DICOM Security in Healthcare IT

Ryan Daley

East Carolina University

Abstract

Digital Imaging and Communications in Medicine (DICOM) dictates protocols for the transfer and storage of medical images. The purpose of digitizing of medical images is to increase productivity, patient turnaround, access to prior studies, and efficiency. For the past 30 years DICOM data has replaced film in areas such as: Magnetic resonance imaging, mammography, computed tomography, and x-rays. Digitized medical images are no exception to the security paradigm of accessibility vs. security. With convince, the risk of a data breech is ever increasing. The security concerns rest in three zones of the DICOM workflow: storage, query / retrieval, and transportation. Due to the fact that DICOM packets contain patient information in the header, they fall under Health Insurance Portability and Accountability Act (HIPPA) regulations. HIPPA legally binds the responsibility of securing patient information in all areas of the information's lifecycle to the healthcare service provider.

Keywords: DICOM, IT Security, Healthcare IT

Table of Contents

Introduction

Medical Image management has changed drastically over the past few decades. One of the most major changes being the creation and standardization of the digital medical image. These medical images dictated under Digital Imaging and Communications in Medicine (DICOM) standards. The advent of using a digital medium for medical images has drastically increased efficiency in patient service and turnaround. It is not uncommon for there to be less than an hour of downtime from when the patient is seen, the Radiologist reads the images, and the patient gets their procedure results. Not only does this increase time efficiency, but it increases the accuracy of the results. These images can have a much higher resolution than was initially possible on film media, this resolution increase allows the Radiologist to read the results more precisely, potentially noticing smaller items that would not have been visible on the traditional film medium. Result accuracy is also improved because the availability of the patients prior studies is no longer by mail. A doctor could acquire a patients studies from, for example, 4 years prior in less than a second, allowing them to reference the results to leverage any potential changes towards the results of the current study. Due to these advantages, many areas of imaging have since been digitized, these areas include; Ultrasound (US), Computed tomography (CT), Magnetic resonance imaging (MR), X-Ray (XR), and Mammography (MG). (NEMA)

Medical imaging is no exception to the security paradigm of accessibility vs. security. Digitizing images that contain identifying patient data raises great concerns. With film, the only concern was physical breeches, but with DICOM data, patient privacy concerns raise evenly with the increase of efficiency. These images must be secured throughout their entire life cycle.

DICOM data is stored, transferred, and opened many times in numerous geographical locations over the time of one patient's procedure, this leaves many opportunities for a potential breech. These images are then archived and saved for use as reference in later studies. This constant stream of patient data falls under the regulation of the Health Insurance Portability and Accountability Act (HIPPA). HIPPA requires that healthcare facilities take great precaution in securing patient data during its entire lifecycle (CMT Medical Technologies). Image storage is conducted in an environment known as a Picture Archiving and Communications Systems (PACS). PACS are responsible for the protection, storage, and management of patient studies. These servers often hold hundreds of thousands of images, if one of these servers were compromised, it would be devastating to patient health and breech confidential patient information, including; names, birthdays, social security numbers, and medical history. Due the importance of this data, it is on the forefront of all modern healthcare IT concerns.

Workflow

The flow of DICOM data is divided into three separate areas; Acquisition, archival, with the last step being the radiologists' reading workstation. DICOM data is created by an imaging device that will scan a patient and create an image, these machines are commonly referred to as a Modality. Modalities are named by the type of data they produce, for example an Ultrasound machine would create data with the modality listed as US (Pianykh, 2012). These common abbreviations can be found in the introduction . After the images are created, depending on network type, they can be sent directly to the PACS servers, directly to the radiologists' workstation, or both. Workstations can either query the PACS server and receive data upon request or be pushed the data where it stores a small amount of data locally. This is a preference that is often dependent on the manufacturer and type of the workstation. Once the data reaches

the radiologists workstation, they will "read" it, essentially diagnosing the patient based on what he or she sees in the image. The doctor will then mark the image's areas of concern, and send the image to PACS post editing. This is used as reference for the patient's diagnosis report.

