

Myron Coulson

DTEC 6823

Final Paper

East Carolina University

ABSTRACT

Today many companies strive to move towards secure, reliable, and cost effective information systems; the healthcare industry is no exception. Securing, storing, and providing reliable access to healthcare data has become more important in healthcare as physicians are expecting immediate and remote access to patient data. While there are many aspects related to patient data and information, the digital capture, storage, and management of radiology images has become an important part of many healthcare organizations. From large hospitals to small clinics and physician offices, the use of systems like PACS (Picture Archiving and Communication Systems) is quickly becoming the standard for medical image storage and distribution.

The Secure Storage, Distribution, and Management of Radiology Images

The transition from capturing patient images on film to a digital format has become a popular alternative for many healthcare organizations. This transition can be complex, expensive, and require a lot of technical support to build and maintain a secure and reliable environment for healthcare professionals. By providing such an environment, physicians, clinical staff, and patients can benefit from immediately retrievable and reliable information. Without the proper management, hardware, and software of this type of information system, the data can become unavailable, unreliable, or the security could be jeopardized which could have a direct impact on patient care. In addition, the complexity and sophistication of many PACS can create a series of economic, educational, integration, and implementation challenges.^[1] With the careful and well planned implementation of PACS, facilities can provide the physicians and patients with technology to enhance and greatly increase the quality of patient care while maintaining the security of patient data.

PACS in its most basic definition is the capture, storage, and distribution of medical images to a central repository. Instead of capturing patient images on film and housing them in a film room or library, the data is stored in a central information systems

repository and can be accessed by many healthcare professionals at the same time. Accessibility by clinicians outside the radiology department is critical to success in sharing digital images for both patient care and productivity improvement.^[2] This type of system increases accessibility to patient data which lends to a more efficient healthcare system. Physicians can access patient data more quickly which can lead to faster clinical decisions, easier access for consulting physicians, and the ability to provide quick access to a patient's prior studies for comparison. In addition, many of the redundant tasks of a film based environment can be eliminated.^[6] The hanging of films, locating lost or misplaced films, or the time taken to retrieve films from a storage facility are no longer necessary in a true PACS environment. Another benefit of a PACS is the ability to write patient studies to CD so the patient can take the study with them for their physician to review.

Transition to a PACS environment can be a difficult change for many organizations. Although PACS has been available to the healthcare industry for about 12 years, the advances in technology have made it a valuable information systems in treating and diagnosing patients.^[3] The challenge of such an implantation often is dependant on the leadership of the healthcare organization and the willingness of the information systems department and radiology department to work together to achieve the goal of a successful implementation.^[7] Three of the major concerns I had when my organization made this transition were: the security of the images, the reliability of the storage system, and the ability to recover from any type of software or hardware failure. All three of these concerns are directly related to the security of the data. Without a secure system, images

could be accessed by unauthorized personnel. Without a reliable storage system, the data could be lost or corrupted which could result in the loss of patient information. And, without a reliable software and hardware environment, the system could become unavailable. All three of these situations would directly impact patient care.

