Fall 2018

Secure Integration of Information Systems in Radiology

Stephen A. Clark
sclark8890@gmail.com

Secure Integration of Information Systems in Radiology

Stephen A. Clark

BIS 437 Murray State University

Abstract

Medical Imaging is an industry where distinctive imaging protocols such as Digital Communications in Medicine (DICOM) and Health Level 7 (HL7) are used to transmit patient data across multiple information systems relaying possible life-saving data their providers. These information systems, unique to radiology departments require proper integration and workflow to achieve the CIA triad of confidentiality, integrity, and availability. This paper discusses the challenges of integrating disparate healthcare radiology information system with particular emphasis on protocol security.

Table of Contents

Abstract 2

Secure Integration of Information Systems in Radiology 4

Introduction 4

Background .... **Error! Bookmark not defined.**

DICOM 6

Network Security for DICOM. .... **Error! Bookmark not defined.**

Modality Security. 12

Outsourced DICOM System Security 37

DICOM Storage. 44

PACS Security. 50

DICOM Conclusion. .... **Error! Bookmark not defined.**

HL7 12

HL7 Interface Security. 17

HL7 Security Countermeasures. 22

Risk Management and Security Assessment of DICOM and HL7 15

References .... **Error! Bookmark not defined.**

Secure Integration of Information Systems in Radiology

Introduction

In the past medical imaging within medical facilities and hospital radiology departments was accomplished by expensive films that were secured in a fireproof room or cabinet. Medical records consisted of paper documents that were kept in a fireproof storage. Networking, telemedicine, and any electronic communication besides the utilization of a landline or a fax machine for results of examinations was not an option. Having availability to transfer these medical records and films was through a physical method such as US Mail or courier. These methods did not provide access to quick patient care. However, data integrity and confidentiality remained intact for the life of the record. Stealing or altering a mass number of physical documents was near impossible and unthought of. The same private data was stored physically then as it is now stored digitally. While this may be true, nobody hacked the film library and sold that data on the dark web. Nowadays advances in technology have allowed information systems to become the backbone of the radiology department by increasing availability, but in other respects the implementation of such technology has increased the risk of loss to confidentiality and integrity. How did the availability of medical records within radiology become priority over the other two parts of the CIA Triad? To find that answer we must step back several decades.

While the medical imaging technology advanced; the increase usage of computers found their place in the healthcare industry. As vendors developed applications for the healthcare industry the need increased for a simple method of electronic communication that did not require significant overhead. Computers and software applications proved to be beneficial for patient care but transferring data from one computer system to another was an issue yet to be resolved.

During the early 1980s, medical imaging started to become a valuable resource in healthcare. Manufacturers of the medical imaging equipment could not communicate with each other. Disconnected silos of data grew due to the vendors grasping the concept of having connection between clinical systems, but the method of communication varied from system to system. Proprietary communication methods were used by the manufactures leaving health care facilities unable to integrate or network these devices. Medical imaging was no different from the innovation path of the personal computer and the Internet. Standardization was required if the new technology was going to flourish and become a widely accepted practice in healthcare. Subsequently, the new technologies remained partly isolated for over a decade.

In the 1990s and early 2000s, innovation within the medical imaging and healthcare applications created a new digital imaging industry. The urgency for more integration increased and therefore a centralized information system protocol for radiology was required to achieve an efficient workflow between the legacy imaging systems. As a result, healthcare facilities purchased expensive digital imaging equipment to provide better patient care, and so the facility would have to find an expense to cut. Because of the modernization in the industry there become a need for a centralized storage and viewing system of the radiology images. Picture Archive and communication systems (PACS) offset the cost of the digital imaging equipment by supporting the storage, transmittal, and retrieval of radiology images. PACS removed the need to print film and saved organizations money and offset the expense of the new imaging equipment purchases.

