mobility produce huge amounts of medical data spread among different healthcare institutions without being shared conveniently, making the traditional PACS model obsolete. The current solutions for sharing non-anonymous medical images (i.e. HIPAA's Protected Health Information - PHI) rely mainly on point-to-point trust relationships (e.g. the radiologist trusts the physician sending image reports by e-mail) or ad-hoc solutions between few institutions (Jacq, 2007). The main problem of the ad-hoc solutions is interoperability, caused by the heterogeneity of methods to exchange information. To overcome this and other issues, the health industry, research and professionals around the world joined forces and started an initiative entitled Integrating the Health Enterprise [1] (IHE) with the main purpose of defining which standards (e.g. DICOM, HL7, ISO, OASIS, etc) may be used in a given situation of the healthcare workflow. IHE does not design standards, but defines integration profiles, i.e. blueprints that describe real-world scenarios or specific characteristics for building integration-ready systems (Størkson & Aslaksen, 2009). Among several integration profiles, one stands out: the Cross-Enterprise Document Sharing (XDS). XDS is gaining momentum and nowadays there are several implementations working in the field. XDS for imaging (XDS-I) is a content profile based on XDS that takes into consideration the particularities of the medical imaging field. However, XDS or XDS-I assume that their architectural components are located inside trustworthy domains, i.e. owned and maintained by Healthcare institutions. Planning and maintaining the IT infrastructure required to support the XDS-I architecture is not simple and demands a significant human and financial effort. Therefore, it would be desirable to delegate this task to a third-party entity and pay for it as a service. For instance, delegating the IT infrastructure to a Cloud Computing provider where the healthcare institutions would just pay to use the data-sharing service and not for the entire IT infrastructure required to support XDS.

Cloud is a computing paradigm that intends to deliver computation and data storage as a utility service (Faruqui, 2005; Michael Armbrust, 2009; Rajkumar Buyya, 2009). A utility

[1] http://www.ihe.org

service in the Cloud follows the same approach as a utility service in currently established utility facilities (e.g. electricity, gas, or telecommunications). Utility services are accessed so frequently that they need to be available anywhere and whenever the consumer requires them. This approach brings obvious advantages since consumers no longer need to plan, invest heavily at the outset or maintain a complex IT infrastructure.

However, combining the concepts of PACS/XDS-I and Cloud computing raises other problems, mainly regarding protection of the patient's private information from unauthorized entities. In this chapter we intend to: (i) - describe the XDS-I and Cloud computing; (ii) - highlight the challenges and opportunities of combining these two concepts; (iii) - present several complementary solutions allowing discussion of whether the benefits of outsourcing the XDS infrastructure on Cloud are worth the associated risk.

2. Background

Medical imaging is a non-invasive technique used to create internal images of the human body for clinical or medical science purposes (i.e. "virtual dissecting" of the human body). The genesis of medical imaging occurred in the final decade of the 19th century (1895), when Professor Wilhelm Roentgen noticed electromagnetic radiation while performing vacuum tube experiments. Not understanding the plenitude of that radiation he decided to call it x-rays (Roentgen, 1898). After these first steps, radiology evolved at a good rate until World War II. The intense use of x-rays during the Second World War, and the arrival of the digital computer and new modalities such as ultrasound and magnetic resonance have triggered a boom in diagnostic imaging techniques in the past years (Hendee & Ritenour, 2002). Digital imaging techniques have been in use since the 1970s after the clinical acceptance of Computer Tomography (CT scanner). Currently, digital medical imaging technology is globally acknowledged and an important part of the healthcare workflow.

2.1 Current medical imaging scenario

Nowadays, the importance of medical imaging in the healthcare system is irrefutable. To physicians it represents a key factor in supporting their clinical thesis and, as a result, delivering high quality healthcare decisions. Images and studies are stored in local repositories following a PACS concept (Huang, 2010). PACS embraces a set of technologies for the archiving, distribution, visualization and acquisition of medical images over a computer network. Compared with the traditional analogue film, the PACS concept brings significant benefits for the productivity, economy and management of a healthcare institution (De Backer et al., 2004; Huang, 2010; Langer, 2009). At the present time, PACS is a widespread concept in the majority of medical centers. This acceptance was encouraged by introduction of the DICOM, a standard for handling, storing, printing and transmitting medical images. It includes data format definition, storage organization and a network communication protocol (Costa et al., 2007; Mustra et al., 2008; Pianykh, 2008). In this way, PACS devices from different vendors are able to interact with each other in a transparent manner. The PACS architecture began mainly on an ad-hoc basis, serving small subsets, called modules, of the radiology department. Each module functioned as an independent island, unable to communicate with other modules (Huang, 2010). Later it evolved into a PACS infrastructure solution, integrating the hospital information system and the radiology information system, serving the entire hospital (figure 1). The core element of a PACS is one (or more) archive that holds all the DICOM images and studies. Although the various PACS archives that serve

the institution are typically accessible within the institution, they tend to be independent from each other. This may be useful to create federations of clinical specialities within the institution, but if a workstation needs to access the full picture of one patient it has to query archive by archive. Furthermore, when the central PACS archive of the healthcare institution or department deteriorates (e.g. not capable of delivering an acceptable Quality of Service), the institution typically replaces it with a more powerful machine (scales up) or appends a new and independent PACS archive, bringing problems regarding data migration and lack of a unified view within the archive of the same department. If inside the healthcare institution such problems still persist, the magnitude and complexity of the problem amplifies when we reach the inter-institutional document-sharing level. Medical imaging exchange among different institutions and e-health in general poses a range of legal and ethical challenges, such as ownership, confidentiality, privacy and integrity of medical data or licensure, accreditation and liability of the health professional or institutions. Legal issues have been a major barrier to inter-institutional medical imaging exchange (Pattynama, 2010). The transmission of PHI across different institutions is not just transferring data from one spot to another. A major problem regarding inter-institutional cooperation is the trust establishment (Lovis et al., 2007; Ruotsalainen, 2009). Due to the rigid laws regarding data privacy and security protection, institutions are reluctant to exchange sensitive data such as non-anonymous medical images. Compromising sensitive data is a present risk when data leaves the institution walls because the institution that controls the data (data controller) may be accountable for any malpractice performed on it, even if the data is sent to other institutions and the malpractices were performed there (Mora et al., 2008). This scenario leads to institutional closure and prevents inter-institutional cooperation due to the lack of trust in third party institutions. Therefore, in order for a group of healthcare institutions to cooperate and share clinical data they must trust each other in the first place. Moreover, besides trusting each other, they must trust in the IT infrastructure that supports the medical imaging cross-transmission.