Common Network Topology

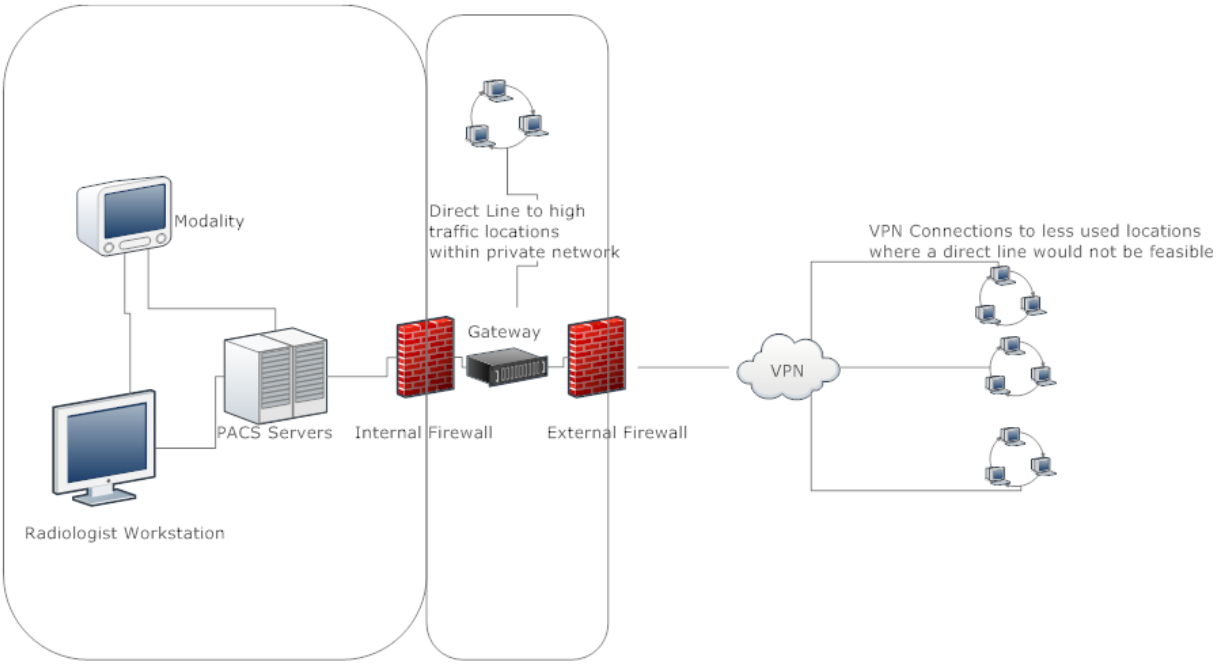

Figure 1.1

In Figure 1.1 you can see a simplified example of a very common topology for medical networks that exchange DICOM data regularly. The private network you can see on the left would be internal to the company, the modalities, PACS, and local reading workstations would all be located internally. This network would be located within one reasonable geographical location, however, it's not uncommon for this "local" network to be hard wired to many locations within one city. This network is often protected by an internal and external firewall as well as physical security within the practice limiting access to any network locations where patient data could be accessible. Within premises security is done by keeping only used ports active, and having extremely restricted wireless, or no wireless access at all. The firewalls are actively

filtering data, as well as monitoring network activity. Security compromise within the internal network, from the internal network, would most likely be a malicious insider, or a careless end user browsing the web. Although, within the private network, it is extremely uncommon for data to be encrypted in any area of transportation of its internal lifecycle, this leaves potential for information compromise if a hacker were able to enter the private network, data would be readily available (W. Dean Bidgood, 1997).

The second zone of the network topology in figure 1.1 is a commonly a separate, yet still private, network created by a wired connection accessible through a direct route through the gateway. This connection allows a high rate of throughput to high traffic locations. It is not uncommon for local hospitals to have connectivity to imaging locations through connections of this type. Security in this area is predominately a trust relationship between imaging locations and third party high use locations. Since your local internal network and WAN connection are an open flow of data, the infrastructure of both locations must be equally protected for data to remain secure since it is simply creating the potential for two weak points in the network topology.