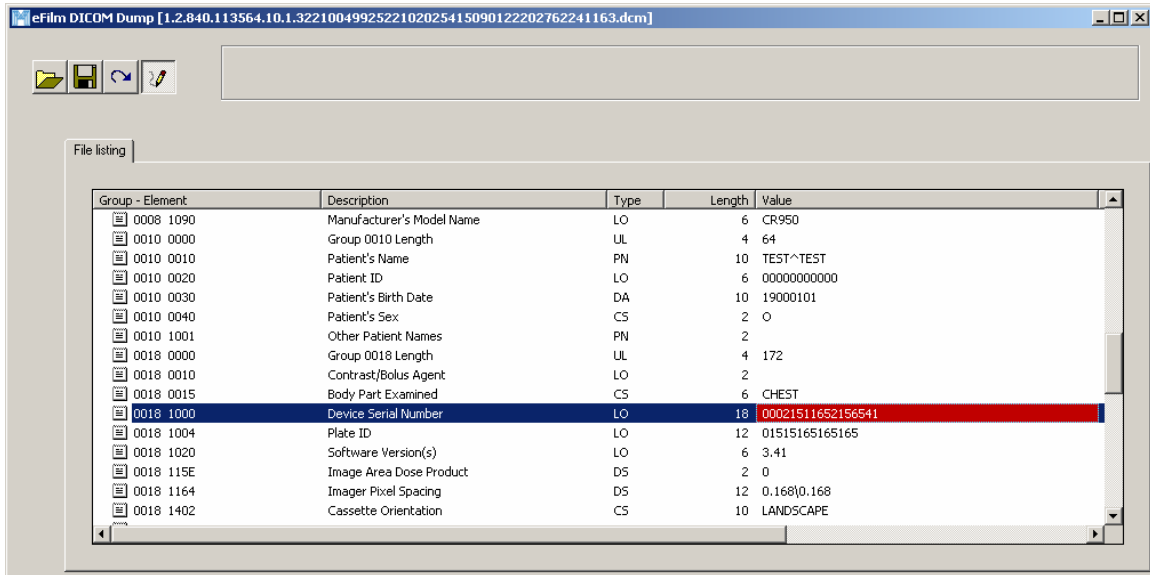
Securing medical images on a local area network and then making these images available to referring physicians across a wide area network such as the Internet can bring some serious security concerns and challenges to the management and technical staff of a PACS environment. The ability to secure patient information is imperative to the organization. Any breach of security to patient information could result in serious implications by the government and destroy the organizations credibility. With new laws and regulations; such as HIPAA, an organization needs to take the appropriate steps necessary to guarantee the secure storage and transmission of patient data. The public has a growing concern about patient data being available via the Internet. According to one survey, 36% of people are very concerned about the privacy of their personal medical records.^[8] With statistics like this, the need for a secure environment is only reinforced.

The standard protocol for capturing and storing medical images is DICOM (Diagnostics Imaging and Communications in Medicine.). A DICOM data packet contains the image from the radiology modality along with the patient information or demographics.^[4] Before the DICOM standard was introduced, most radiology devices were considered stand alone systems that could not communicate with other devices.^[6] With the

standardization of a communication protocol, devices from several different vendors could communicate and data could now be captured and stored in a central repository. DICOM data transmission is often not encrypted and transmitted in clear text across many networks. Figure one below, shows a “DICOM Dump” of a fictitious patient record. The patient information is visible in the header of the data packet. Since this information is protected and considered patient information that should not be jeopardized, the security of these packets across the network should be a concern. Access to the data on the network and the visibility of the packets themselves were the two major concerns I had with the implementation of PACS. While the actual transmission of the DICOM packets is usually not encrypted within the secure LAN (Local Area Network), encryption or some other secure transmission method is recommended for data transmissions on unsecured or untrusted networks. The figure below (figure 2) shows a DICOM packets captured on a local area network with packet capturing software. The patient data is clearly visible in this data capture. If this type of transmission were to be used over the Internet, patient data could be captured and viewed by unauthorized users. Although it is possible to secure the data within the local area network, doing so will increase the complexity and cost of the PACS. In addition, a performance decrease could result in added security methods on the local area network. Internal VPNs, data encryption, and private VLANs are a few methods that could be used to better secure data transmission on the private local area network. Securing the transmission of data on the local area network was an intermediate concern because access to the network is already secure and is monitored and maintained by the security team of the information systems department. Most of my concerns were remote access to patient data across the

The Secure Storage, Distribution, and Management of Radiology Images

Internet from physician offices and private homes. Providing this access can be done in many ways, but the use of Internet based web browsers has become popular because it requires minimal software installation on the client side and makes the system more accessible and most everybody already knows how to use an Internet web browser.