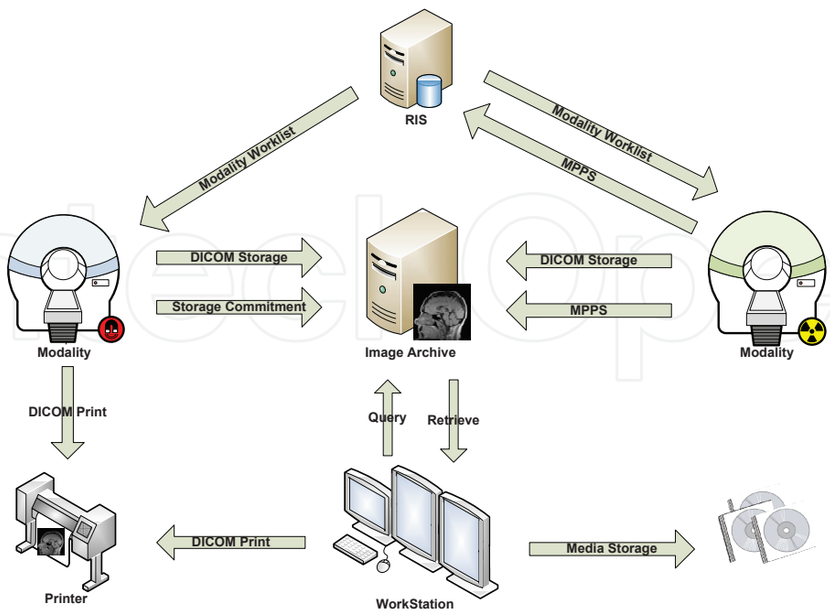


Fig. 1. PACS traditional workflow.

2.2 Integrating the healthcare enterprise

As mentioned before, DICOM supports interoperability inside the healthcare institution, but inter-site interoperability is a different situation. Ideally, an authorized entity would have access to the entire clinical history of the patient, relevant for one specific episode, whether or not the exams were performed by the institution. IHE aims to make this possible by improving system integration and eliminating barriers to achieving optimal patient care. IHE provides integration profiles, every one composed of several actors and transactions. The IHE actors and transactions are abstractions of the real-world healthcare information system environment. While some of the transactions are traditionally performed by specific product categories (e.g. HIS, Electronic Patient Record, RIS, PACS, Clinical Information Systems or imaging modalities), IHE intentionally avoids associating functions or actors with such product categories. For each actor, the IHE defines only those functions associated with integrating information systems. The IHE definition of an actor should therefore not be taken as the complete definition of any product that might implement it, nor should the framework itself be taken to comprehensively describe the architecture of a healthcare information system. The reason for defining actors and transactions is to provide a basis for defining the interactions among functional components of the healthcare information system environment (IHE, 2006a).

2.2.1 Cross-Enterprise Document Sharing for imaging

Cross-Enterprise Document Sharing (XDS) is IHE's integration profile that provides core guidelines for sharing documents among any healthcare institution, more precisely it supports: querying, retrieving, publishing and registering Electronic Health Records (EHR) documents. However, XDS is content neutral this means that its architecture was designed to support any type of EHR document. This document independence allows XDS to be a generic framework and more resilient to the appearance of future document standards or formats. In the other hand, being so generic could raise challenges dealing with more specialized domains (e.g. radiology, cardiology). Therefore, it is possible to extend the XDS integration profile and create more specific profiles, entitled content profiles. XDS for Imaging (XDS-I) is a content profile scoped to the medical imaging domain, where systems like PACS, RIS or DICOM objects are taken into account on the XDS architecture.

XDS-I profile facilitates the registration, distribution and access of medical images and imaging related documents across multiple healthcare institutions. Its focus is to provide a standard-based specification for managing the sharing of documents between any healthcare provider, ranging from a small physician office to a metropolitan Hospital (IHE, 2006a; 2008). XDS-I may be seen as a content profile of the integration profile XDS specialized in the radiology domain. Like XDS, XDS-I is document type independent however XDS-I takes in consideration some radiology particularities such as the integration of PACS and RIS in the conceptual architecture.

XDS, and as a consequence XDS-I, assumes that the healthcare institutions belong to one, or more, XDS Affinity Domains (XAD). XAD is a community of healthcare providers that agreed to cooperate using a common set of policies, share a common infrastructure of repositories and a common document registry. Inside an Affinity Domain policies must be defined, such as patient identification (e.g. using IHE Patient Identifier Cross-Reference - PIX), control of access, security model, as well as the format, content, structure, organization and

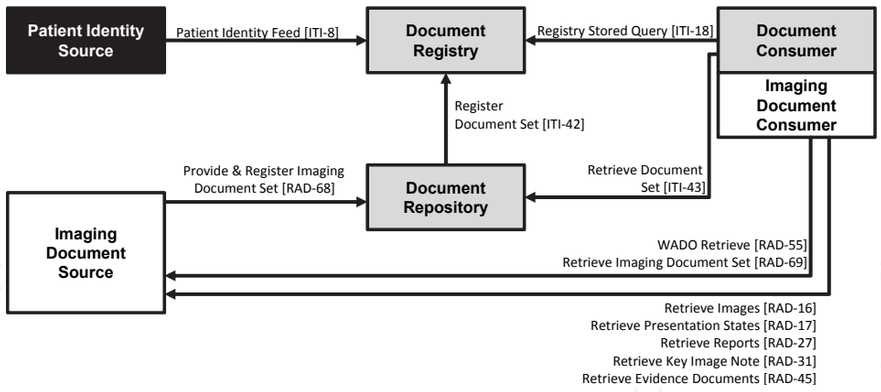


Fig. 2. Diagram of the XDS-I content profile with respective actors and main transactions.

representation of the clinical information (IHE, 2006b). Although XAD is a trust community and authorized participants may access the documents, the healthcare provider that produces the documents may select which documents are to be shared and which are just for internal use.

As mentioned before, the IHE actors communicate through well defined IHE Transactions. These Transactions are based on ebXML messages developed by the OASIS standards [2]. So, the exchanged XDS documents are wrapped in ebXML. The receiving actor by analyzing the message will know what type of information the message contains and who the sender entity was. Figure 2 shows the actors taking part in the XDS-I profile and the transactions between the actors. The Imaging Document Source is the actor that provides or holds the clinical documents (e.g. PACS) typically within the healthcare institutions. It is responsible for pushing the documents and its metadata to the respective Document Repository. If the document is a DICOM object the Repository will only hold the DICOM Key Object Selection (KOS). The KOS objects are small DICOM objects containing a list of UID references (instead of the image data itself) in order to the Document consumer retrieve the images from the Imaging Document Sources. Besides being responsible for the persistent storing of the documents, the Document Repository actor is also responsible for registering the document's metadata in the appropriate Document Registry. The Document Registry actor is the central player of the entire XDS Affinity Domain. It maintains the metadata of each registered document and its mapping to the respective Document Repository, where the actual document is stored. Furthermore, the Document Registry responds to queries from the Document Consumer actor with the locations of the matching documents. Moreover, the Document Consumer actor queries the Document Registry to find the location and the identifier of the document. With this information, it contacts the respective Imaging Document Source (or Sources) requesting the access to the respective image (or images). If the Imaging Document Source authorizes the access, the set of images are typically retrieved through the WADO retrieve protocol - a sub-protocol of the DICOM standard. Finally, Patient Identity Source from the PIX integration profile, and not from XDS, is the actor that provides a unique patient identifier within the Affinity Domain.