The third area of the previous graphic is the most concerning of them all. This area is where an imaging location would have a VPN to exterior locations and referring physicians that send patients to have medical images created and read by radiologists' for use in diagnosis. The results of these cases are then sent over VPN to other locations, often with great geographical distance between. The VPNs are often more open than the usual VPN due to the fact that the referring physicians need to access a variety of items for billing, scheduling, reporting etc. This leaves a large gap in security. VPNs on the whole, are fairly secure, however, you are subjecting your network to the whim of many other locations security risks. This acts as a network risk

multiplier for each added VPN location, this is due to the fact that if a location, which your network is connected to, is compromised, it could leave your network at the hacker's whim simply because of how open it must be to allow the patient turn over to be efficient. This area is a perfect example of the accessibility vs. security paradigm, making it an essential evil with little area of improvement in security.

Archival

HIPPA mandates that all PACS systems and other systems that store DICOM data meet a certain level of security requirements. These requirements can be grouped into four major areas: Authentication, Authorization, Accountability, and Secure transfer. All of these requirements are to maintain secure and well documented environment for patient data. Archival and archive management is predominately in the hands of the PACS systems. Most commonly used PACS management software has all of the following functionality built in, which is then monitored and maintained (commonly) by a team of PACS administrators (CMT Medical Technologies).

Authentication is a familiar term in the IT world, and is no different in terms of PACS access. PACS administrators will determine access controls that determine where data is allowed to flow, as well as what users can read write or modify data. This is done commonly through the use of passwords in conjunction with email contact and release forms.

After a user is granted access, it is very important to allow the user to only view data he/she is authorized to see. Often many medical locations will have images stored on a singular PACS system, it is important that third party PACS users (referring physicians) only have access to data they are cleared to access, being able to access other locations data is done most often

through the signing of more release forms or out of pure necessity. Keeping in mind the data stored on these servers is patient medical information, this may need to be immediately accessed if a patient was in a dire emergency where data speed was critical, medical IT is subject to on the fly modifications to the typical commonalties. These on the fly decisions are often made on judgment calls of system administrators and PACS administrators alike.

Accountability is a mechanism that essentially as a log that contains all user interactions with different areas of patient information. This is used to make sure users are not escalating their own provides and monitoring user activity. If a user is suspected to have more access that what is needed for their role, you can use the accountability information to prove and remove that ability. This is also used to audit items. Auditing is useful for finding out if a technician or another end user may be doing a task incorrectly on purpose of by mistake. These logs can also be used by the PACS administrators to troubleshoot the lifecycle of patient information.

Secure transfer refers to the third area of figure 1.1. This encompasses the transmission of data leaving the local network. It is required that this information has been protected by appropriate security mechanisms.

(CMT Medical Technologies)