By the late 2000’s paper medical records and medical images on physical film was fading away from modern healthcare. During this time of modernization and growth, information security was not the focus of both the vendors nor the healthcare facilities. Improved cost savings and availability of clinical data was the main focus for application developers and healthcare facilities. Unfortunately, the result was that the foundational standards and protocols were developed without any regard to security. The technology in radiology expanded and became more widely implemented; the gap in integration got wider.

Prior to the technological gains in healthcare, application developers and standards organizations began discussions on how to allow free and open communication between their products. Their concentrated efforts focused on solving the communication and integration problems with little or no priority on application or network security. Two standards formed out of these discussions that transformed how radiology functions today, Digital Imaging and Communications in Medicine (DICOM) and Health Level 7 (HL7).

DICOM

The American College of Radiology (ACR) and National Electrical Manufacturers Association (NEMA) allied to help alleviate the communication problems between medical imaging devices. These two organizations worked closely with manufacturers to create the standard in medical imaging known as DICOM.

According to NEMA the protocol known as DICOM was created for three reasons:

- Encourage communication of digital image information, from all the device manufacturers.
- Create a technology ecosystem where the development of PACS and allow medical providers the ability to interface with other information systems within healthcare.
- Structure a base technology for a diagnostic imaging database that would have the potential to span global networks and encourage data mining to improve medical research.

Since the inception of DICOM, the landscape of healthcare has advanced. Standardizing digital imaging has played an essential role in modern medicine. DICOM has become the universal standard protocol for medical imaging. The protocol allows the data transfer, storage, and display of digital medical imaging (Pianykh, 2008). According to (Baxter & Zeleznik, 1983) not only did standardization resolve compatibility issues between vendors but also solved complex issues such as archiving and retrieving to centralized vendor-neutral storage.

DICOM was developed to solve incompatibility issues between disparate digital medical imaging system and has become the technological foundation for many advances in patient care. However, the DICOM protocol itself does not provide a secure environment or vehicle to communicate patient data.

Dicom Workflow

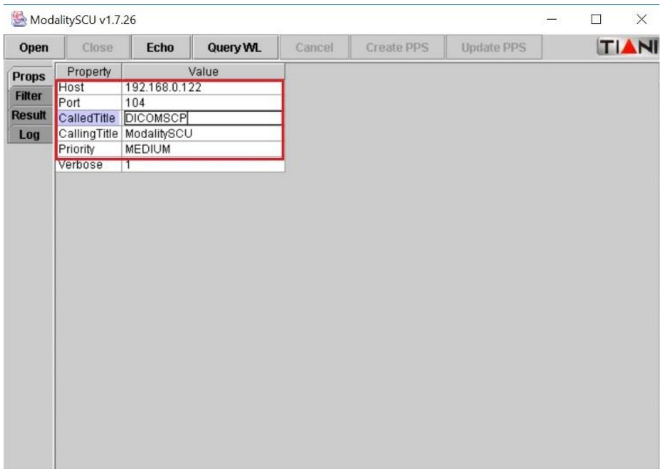
A review of how DICOM functions is necessary before examining the security issues that exists with the protocol. In radiology, there are various medical imaging devices called modalities. The modality can be a Computer Tomography (CT), Ultrasound (US), Magnetic Resonance Imaging (MRI), or Nuclear Medicine (NM). All modalities perform similar functions; to scan the body and provide a diagnostic overview of the patient to a physician. Before standardization, it was difficult at times to view a diagnostic study on another workstation, even when the study was created on a device by the same vendor. This kind of instability in digital imaging products is what paved the road for DICOM to be created and agreed upon to be the standard of the industry.

In 1999 in response to the newly passed Health Insurance Portability and Accountability Act (HIPAA) regulation, that implemented laws on Personal Identifiable Information (PII) is managed in modern healthcare information systems, the DICOM standard included options for encryption and data protection during network transmission. Security was expanded again in 2001, when the DICOM standard included Cryptographic Message Syntax (CMS). The purpose of CMS was to encrypt portions of the DICOM object header which stored patient data. Unlike prior security changes in the standard, this one allowed the data to be encrypted through the data lifecycle. It is noted in the documentation of the standard, that patient data encryption is supported but not mandated. A method of encryption can be used is defined, but the patient data encryption implementation is the responsibility of the healthcare facility and DICOM vendors. This made it easier for vendors and the owners of the DICOM data to apply encryption to the data. (Medema, Horn, & Tarbox).