[2] http://www.oasis-open.org

Usage example

Figure 3 illustrates a real world application of the XDS-I approach on the inter-institutional cooperation within an Affinity Domain. At this example, the XAD is composed by a shared document registry and each institution owns a document repository and an imaging document source within its walls. This example highlights possible interactions between professionals, institutions and patients in an inter-institutional clinical episode enabled by the XDS-I content profile:

- **Physician Office:** A referring physician, working in a private office, orders one examination and the patient goes to the Imaging Acquisition Center to perform the exam.
- **Imaging Acquisition Center:** An imagiology institution with modality equipment and a RIS/PACS to manage report and imaging information. The healthcare professional queries the Document Registry for previous studies relevant to this clinical episode. Then, the images studies (acquisition and report) are preformed and, finally, the new documents are registered on the Document Registry.
- **Diagnostic Center:** Eventually, the private physician determines that a consult with a specialized physician is required after analyzing the new exams. At the healthcare institution with specialized physicians (e.g. oncologist) the physician queries the document registry and fetches, from the distributed document repositories, all the needed documents. It performs the evaluation reports of the clinical episode and, finally, registries the documents on the Document registry of the Affinity Domain.
- **XDS Document Registry:** The Document Registry it is the heart of the affinity domain. It is this entity that enables the lookup of documents by indexing the documents' metadata.

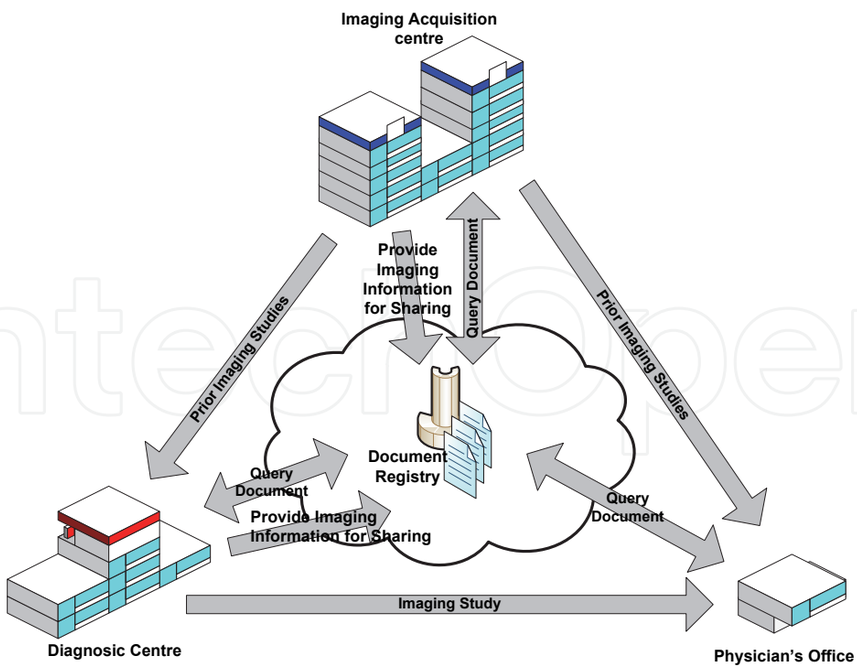


Fig. 3. Data flow within an XDS-I Affinity Domain for a clinical consult.

2.2.2 Cross-community access for imaging

In the last section, the reader learned how XDS enables the creation of trust communities for document sharing. However, the scenario of a unified cluster of healthcare institutions sharing documents is not always possible. As mentioned before, the participants of a XAD have to agree a priori to several matters that might slow down the creation of XAD or even make it impossible. For instance, XDS assumes that the patient identifiers are globally unique inside the XAD. However, each institution has their own patient identifiers and the effort of merging, or mapping, the identifiers into a master patient identifier can be great and, as a consequence, jeopardize the project. Whether for technical or conjectural reasons it is certain that patients will flow across several XADs or independent care communities. Therefore, having a way to access documents from outside the community is a desirable feature. Foreseeing this scenario, IHE proposed the Cross Community Access (XCA) integration profile that enables independent communities to exchange documents.

The Cross-Community Access (XCA) integration profile was designed to complement XDS. If XDS creates islands of institutions and XCA creates bridges between those islands. In other words, XDS provides the blueprints for building concise domains of document sharing. While on the other hand, XCA defines a way for extra-domain entities to access the documents shared within the community.

Although XCA does not specify that communities must be XDS Affinity Domains, the reality is that its design makes it the natural choice to connect XDS Affinity Domains. However, the actions allowed to an entity using XCA are not the same as if the entity belonged to the XAD. XCA only allows search and retrieval of documents among communities and does not support pushing or registering of documents inside those communities.

2.3 Cloud computing

Cloud computing is a new buzz word for an old dream of computing as a utility, more precisely the 5th utility after water, electricity, gas and telecommunications. Cloud computing does not stand for a completely new concept, as several computing paradigms have promised to deliver this utility computing vision such as Cluster computing, Grid computing, and more recently Cloud computing. A utility service in the Cloud follows the same approach as a utility service in the current established utility facilities (e.g. electricity). Cloud's business model is based on Economies of Scale where efficiency of the provided service increases as the number of services being delivered increases. Hence, the average unitary cost of the service decreases, because the fixed costs of the service are shared over the increased number of provided services. For instance, state of the art magnetic resonance (MR) modalities have high purchase costs; if every healthcare institution (independently of its dimension) had a MR modality, the unitary price of each exam would be higher because there would not be enough patients to fill the modality's schedule. Therefore, the usage efficiency of the provided service would be low and, as a consequence, the service would have to be more costly. As result, typically there are imaging centers that own several modalities and sell the service to the patients of nearby healthcare institutions. This scenario brings several advantages: (i) - healthcare institutions do not need to invest heavily up-front in modalities to conduct their healthcare core business; (ii) - the institutions do not need to maintain the modalities; (iii) - there is more efficient use of the modality and therefore the costs of patients' exams may become lower.