Common PACS server architecture

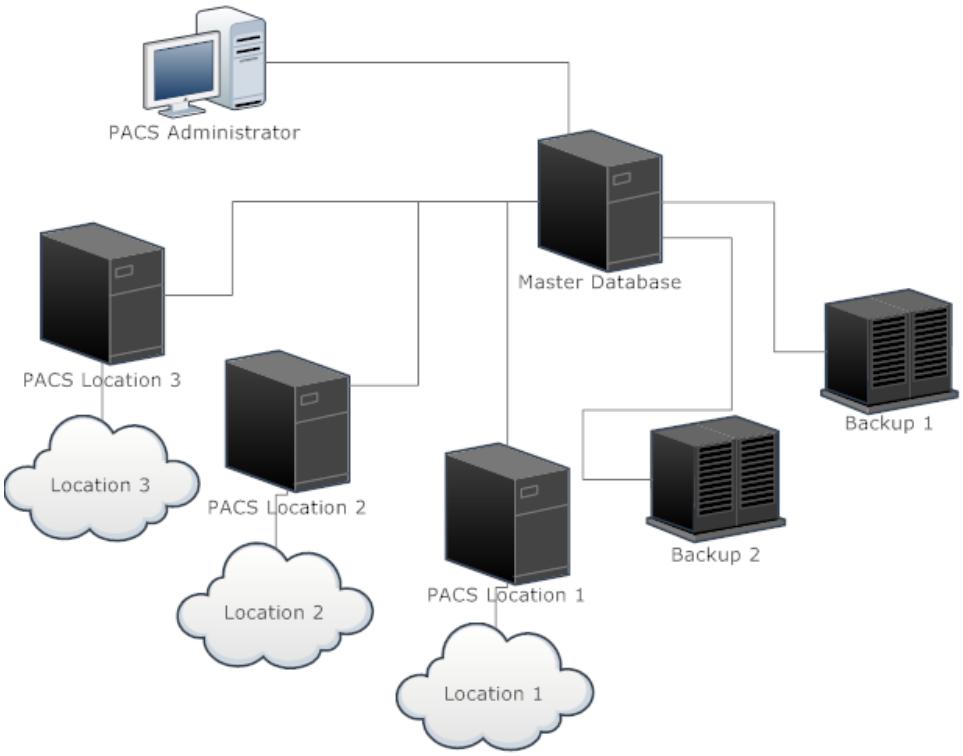

Figure 1.2

It is extremely common in PACS systems configuration to have one answering PACS server for each major high traffic location, while other smaller less frequent locations will piggy back onto the larger PACS servers. Once the sub-servers are populated with new information, it will then be sent to a master database that manages the long term storage of DICOM data. The master database (MDB) is usually a very robust system attached to some sort of redundant network storage. After the data reaches the MDB it will the populate the backup servers. These are usually of a similar level of robustness as the MBD, however these will often be located in other geographic locations. This location difference allows fault tolerance in the event of a larger data threatening events, such as tornados, flooding, etc (Wong).

Query and Retrieval

Q/R is the backbone of how patient images are retrieved by request. This is often done by a radiologist searching a patient's medical record number. This number known as an MRN then is formed into a request for the PACS server in question. This request is known as a C-FIND command. The PACS server then searches its massive databases to find the DICOM object with that particular MRN. C-FIND can be used to query the information listed in the DICOM objects' header. Once a C-FIND command returns positive results, the workstation will then issue a C-MOVE which then triggers a movement of the DICOM objects to either cached or stored long term on the workstation. These commands work the same way in every direction between the three main parts of the image lifecycle, the modality, the workstation and PACS. C commands move DICOM information, there are many more commands, however these two are used much more frequently than others. (Roni)

DICOM Header

The DICOM header is a block of text that describes the contents of a particular object. This area of information is used as the target for C-FIND commands. The header is divided into many individual fields that list various information based around the study and the patient that the image was generated to represent. It contains data such as; MRN, modality of origin, sex, birth date, referring physician, and the accession ID. Accession ID is an alphanumeric value that uniquely describes a single study. (Parisot, 2003)

Transportation

Under HIPPA regulation it is mandated that image data flow unimpeded through internal networks that are adequately protected with viable and effective firewalls (F. Cao, 2003). This means that all DICOM data that exists locally must be query / retrieved free of any non-medical modifications, this makes encryption of DICOM data only possible, in regards to HIPPA regulation, when transferring from network to network, or when transferring mediums.

Transport (Internal)

Local transportation, under HIPPA, would be considered everything done on your companies private network. This could be a modality, information moving to / from a workstation, and information moving in / out of the local PACS. This information is no encrypted and is transferred with few security measures. Transportation within the network is done through the implementation of something called an Application Entity Title, AE title for short. Essentially, an AE title is a hostname for DICOM sender and receivers. This is used in conjunction with IP addresses and a port that is open and ready to handle DICOM data. This data is used to make each entity aware of others that they will be sending to and entities they plan on receiving from. If an entity lacks an association, or has a miss configured association, any Q / R commands from the opposing entity will fail. Associations between AE's are confirmed with a command known as a C-ECHO. (Santesoft)

It is not uncommon to be able to issue C-FIND commands without having a fully associated level of communication, this leaves a potential void in security, even though this option only exists freely on the internal network. Any user with network access and software like NMAP would be able to find established DICOM entities simply by viewing open ports with a port sweep. Identifying AE 's could be done by comparing open ports to commonly used, or

default, DICOM Q / R ports such as 104, which is by far the most common. Issuing a C-FIND, with a common last name, to that AE and port would (semi) valuable information, such as patient full name DOB and other study related information. (Whitby, 2007)