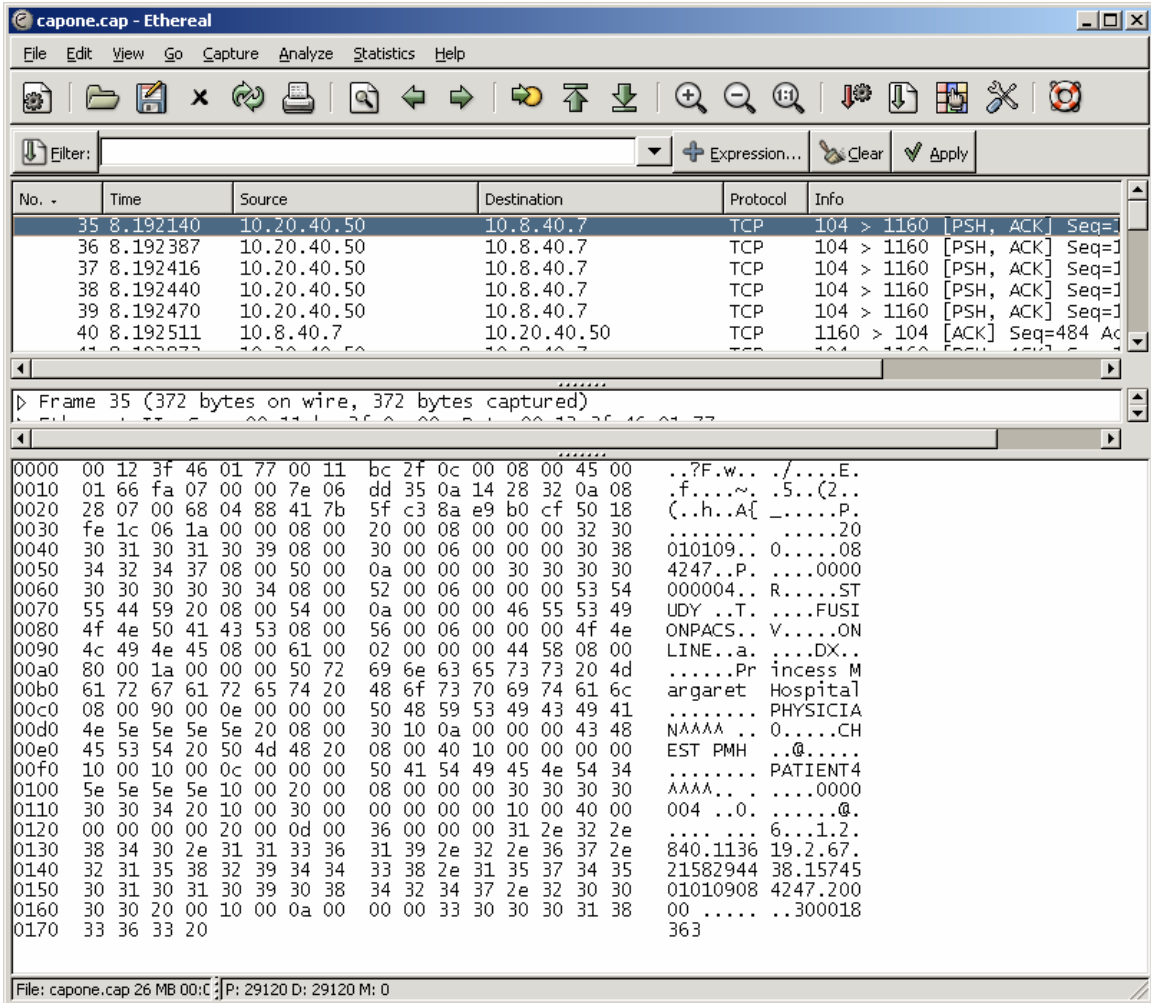
eFilm DICOM Dump [1.2.840.113564.10.1.3221004992522102025415090122202762241163.dcm]

File listing

Group - Element	Description	Type	Length	Value
0008 1090	Manufacturer's Model Name	LO	6	CR950
0010 0000	Group 0010 Length	UL	4	64
0010 0010	Patient's Name	PN	10	TEST^TEST
0010 0020	Patient ID	LO	6	0000000000
0010 0030	Patient's Birth Date	DA	10	19000101
0010 0040	Patient's Sex	CS	2	O
0010 1001	Other Patient Names	PN	2	
0018 0000	Group 0018 Length	UL	4	172
0018 0010	Contrast/Bolus Agent	LO	2	
0018 0015	Body Part Examined	CS	6	CHEST
0018 1000	Device Serial Number	LO	18	00021511652156541
0018 1004	Plate ID	LO	12	01515165165165
0018 1020	Software Version(s)	LO	6	3.41
0018 115E	Image Area Dose Product	DS	2	0
0018 1164	Imager Pixel Spacing	DS	12	0.168 0.168
0018 1402	Cassette Orientation	CS	10	LANDSCAPE

(FIGURE 1 – This is a DICOM dump of test data. The DICOM data contains the patient information along with the digital image)

The Secure Storage, Distribution, and Management of Radiology Images



(FIGURE 2- this data capture shows packets captured during a DICOM query for patient information. For privacy reasons, dummy data was used for this example. You can see the patient name as “PATIENT4”, medical record number, and type of procedure.)

The use of web based applications has become a popular standard for providing access to patient data for referring physicians. The security of the web based application needs to be considered when offering this type of access for remote users.