In addition to economic advantages, the quality of service is a major incentive to use Cloud services: high availability, high reliability and high scalability (Binnig et al., 2009). Technologically, Cloud may be seen as a Grid with a different business model, managed by a single entity and with a virtualization strategy (Foster et al., 2008; Rajkumar Buyya, 2009). Its economic approach could make Cloud computing more sustainable than the Grid in the long term, because it is driven by economic goals and does not rely on uncertain and ephemeral project founding. As a consequence, Cloud computing could be seen as the next step of the Grid's technology to deliver computing as the 5th utility (Rajkumar Buyya, 2009; Rimal et al., 2009).

Cloud computing relies on virtualization. Virtualization fits the extremely dynamic Cloud environment very well. With it, computing environments may be dynamically created, expanded, shrunk, replicated or moved according to demand (Rimal et al., 2009). With virtualization, it is possible to easily build scalable and fault-tolerant systems according to the quality of service purchased by the cloud consumer. Virtualization is boosted by the increasing ability of hardware to run applications within Virtual Machines efficiently (Rajkumar Buyya, 2009), more precisely the recent advance in the field of multi-core microprocessor. Cloud Computing stands for the applications, the hardware resources and everything in between is delivered as a service.

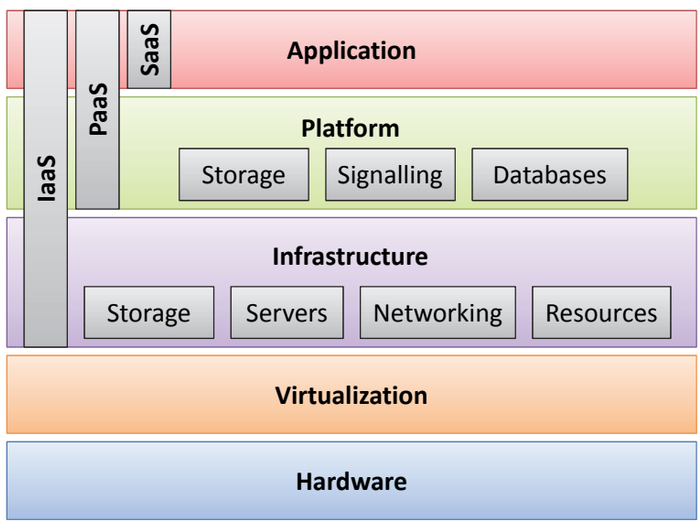


Fig. 4. Cloud Computing layers.

Figure 4 illustrates Cloud's abstract layers (Fu & Chen, 2010):

- **Hardware layer:** refers to the actual physical machines that compose the data center.
- **Virtualization layer:** the hardware resources of the below layer are shared among all the virtual machines supported (i.e. the hardware capabilities are sliced into virtual machines). Each virtual machine has a self-contained operating system and may be seen as an individual and independent machine.
- **Infrastructure layer:** Known as Infrastructure as a Service (IaaS) extends the services provided by the virtualization layer. It provides the mechanisms to manage, monitor, and configure all the supported virtual machines into a utility computing manner. IaaS is the

abstraction allowing access to infrastructure resources (e.g. storage, computation, server, data center) on-demand and paid according to the required quality-of-service (QoS).

- **Platform layer:** Known as Platform as a Service (PaaS) extends the IaaS layer by hiding the IaaS complexity. PaaS is accessed as one big system and not by accessing individual virtual machines. Therefore, it provides an abstraction where the virtual machines are automatically managed by the cloud service provider. Offering reliable services by default such as storage, databases and signalization.
- **Application layer:** Layer usually entitled as Software as a Service (SaaS) where the applications hosted on the Cloud are deployed on local computers typically through web-browser. On this layer, the payment is associated with the application itself and not with the platform or infrastructure below it. Typically, this layer is where developers build their applications.

The services themselves have long been referred to as Software as a Service (SaaS) and Cloud does not change that (Michael Armbrust, 2009). Nevertheless, Cloud Computing allows the application providers the choice of deploying their product as SaaS without providing a data center.

3. Challenges

Cloud promises to deliver financial benefits to enterprises by reducing the costs of the IT department. The IT infrastructure supporting the storage of medical images is a heavy burden for healthcare institutions. Besides storing the clinical data in a reliable manner, it is also required to make that data available 24/7 and provide appropriate access performance - a true management nightmare (Huang, 2010). When the scope of the IT infrastructure ranges from an intranet to a cross-enterprise solution, the associated costs, complexity and effort of deployment also increase. Regarding the financial dimension, Cloud's business model is attractive to build cross-enterprise solutions, such as XDS-I, due to the fact that the costs associated with components shared by the community (e.g. XDS Document Registry, XDS Document Repository) would be paid as a service and according to each institution's use. In this way, the significant costs of developing and maintaining such infrastructure would be eliminated. Unfortunately, the outsourcing of clinical data to the Cloud faces many challenges that must be considered before moving the clinical data or components of the IT infrastructure to the Cloud.

3.1 Privacy and confidentiality

The privacy and confidentiality of the data placed on the Cloud are the main barriers that delay Cloud's general acceptance. The World Privacy Forum (WPF) released a report spelling out the risks to privacy and confidentiality posed by Cloud computing. The report unveils concerns regarding Cloud's current state: what happens to the data after the consumer uploads it to the Cloud and how its confidentiality will be protected. The answer to this question is somehow disappointing. In the current state of Cloud computing it does not ensure privacy or confidentiality of the stored data. The simple fact of uploading data to the Cloud makes that data more suitable for disclosure or unauthorized usage. The WPF published several privacy advices in order to aware the cloud consumers:

- Read the Terms of Service before placing any information in the cloud. If the Terms of Service are not understandable, a different cloud provider must be considered.

- Information in the cloud is legally easier to access through the Cloud than by seizing a private computer. Therefore, sensitive information should not be uploaded to the Cloud.
- In the Term of Services one must notice if the Cloud provider reserves rights to use, disclose, or make the uploaded information public.
- Read the Privacy Policy before placing any information in the cloud. If the Privacy Policy is not understandable, a different cloud provider must be considered.
- Beware if the Cloud provider retains rights over removed data by the consumer.
- Beware if the cloud provider notifies their consumers when the Terms of Service or Privacy Policy change.

Furthermore, WPF extends its advices to companies or governments that are considering the upload of data or the migration of the IT infrastructure to the Cloud:

- Caution on ad-hoc Cloud computing is advised. Organizations should have standardized rules for employees to know which data they may (or not) upload to the cloud.
- Sensitive information that is of the interest of the organization to keep away from the government, other competitive organizations or other governments should not be uploaded.
- Information disclosure of cloud's data should be considered before uploading the actual data.
- Hire professional support for understanding the Terms of Service or Privacy Policies of the Cloud provider.