However, the medical imaging industry is made up of multiple vendors, and a single Radiology department could have various vendors for the modalities, PACS, printers, and other related DICOM devices. If one was to look at the purpose of DICOM, it was to standardize a method of communication because no single vendor could agree on how to create cross compatibility DICOM functionality. If the vendors could not agree on an industry standard to network and communicate until they were mandated, then the security of the communication should not be handled any differently.

DICOM is the format and encoding of how electronic communications function within a PACS, although vendors can have various interpretations of the protocol. Vendors of DICOM information systems create documentation known as a conformance statement that detail how the software will interconnect to other DICOM interfaces. How does DICOM differ from other communication protocols?

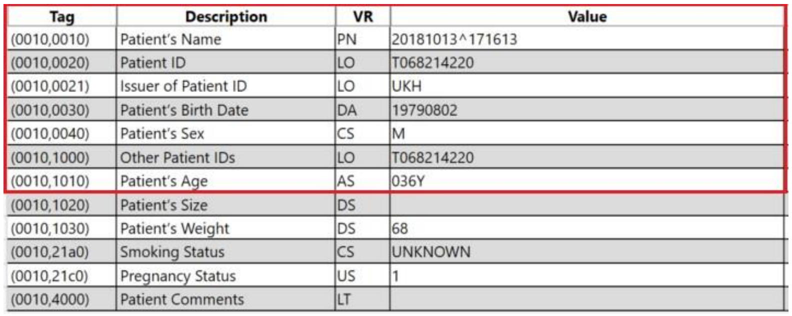
DICOM entails various components that allow the communication to take place. What is known as an Application Entity (AE) title must be assigned for each system that needs to communicate with DICOM compliant devices (Branstetter, 2009, p. 84-86). An AE title is not specific to a server or workstation but software running on the device, by the way of comparison, the AE title is comparable to a hostname but has a limitation of sixteen characters and a workstation or server can have multiple AE titles running on the same port and IP Address. The AE title should define what type of function of DICOM it is serving. (Pianykh, 2008, p. 116-118). For example, Fig 1 shows a typical DICOM configuration on a modality.



Property	Value
Host	192.168.0.122
Port	104
CalledTitle	DICOMSCP
CallingTitle	ModalitySCU
Priority	MEDIUM
Verbose	1

Figure 1. Modality Configuration Example.

One of the first steps of the workflow in a Radiology department is the image acquisition that takes place on a modality. The digital images are stored in a DICOM format and then usually transmitted over Transmission Control Protocol (TCP) port 104, which is the common TCP port used for DICOM. For a DICOM network transmission to take place an agreement between the communicating devices must take place. During the agreement outlined in the DICOM standards each modality type has a Service-Object Pair Class (SOP Class) that defines items such as storage, encoding, and presentation of the diagnostic images (Mildenberger, Eichelberg, & Martin, 2001). During the acquisition of the DICOM files there is an encoding process that contains metadata about the digital imaging examination. This data is known as the DICOM tags. The data categories are broken down into elements using a hexadecimal numbering system for identification. For example, the patient’s date of birth (DOB) is element (0010, 0030). This is the DICOM standard place for the patient DOB to be inserted into the DICOM files (Pianykh, 2008, p. 42). As an illustration Fig 2 displays an example of the portion of the DICOM header that contains the patient demographics.