There are many methods for securing data over the Internet. However, many issues can arise when using different security methods. I have found that using a SSL web server that only forwards query requests to servers in the trusted network to be one of the most trouble free solutions for providing remote users access to patient data. Anytime the security is increased at the application level, the potential for application software problems increases. Many vendor software applications will not work with certain security software packages. And, requiring every remote user to have a software or hardware based security application, such as VPN software or hardware, can turn into a management nightmare and prove to be unfeasible. By working with the vendor of the PACS chosen, usually a suitable security plan can be developed and implemented. However, I have found that some vendor implantation teams will install the minimum security features to ensure a successful install and not inform the organization of other options for securing the PACS.

Legality issues require authorization and verification of the individuals accessing the DICOM data at any level of the network. With this concern, the ability to secure the data and provide some type of auditing mechanism becomes essential. I have seen two different scenarios in which the data can be accessed in a PACS environment. By actually logging into the software application with a user name and password and by providing an Application Entity Title (AE-Title) and port number that would allow a device to query the database software. These two methods of data access should be controlled and monitored by radiology or information systems staff. The ability to query the database and actually retrieve patient data and images should be carefully monitored and restricted to those people and devices that truly need this access for providing patient care.

The simple use of a username and password is the basic authentication method found in most software applications. PACS is no different and should provide this authentication and authorization method at the very least. The ability to control, force change, and require strong passwords should be another security feature of the system. Along with the use of usernames and passwords, the system should have the ability to monitor and audit user access. When users access the system and retrieve patient data, a detailed audit log should be accessible for review of the users actions incase any question about a patient's healthcare record is ever questioned. A good PACS should have this ability built in and easily accessible by the systems administrator. Without monitor and auditing, there would be no way of tracking users of the system.

A PACS should also have the ability of only accepting queries from known devices. A device list should be created and the PACS will only recognize queries from devices off this list. Most PACS that I have seen control this by only accepting communications from devices that have the correct AE Title, Port Number, and IP Address. This security feature of the system is not always on by default and has to be enabled by the system administrator. Many times during implementation of a PACS, this feature will be disabled until the system is up and running and then security features like this are turned on to better secure the system. The reason many implementation teams prefer to disable this feature during implementation is to allow easy connectivity for existing modalities and other network devices. Once connectivity has been established and tested, the enabling of security device lists is usually a best security practice. This will ensure that only authorized devices are allowed to query for patient data. While secure access to patient data is a major concern, the storage of patient data should not be overlooked.

When discussing secure storage of patient data, the security of where and how the data is stored should be considered. Storing data on one server without any replication or data mirroring would

not be a very secure solution. If the one server is jeopardized or has hardware or software failure, the system could become unusable resulting in system down time which would impact patient care. By providing a redundant system and having the data stored in a physically secure location, the system becomes more reliable and secure. And, with evolving technology in medical imaging, the need for large amounts of storage has become essential.^[10] Current and future medical studies can contain thousands of images for one patient study.^[10]

Many organizations use Storage Area Networks (SANs) or Network Attached Storage (NAS) to store patient data and images. Because images require a lot of storage space, it makes sense to use one of these two storage methods for a PACS. Another method of storage is the use of a Storage Service Provider (SSP). With this solution, data is stored off site by a third party vendor. Most storage providers make data available at three levels: online storage, data that is accessed all the time and needed quickly, long-term storage, data that is not accessed frequently and the retrieval time would be around one minute, and disaster recover storage, data that is need to rebuild a system in the event of a disaster.^[5] SSP storage is relatively new and many organizations do not feel comfortable having their data stored in a location they can not access. Many Information systems professionals like to have the data stored where it can be physically accessed and not have to rely on a third party to troubleshoot or bring the system back online in the event of a failure.

With a NAS or network attached storage system, the storage hardware can be physically located away from the actual PACS servers. This provides physical security of the data by allowing the data to be stored outside of the radiology department and in an appropriate building that is designed for data storage. The physical security of the data is often over looked in many organizations. Many small organizations do not have designated computer facilities and sometimes have no choice in where the data will be located within the facility. Physical security

of the data provides the data to only be accessible by authorized personnel, protects the data from accidents, provides an environment ideal for operating conditions of the hardware, and should safe guard the data from fire or water damage. By using network based storage, many radiology departments can house the servers within the department and store the data in a more suitable secure location that would promote a more secure environment for the patient data.