After analyzing these advices, answering the question: Is the current state of Cloud computing suitable for storing any PHI? The answer is pretty straightforward: No! Any cloud consumer should consider that any uploaded data could be used by others e.g. statistics, publicity or even be sold to competitors. For instance, health insurance companies may buy information regarding the health history of a patient in order to assert fees or deny the health insurance to the patient. At this case, the patient privacy right was jeopardized and there was a confidentiality breach. Even if the uploaded medical data is anonymous for safeguarding the patient's privacy, it is still possible to infer statistical analysis to the data identifying geographical regions propitious to certain pathologies and sell that information to health insurance companies. Terms of Service and rigid Privacy Policy agreements may raise the protection of the stored data by adding liability to the Cloud provider. However, is extremely difficult to prove that the stored data was violated, or not, by the Cloud provider. Therefore, Cloud computing, without any privacy and confidentiality protection system built over the Cloud, is not suitable to store any data undesirable to be disclosed.

3.2 Interoperability and standardization

Although some efforts towards reaching standardization among for Cloud Computing, such as the Cloud Computing Interoperability Forum (CCIF) or the European Telecommunications Standards Institute (ETSI), the reality is that cloud standardization is far from being achieved and at some levels maybe it never will, as a consequence, the lack of interoperability inter-cloud provider is a resilient issue. If it is possible and relatively easy to guarantee cloud interoperability at the IaaS level even without standardization (e.g. DeltaCloud [3]),

[3] http://incubator.apache.org/deltacloud/

accomplishing interoperability between the several PaaS is a more demanding task. Not only due to possible economical interests of the Cloud providers, but as well at the technical level. PaaS APIs abstract the complexity of the IaaS and provides the developers with embedded functionalities (e.g. automatic scaling) that at the IaaS level have to be implemented from scratch . This facilitated API of PaaS is more convenient for the developer but less flexible at the same time (Michael Armbrust, 2009). PaaS automatic features turn the standardization or interoperability efforts more complex. Each Cloud provider follows its unique IT architecture - especially above the IaaS level (PaaS or SaaS). If some features are easy to accomplish in some cloud architectures, the same features could be extremely difficult to achieve at other architectures. This heterogeneity of features and architectures may push back standardization, and turn full interoperability above the IaaS level extremely difficult.

3.3 Geographical distribution

The Cloud providers are private companies adjudicated to a country obligated to follow the countries laws. However, they compete with each other on a global market, ignoring countries borders. Enabled by the Internet, a Cloud provider from the USA may easily offer its Cloud services to a consumer from Singapore or Australia. At the same level, a Cloud provider may have several data centers around the world. For instance, one of the major expenses of a data center is the energy consumed for refrigerating the machines and, if the data center is placed in a cold natural geographical location (e.g. Alaska) the cooling costs will be much lower and the Economics of Scale enhanced. However, this cross-border logistics of the Cloud business model may aggravate liability and jurisdiction risks, due to the fact that cross-border litigation is typically more complex and high-staked than litigations within borders, and is not clear which court have jurisdiction over the Cloud where the illegality occurred: would it be treated in the jurisdiction of the consumer, the provider or the vendor?

3.4 Consumer lock-in and bankruptcy

Consumer lock-in and bankruptcy of the Cloud provider are two serious risks and both have a similar consequence, which is losing control of the data trusted by the cloud consumer to the cloud provider. Consumer Lock-in may be performed at two different levels: data lock-in and vendor lock-in. Trusting valuable data to a single provider may lead to opportunistic reprising, where the provider uses the held data at its data centers to blackmail the costumer and rise prices while renegotiating contracts. Vendor lock-in is more subtle type of consumer lock-in. Due to the fact that each Cloud provider offers, to its customers, a unique development API which turns the applications specific to the Cloud provider. Therefore, the consumer is locked-in with the Cloud provider since migrating the applications to other Clouds means recoding the applications following the new cloud API. As a result, the cost of migration does not compensate the eventual competitive prices of other Clouds. As it was mentioned before, other risk that could lead to losing control of the consumer's data is the bankruptcy of the Cloud Provider. Cloud Providers are companies and companies may go bankrupt. The obvious question that arises is what happens to the consumer's data and applications if such scenario becomes a reality? Migrating data (e.g. images or documents) probably would be less demanding than migrating applications developed with specific PaaS API. As a result, the lack of interoperability at the PaaS may turn the migration process extremely difficult, requiring the refractor of the majority of the source code.

4. Available solutions and new opportunities

As we mentioned at the Challenges section, the architecture of Cloud Computing is not suitable by itself to sustain PHI. There were identified several issues that turn the outsourcing of PHI on the Cloud inappropriate or even illegal. However, when the challenges are identified, opportunities also may emerge to mitigate them. At this following section we will present some design approaches, built over the Cloud, in order to enable XDS-I IT infrastructure to be outsourced to the Cloud taking into consideration the previous identified challenges.

4.1 Encryption and decryption client-side

The public Cloud design permutes the previous trust patterns of older computing paradigms such as Client-Server. For instance, at the Client-Server paradigm the Server is considered the most trustworthy entity of the architecture. This trust assumption fades away when the data to be dealt on the Cloud is PHI. At this scenario of storing PHI on the Cloud the trustworthy entities are the clients and it must be assumed that the Cloud's data center is untrustworthy. Therefore, besides the transmission channels between nodes, the information must be hidden from the central node where the information is stored or relayed, more precisely the Cloud's data center. To do so, the encryption must be performed on the client machine and stored ciphered at the Cloud data center. Consequently, a reverse procedure must be performed while retrieving the information from the Cloud: download the ciphered data and decrypt it at the client machine. The described workflow may seem trivial but is the core essence of several systems that use the Cloud to connect trustworthy nodes. With this strategy two approaches may emerge: Cloud as a Relay or Cloud as a Repository.