Transport (External)

Transferring DICOM data out of your internal network over public space is a topic left up to most security officials within a company. This varies from practice to practice. This is accomplished most commonly as a classical VPN set up by IT security officials and systems administrators between two joining locations. Another way, although less common, is to have an ISP negotiated dedicated point to point connection to each location. Each choice leverages about the same security benefits, however, the personally facilitated VPN has more customization as well as more IT support overhead. (Johns Hopkins University)

To serve as a security multiplier on the previous two options, there is a "Digital Envelope" (DE) option which was created by researchers at the University of Southern California. The packaging of the DE occurs when exiting the creators' PACS with the intent of traveling over external networks. The DICOM data is taken, ran through an algorithm which then creates a unique digital signature for that particular image. The same algorithm then will create a rectangle around the image itself, it will then create a black space in the background in which the image signature will be imprinted on like a watermark. This data is then encrypted using public key cryptography, where only the intended PACS would have the private key. Upon arrival, the image is decrypted, the watermark is removed using a similar algorithm, and the original algorithm creates a signature once again. This second signature is used as a comparison with the first to insure data integrity (F. Cao, 2003). This process is displayed in the following graphic:

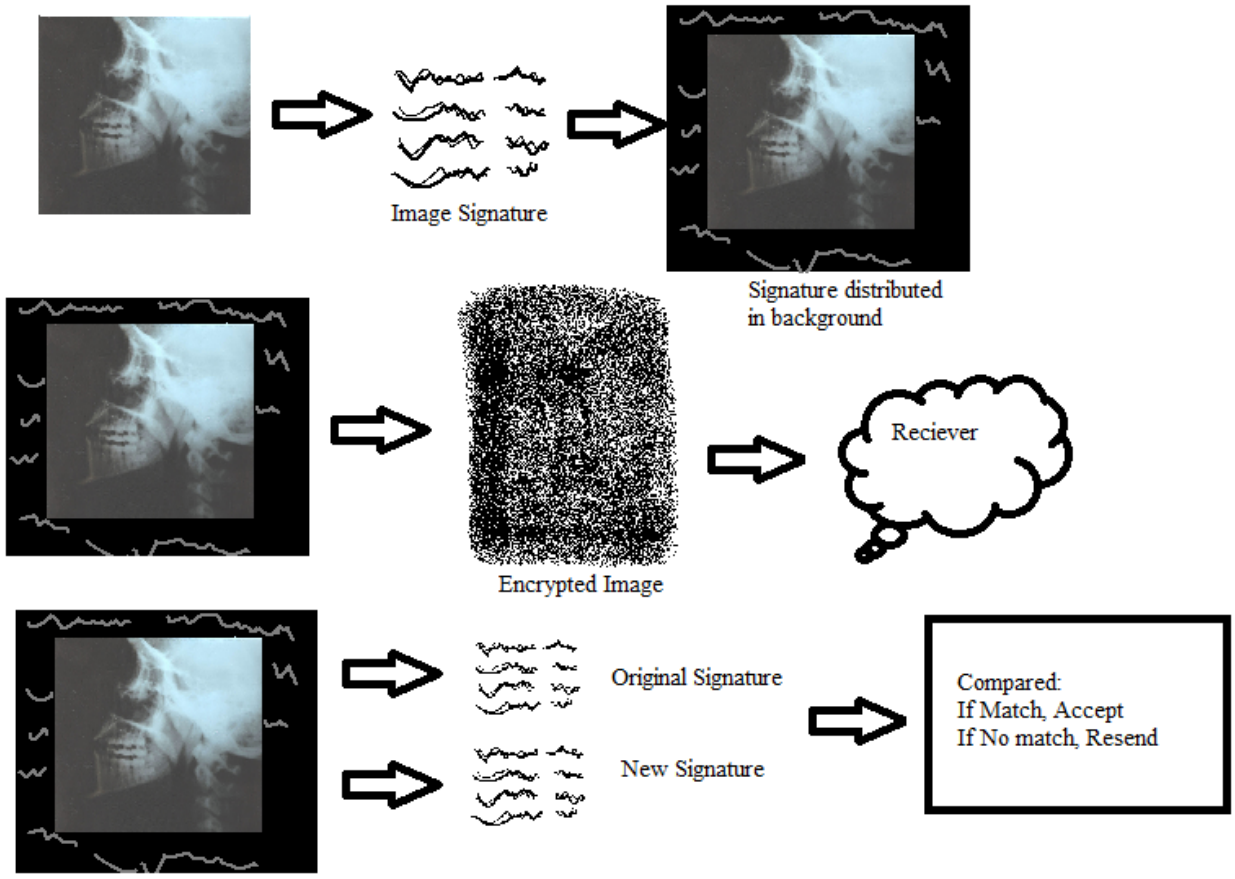

Figure 1.3 (F. Cao, 2003)

This option is also viable as a last resort if patient health is of immediate concern and VPNs or Point to Point links are down, as it could, theoretically be sent over public web with little risk.

Physical transport

Physical transport is a method used very frequently when seeing new patient who had prior studies done at a location that has no significance to the practice as a whole. For example, a patient could move from the west coast to the east coast that was recently found to have dense tissue in the left breast and needed to move as well as needed further examination. In cases like these, physical transport is the only feasible option most of the time. On a patients first visit to a new location, they will then have the new practice release a request for prior studies. This request will then be processed by the original practice, and the patients relevant prior studies will be