With the use of Storage Area Networks or SANS, the storage of data can be a little more complicated. With a SAN, there are sometimes limitations in how far the application servers can reside away from the storage. The SAN does provide a private network for the data and the data can only be accessed by servers attached directly to the SAN. Many debates over NAS versus SAN as a storage solution have been published. The cost difference between the two, scalability, and the complexity of management have been the main focus of these debates. There is not any one formula that will help decided which system is best for any organization's storage needs. Research and planning will be the best methods of determining the storage needs of an organization.

In considering storage for the PACS I was involved in implanting; two identical storage solutions were installed to provided redundancy and better security of the data. Both storage systems were installed in physically separate locations and in a secure, locked, and environmentally controlled computer rooms. I felt this solution, although a little more costly, provided the best solution and security of the patient data. In the event that one storage system would fail, the other would become immediately available for use. The data is replicated between the two systems and both systems are in use at the same time to provide load balancing and enhance performance of the PACS. By storing the patient data in two separate physical locations, the data is more secure and the organization is in a better position to recover from any failures or problems that could otherwise make the system unavailable.

When discussing disaster recovery in relation to PACS, it becomes imperative that the data be available to restore a system as quickly as possible. Disaster recovery is a security concern when focusing on how the data is archived or saved and how the data is restored to bring a system back online. Data should not only be stored onsite, but should also be archived and stored offsite for a disaster recovery situation.

Disaster recovery should be apart of any information system. With PACS, the recovery of patient information and images is imperative because the patient records could be permanently lost in the event of an onsite disaster. In addition to having redundant systems onsite at the facility where I was involved with a PACS implementation, it was also decided to create a disaster recovery tape archive system. This system was installed in another location on the campus and all images are written to a tape library. Once the tapes are filled, they are removed from the tape library, coded, and cataloged. The tapes are then moved to an offsite location and only recalled in the event of a disaster recovery situation. The offsite location is a secure and professional storage facility and the tapes can only be accessed by authorized personnel.

Advances in information systems technology can have many benefits to healthcare organizations. The ability to capture and manage data in systems like PACS can greatly reduce cost and increase accessibility to patient information and images. The management of systems like PACS can add complexity to an organization and increase costs if not implemented and maintained correctly. However, with the proper planning, implementation, and management of a PACS, physicians and other clinical staff can become more efficient and provide better patient care. The sharing of data and making data available from anywhere there is Internet access, lends to a more productive and environment that will benefit patients, clinical staff, and physicians. Although the technology, hardware, and software are key elements to the successful implementation of PACS, the support of upper management, teamwork across departments within the organization, and the willingness

of the users of the system to adopt and learn the system are the key factors to implementing a secure and successful PACS.

References

- [1] Bruce I. Reiner, M.D., Eliot L. Siegel, M.D., Khan Siddiqui, M.D., Evolution of the Digital Revolution: A Radiologist Perspective, Journal of Digital Imaging, Volume 16 Number 4 December 2003, p 324-330.
- [2] Karen Ondo, PACS Direct Experiences: Implementation, Selection, Benefits Realized, Journal of Digital Imaging, Volume 17 Number 4 December 2004, p 249-252.
- [3] Rita Eyer, Building our Image, Welch Memorial Lecture, Volume 34 Number 3 Fall 2003, p 22-24.
- [4] The DICOM Standard, An Introduction to the DICOM single-file format,
<http://www.psychology.nottingham.ac.uk/staff/cr1/dicom.html>

[5] Edward M. Smith, Storage Service Provider (SSP), Imaging Technology News, Research Report 476, March 2004.

[6] James A. Brink, M.D., Vladimir P. Neklesa, M.D., Pradeep Mutalik, M.D., Howard P. Forman, M.D., PACS Innovations Leading to Improved Patient Care, Applied Radiology, August 1998, p. 29-30.

[7] Paul Nagy, PhD, Keys to the Kingdom of the PACS Enterprise, Applied Radiology, July 2002, p. 7-9.

[8] Andis Robeznicks, Privacy Fear Factor Arises, Modern Healthcare, November 14th 2005, p. 6-8.

[9] Nelson Hazeltine, HIPAA Compliance Handbook 2002

[10] Integrated RIS-PACS Means Better Workflow & Data Management, Health Imaging and IT, September 2004 p.52-56.

Software

Ethereal, <http://www.ethereal.com>

Merge E-film, <http://www.merge.com>