4.1.1 Cloud as a eelay

In the Cloud as a Relay approach the Cloud is used to create a virtual bridges between the intranets of different healthcare institutions enabling the exchange, search and store of medical images within a wide domain (Ribeiro, Costa & Oliveira, 2010; Ribeiro, Silva, Costa & Oliveira, 2010). They add at each trust node (i.e. intranet of the healthcare institutions) one device that acts as a proxy for the income data and as a gateway for the outcome data. The proxy/gateway device installed within the healthcare institution speaks DICOM (i.e. the device is DICOM compliant and implement several DICOM services) and with the outside it communicates through Internet standards such as IMAP and HTTPS (figure 5). The mentioned solutions are interoperable within the institution due to the fact that they implement the DICOM services. However, at the cross-enterprise scale the communication is ad-hoc. Nevertheless, they were managed to enable the exchange of medical images through a Cloud bridge without jeopardizing the confidentiality and privacy of the clinical data. Furthermore, because the Cloud is just used as a relay and the PHI is stored temporally it mitigates identified issues, namely consumer's lock-in, bankruptcy of the Cloud provider, and the geo-distributed nature of the Cloud is irrelevant. However, the major drawbacks of such solutions are: (i) - the Cloud is just used as a relay and the IT infrastructure remains at within the institution. Therefore, the Cloud's benefit, of outsourcing at lower prices, is not ideal. Furthermore, a VPN connection would have the same effect (although in several countries opening a VPN connection in a public healthcare institution is a bureaucratically and procedure and such solutions may diminish the initial inertia of inter-site cooperation). (ii) - The performance of the relay strategy decreases while comparing with storing the data at the Cloud in a repository

approach, since the data must be uploaded to the cloud and downloaded from the cloud for all inter-site interactions. (iii) - Such solutions may not be considered pure cross-enterprise because, for instance, they do not deal with cross identification of patients so that task is managed manually.

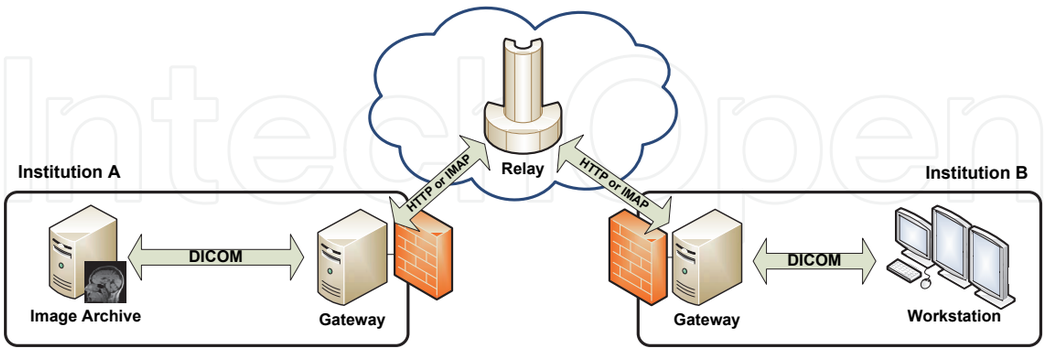


Fig. 5. Example of using Cloud as a Relay inter-connecting two different healthcare institutions.

4.1.2 Cloud as a repository

In the Cloud as a Repository approach the Cloud is used as repository of medical images (i.e. Image Document Source) (Silva et al., 2011). The architecture is similar to the Cloud as a Relay: there is a device (e.g. gateway) that encrypts/decrypts the clinical data client-side. However, the ciphered data is stored in a persistent manner at the cloud (figure 6). Furthermore, the trivial approach does not enable rich search queries (e.g. by patient demographics) only queries by unique identifier of the document. To overcome this problem Silva et al. (2011) decoupled the searchable text based data of the images (metadata) from the image data pixel itself. The pixel component data is encrypted and stored at the Cloud while the searchable metadata is stored is a server that is owned (therefore trustworthy) by the healthcare institution. This approach diminishes the IT infrastructure more than the Cloud as a Relay approach, since the metadata represents a small portion of the data required to be stored. Furthermore, the privacy and confidentiality of the clinical data is guaranteed and the geo-distribution nature of the Cloud is diminished. However, this approach may be affected from Cloud bankruptcy or data lock-in due to the fact that the actual pixel data is at the Cloud-side. These risks are minimized since the gateway of Silva et al. (2011) enables Cloud provider redundancy, by following a similar approach of DeltaCloud. This way, healthcare institutions are able to store the ciphered pixel data at more than one cloud provider in a transparent manner for the institutions' DICOM devices, increasing the reliability of the system. The Silva et al. (2011) PACS solution is ideal for a multi-site healthcare institution enabling the institution's distributed nodes to share the same PACS archive. However, the trust community created does not follow the communication standards recommended by the XDS-I content profile and vendor lock-in is still possible at the cross-enterprise scale. Nevertheless, XDS-I does not predicts the outsourcing of the IT infrastructure and Silva et al. (2011) was capable of developing a cross-site solution enabling it without jeopardizing the privacy and confidentiality of the clinical data, and with an acceptable performance degradation while comparing with local PACS archive.

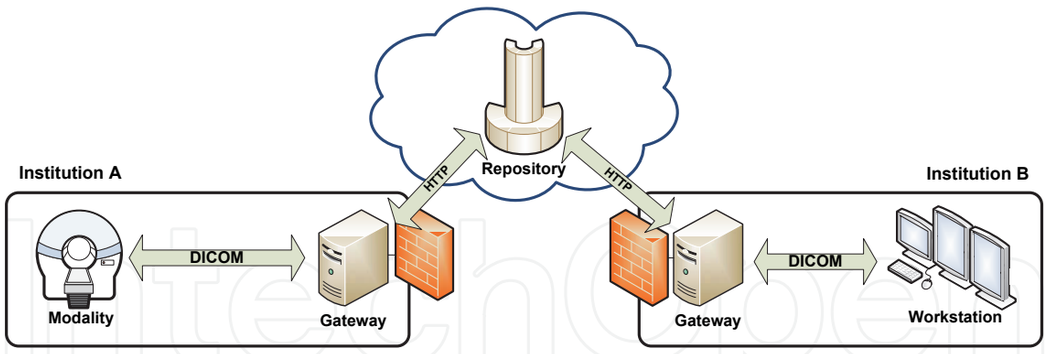


Fig. 6. Example of using Cloud as a Repository of clinical information.