burnt onto a DVD. This DVD will then be mailed from location to location. Upon arrival the information is validated against the patients new information, and inserted into the PACS system to be viewed later by the radiologists.

DICOM data traveling by mail is essentially the same thing as DICOM data traveling over public networks, and should be treated like such, however it currently is only being treated like this by a few practices. The few locations that do implement securing their patients DVDs do so by encrypting the disk using encryption programs like True crypt. Upon sending the DVD, they will verbally share the password over the phone, allowing only the two parties to know the password to unlock the DICOM data on the disk. This is by far the more secure method of transferring DICOM data via mail, it can cause burden to each practice in the form of time spent getting data from the disk (or installing the desired decryption software), however it adds leagues of security to the ever valuable patient data.

Works Cited

CMT Medical Technologies. (n.d.). *HIPAA Compliance*. Retrieved 11 15, 2013, from http://www.cmt-med.com/site/english/dicom/hipaa.asp: http://www.cmt-med.com/site/english/dicom/hipaa.asp

F. Cao, H. H. (2003). Medical image security in HIPPA mandated PACS environment. *Computerized Medical Imaging and Graphics* , 185-196.

Johns Hopkins University. (n.d.). *DICOM Security.* Retrieved 11 15, 2013, from http://cs.jhu.edu/: http://cs.jhu.edu/~sdoshi/jhuisi650/papers/dicomsecuritychap11.pdf

NEMA. (n.d.). *http://medical.nema.org/.* Retrieved 11 15, 2013, from Digital Imaging and Communications in Medicine (DICOM): Part 1: Introduction and Overview: http://medical.nema.org/Dicom/2011/11_01pu.pdf

Parisot, C. (2003). The basic structure of DICOM. *SSRPM* , 1-39.

Pianykh, O. S. (2012). *Digital Imaging and Communications in Medicine: A practical introduction and survial guide.* Boston Massachusetts: Springer.

Roni. (n.d.). *dicomiseasy.blogspot.com*. Retrieved 11 15, 2013, from DICOM is Easy: http://dicomiseasy.blogspot.com/

Santesoft. (n.d.). *Medical Imaging software*. Retrieved 11 15, 2013, from www.santesoft.com: http://www.santesoft.com/howto/network.html

W. Dean Bidgood, J. M. (1997). Understanding and Using DICOM, The data interchange standard for biomedical imaging. *J AM Med Information Associates* , 199-212.

Whitby, J. (2007). The DICOM Standard. *Barco: White Paper* , 1-14.

Wong, E. (n.d.). *PACS Introduction.* Retrieved from pacs.hk: www.pacs.hk/Doc/MIIAExam/PACS%20introduction.ppt