4.2 XDS-I infrastructure on the cloud

The current state of Cloud Computing does not guarantee privacy or confidentiality of the stored data. Even if the Service Terms and the Privacy Policy of the Cloud provider claim privacy and confidentiality of the trusted data, it is extremely difficult (if not impossible) to prove that there was not any leak of information or if there was some data mining processes to extract patterns of the clinical data. Therefore, the system's design running above the Cloud must take this issue in consideration. As we mentioned previously, XDS-I assumes that the nodes where its actors are instantiated are trustworthy. Therefore, the clinical data may be stored in a readable manner - assumption possible to have in private Clouds owned by trustworthy entities (e.g. hospital, National Healthcare System) but inappropriate to have in public Clouds. In order to combine these two concepts (public Cloud and XDS-I) one must ensure privacy and confidentiality of the PHI without removing the interoperability of the XDS-I content profile. Analyzing the XDS-I actors (figure 2) we have three candidates to be migrated to the Cloud: Document Registry, Document Repository and Imaging Document Source. The only central and unique component of the Affinity Domain is the Document Registry, which searches the registry to locate documents that meet the criteria specified in the query request by the Document Consumer IHE (2006b). The queries supported by the Document Registry are well defined by the transaction Registry Stored Query (IHI-18). This transaction reduces directly or indirectly the scope of the search to the global patient ID of the respective affinity domain. For instance, to find documents' metadata the patient ID must always be supplied and within that patient scope the search query may filter according other attributes (e.g. document's type, author's ID). Therefore, queries only based on patient demographics are not supported. Patient demographics are an optional field only intended as an audit/confirmation mechanism for the Document Consumers (IHE, 2010). Ribeiro et al. (2011) was able to launch XDS Document Registries on the public Cloud in a secure manner and keeping the privacy and confidentiality of the metadata. Any fields of the metadata on the XDS Registry possible to extract meaning (e.g. patient demographics, institution's name) are protected. The level of protection is defined by the administrator of the Affinity Domain that may vary from storing the meaningful fields encrypted to not allowing those fields to be stored at all. This is possible due to the fact that the readable metadata with meaning is optional. Nevertheless, from the three above mentioned candidate actors the XDS Document Registry is the one that offers less consequences if disclosure of the meaningful fields occurs. In the other hand, the other two candidate actors, Document Repository and Imaging Document Source, hold valuable clinical information and must be protected accordantly from disclosure.

The approaches to ensure privacy and confidentiality, and at the same time interoperability while migrating these two actors to the Cloud may pass by:

1. **Encrypted Storing and on-the-fly Decryption:** The PHI is cloud-side encrypted with one symmetric key generated by the XDS-I actor (unknown to any other entities). The encrypted PHI is stored on the cloud. Whenever transaction triggers the access to the encrypted data, the data is decrypted on-the-fly and the transaction is answered with readable data. This approach guarantees interoperability and adds some level of data privacy/confidentiality protection. However, it is possible that when the data is being decrypted on-the-fly the Cloud provider sniff it leaking the PHI.
2. **Middleware encryption/decryption:** One middleware device is added between the communication of the Document Consumer and the Document Repository or Image Document Source placed on the cloud. The middleware device is owned by the healthcare institution and is responsible for translating (encrypting/decrypting) the flow of data between the two end actors. The middleware device implements the XDS-I transactions and therefore it is interoperable. Furthermore, privacy and confidentiality of PHI is ensured due to the fact that PHI is stored ciphered and encrypted in a trustworthy node. However, this approach may bring performance degradation compared with the previous approach since the message flow required is always bigger. Finally, the middleware machine owned by the healthcare institution would be a bottleneck and scalability and availability issues could rise.
3. **XDS for private imaging:** The XDS integration profile was designed to be document format independent, i.e. it supports any document type. When the Document Consumer retrieves data from the Document Repository like, for instance, a report in the Portable Document Format (PDF) the document requires a PDF reader in order to be accessed by the healthcare professional. The same occurs at XDS-I when a DICOM object is retrieved from the Imaging Document Source. XDS-I is a content profile based on the XDS integration profile for dealing with medical imaging. Following the same thread of thought and taking in account that XDS is format independent it is possible to design a new content profile XDS for private images (XDS-π). At XDS-π the three candidate actors could be migrated to the public cloud, storing the documents and the medical images encrypted, and the encryption/decryption would be performed client-side. This approach ensures the PHI privacy and confidentiality and interoperable at the architecture level since the transactions and the actors of the XDS-I would be the same. However, the drawback of this approach would be the lack of interoperability at the document level since it is not yet predicted by IHE.

Furthermore, the three above approaches may follow a Searchable Symmetrical Encryption (SSE) to discover wanted documents among the encrypted resources stored on the cloud. Single private-key encryption inhibits the search document among encrypted blobs of data. SSE enables the search of keywords over the encrypted data without the need to decrypt the data or disclosure the keyword (Curtmola et al., 2006). Therefore, SSE ensures privacy and confidentiality of the data and at the same time the ability of retrieve selectively documents from the Cloud is maintained. Finally, comparing the risk associated with each approach the 1^{st} approach is the one that offers less privacy and confidentiality protection. In the other hand, the 2^{nd} and 3^{rd} approaches offer higher levels of protection from disclosure which, in our opinion, are adequate for storing PHI on the Cloud.

5. Conclusion

It is expected that the production of medical imaging will continue to increase in the following decades. For instance, the PET-CT modality requires space for storing the PET images, the CT images and the outcome fusion images and, the same situation happens with the new modality PET-MRI. Furthermore, there is a new research trend of content-based image retrieval, where it is possible to discover and retrieve images based on the pixel data of the image. This content-based retrieval is enabled by models describe the image and these models also require store space. As result, the storing requirements of the medical imaging fields are demanding and will be even more demanding in the future. Therefore, new storage solutions with flexible business models are needed more than ever. The Cloud computing paradigm offers an elastic framework to allocate or release computational resources on-the-fly and enabling a more efficient usage and, as a consequence, reducing costs. Current PACS architectures, hospital oriented, with their own short-term and long-term archives with no or little interaction with other institutions or PACS are difficult to extrapolate to the cross-institutional environment. XDS-I allied with XCA integration profile set the roadmap to enable the cross-enterprise medical imaging sharing. The conjugation of both integration profiles offers to the healthcare institutions flexible levels of inter-institutional coupling: through XDS-I the institutions create a common trust community (XAD) aggregating their federations into one single federation of medical imaging inter-site sharing or through XCA allowing access to the documents of other XADs without the need of federation fusion. Ribeiro, Costa & Oliveira (2010); Ribeiro, Silva, Costa & Oliveira (2010); Silva et al. (2011) proved that storing and/or distribute medical images and related exams using public Cloud providers is possible. Although, these solutions are interoperable within institution (since are DICOM compliant) at the cross-enterprise level they do not follow the transactions defined by the IHE. Nevertheless, based on their experience and on the hypothesis analysis performed at the new opportunities section we conclude that the public Cloud Computing utility has potential to host several actors of the XDS-I content profile safeguarding the privacy and confidentiality of the PHI.

6. Acknowledgment

The research leading to these results has received funding from Fundação para a Ciência e Tecnologia (FCT) under grant agreement PTDC/EIA-EIA/104428/2008.

7. References

Binnig, C., Kossmann, D., Kraska, T. & Loesing, S. (2009). How is the weather tomorrow?: towards a benchmark for the cloud, *DBTest '09: Proceedings of the Second International Workshop on Testing Database Systems*, ACM, pp. 1–6.

Costa, C., Silva, A. & Oliveira, J. (2007). Current Perspectives on PACS and a Cardiology Case Study, *Computational Intelligence (SCI)* 65: 79–108.

Curtmola, R., Garay, J., Kamara, S. & Ostrovsky, R. (2006). Searchable symmetric encryption: improved definitions and efficient constructions, *Proceedings of the 13th ACM conference on Computer and communications security*, CCS '06, ACM, pp. 79–88.

De Backer, A., Mortele, K. & De Keulenaer, B. (2004). Picture archiving and communication system–part 2 cost-benefit considerations for picture archiving and communication system., *JBR-BTR: organe de la Société royale belge de radiologie (SRBR)= orgaan van de Koninklijke Belgische Vereniging voor Radiologie (KBVR)* 87(6): 296.

Faruqui, S. A. (2005). *Utility computing: certification model, costing model, and related architecture development*, California State University.
URL: *http://books.google.pt/books?id=wMdENwAACAAJ*

Foster, I., Zhao, Y., Raicu, I. & Lu, S. (2008). Cloud computing and grid computing 360-degree compared, *IEEE Grid Computing Environments* .

Fu, L. & Chen, T. (2010). Building enterprise application based on cloud computing, *E-Health Networking, Digital Ecosystems and Technologies (EDT), 2010 International Conference on*, Vol. 2, pp. 534 –537.

Hendee, W. R. & Ritenour, R. (2002). *Medical Imaging Physics; 4th ed*, Wiley, New York, NY.

Huang, H. (2010). *PACS and Imaging Informatics: Basic Principles and Applications*, John Wiley & Sons.

IHE (2006a). It infrastructure (iti) technical framework integration profiles, revision 6.0 - final text, *Technical report*, Integrating the Healthcare Enterprise.

IHE (2006b). Iti technical framework supplement: Cross-enterprise document sharing for imaging, *Technical report*, Integrating the Healthcare Enterprise.

IHE (2008). It radiology technical framework integration profiles, revision 9.0 - final text, *Technical report*, Integrating the Healthcare Enterprise.

IHE (2010). It infrastructure technical framework: Cross-transaction specifications and content specifications, *Technical report*, Integrating the Healthcare Enterprise.

Jacq, N. (2007). *From genes to personalized healthcare: grid solutions for the life sciences : proceedings of HealthGrid 2007*, Studies in health technology and informatics, IOS Press.

Langer, S. (2009). Issues Surrounding PACS Archiving to External, Third-Party DICOM Archives, *Journal of Digital Imaging* 22(1): 48–52.

Lovis, C., Spahni, S., Cassoni, N. & Geissbuhler, A. (2007). Comprehensive management of the access to the electronic patient record: Towards trans-institutional networks, *International Journal of Medical Informatics* 76(5-6): 466–470.

Michael Armbrust, e. a. (2009). Above the clouds: A berkeley view of cloud computing, *Technical Report UCB/EECS-2009-28*, EECS Department, University of California, Berkeley.

Mora, L., Nevid, J. & Chaplin, W. (2008). Psychologist treatment recommendations for internet-based therapeutic interventions, *Comput. Hum. Behav.* 24(6): 3052–3062.

Mustra, M., Delac, K. & Grgic, M. (2008). Overview of the DICOM standard, *ELMAR, 2008. 50th International Symposium*, Vol. 1.

Pattynama, P. M. T. (2010). Legal aspects of cross-border teleradiology, *Eur J Radiol* 73(1): 26–30.

Pianykh, O. S. (2008). *Digital Imaging and Communications in Medicine: A Practical Introduction and Survival Guide*, Springer Publishing Company, Incorporated.

Rajkumar Buyya, e. a. (2009). Cloud computing and emerging it platforms: Vision, hype, and reality for delivering computing as the 5th utility, *Future Generation Computer Systems* 25(6): 599–616.

Ribeiro, L. S., Blanquer, I., Costa, C. & Oliveira, J. L. (2011). On demand ihe xds document registries on the cloud, *international Journal of Computer Assisted Radiology and Surgery*, Springer, pp. 297–298.

Ribeiro, L. S., Costa, C. & Oliveira, J. L. (2010). A proxy of dicom services, *Advanced PACS-based Imaging Informatics and Therapeutic Applications*, SPIE Medical Imaging.

Ribeiro, L. S., Silva, L., Costa, C. & Oliveira, J. L. (2010). Email-p2p gateway to distributed medical imaging repositories, *3th International Conference on Health Informatics*, pp. 310–316.

Rimal, B. P., Choi, E. & Lumb, I. (2009). A taxonomy and survey of cloud computing systems, *Networked Computing and Advanced Information Management, International Conference on* 0: 44–51.

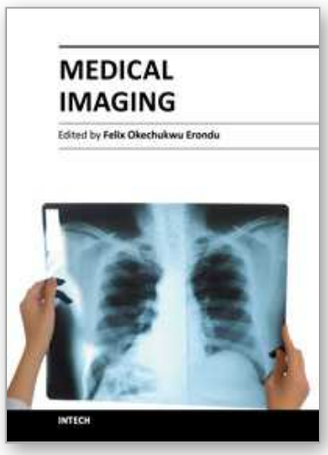
Roentgen, W. (1898). Ueber eine neue art von strahlen, *Annalen der Physik* 300: 12–17.

Ruotsalainen, P. (2009). Privacy and security in teleradiology, *European Journal of Radiology* .

Silva, L., Costa, C. & Oliveira, J. (2011). A pacs archive architecture supported on cloud services, *International Journal of Computer Assisted Radiology and Surgery* pp. 1–10. 10.1007/s11548-011-0625-x.
URL: *http://dx.doi.org/10.1007/s11548-011-0625-x*

Størkson, S. A. & Aslaksen, A. (2009). Pacs: Beyond radiology, *International Journal of Computer Assisted Radiology and Surgery* 4: 168–170. 10.1007/s11548-009-0321-2.

IntechOpen



Medical Imaging

Edited by Dr. Okechukwu Felix Erondu

ISBN 978-953-307-774-1
Hard cover, 412 pages
Publisher InTech
Published online 22, December, 2011
Published in print edition December, 2011

What we know about and do with medical imaging has changed rapidly during the past decade, beginning with the basics, following with the breakthroughs, and moving on to the abstract. This book demonstrates the wider horizon that has become the mainstay of medical imaging sciences; capturing the concept of medical diagnosis, digital information management and research. It is an invaluable tool for radiologists and imaging specialists, physicists and researchers interested in various aspects of imaging.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

Luîs S. Ribeiro, Carlos Costa and José Luîs Oliveira (2011). Current Trends in Archiving and Transmission of Medical Images, Medical Imaging, Dr. Okechukwu Felix Erondu (Ed.), ISBN: 978-953-307-774-1, InTech, Available from: http://www.intechopen.com/books/medical-imaging/current-trends-in-archiving-and-transmission-of-medical-images

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2011 The Author(s). Licensee IntechOpen. This is an open access article distributed under the terms of the Creative Commons Attribution 3.0 License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

IntechOpen

IntechOpen