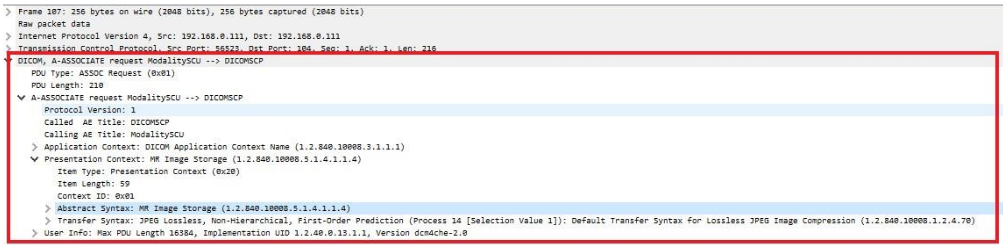
Tag	Description	VR	Value
(0010,0010)	Patient’s Name	PN	20181013^171613
(0010,0020)	Patient ID	LO	T068214220
(0010,0021)	Issuer of Patient ID	LO	UKH
(0010,0030)	Patient’s Birth Date	DA	19790802
(0010,0040)	Patient’s Sex	CS	M
(0010,1000)	Other Patient IDs	LO	T068214220
(0010,1010)	Patient’s Age	AS	036Y
(0010,1020)	Patient’s Size	DS	
(0010,1030)	Patient’s Weight	DS	68
(0010,21a0)	Smoking Status	CS	UNKNOWN
(0010,21c0)	Pregnancy Status	US	1
(0010,4000)	Patient Comments	LT	

Figure 2. DICOM Tags Containing Pateint Demographics.

Of course, this data has been anonymized, but as shown in figure 2, DICOM files, contain multiple pieces of personal identifiable information and the data is not just stored directly on the modality. The next section discusses the complexity of DICOM network storage and communications.

Another goal of DICOM is to provide a standard for diagnostic imaging devices to communicate. The DICOM standard supports the Transmission Control Protocol/Internet Protocol (TCP/IP) protocol suite’s network transport services. These services are the method that data is transmitted between the information systems. The Storage Class Provider (SCP) is the storage device such as a PACS or Vendor Neutral Archive (VNA). The Storage Class User (SCU) is the medical imaging device itself, which is the device acquiring the diagnostic images and initiating the network communication. These roles can be reversed and are interchangeable. The SCP is not always the storage device and the SCU is not always the imaging device (Mildenberger, Eichelberg, & Martin, 2001).

The association handshake is much like the TCP/IP three-way hand shake process. The packet headers contain information about the Application Context, Presentation Context, Abstract Syntax, Transfer Syntax, and User Information, which contains information about the DICOM devices communicating (Pianykh, 2008, p. 182-18). The packets involved in the handshake process is referred to the DICOM Association Request (A-Association-RQ) for requesting the communication, the request is followed by the DICOM Association Acceptance (A-Association-AC) for acceptance of the request. In Fig 3 the packet capture displays an DICOM Association request transfer syntax is occurring between a SCU and SCP.

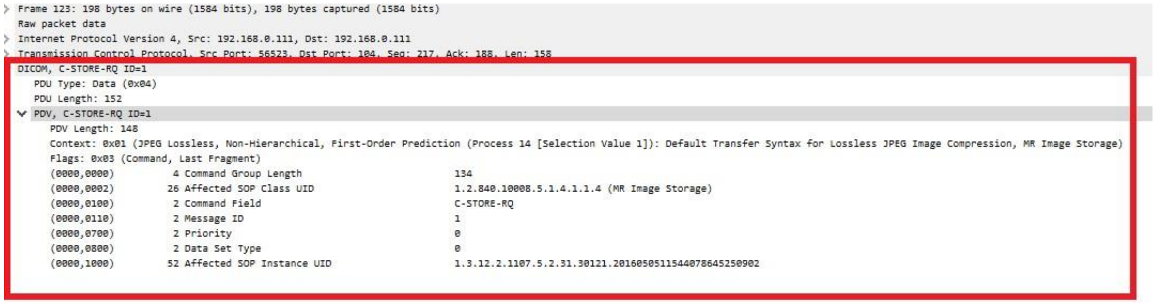


```
> Frame 107: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.111
> Transmission Control Protocol, Src Port: 56523, Dst Port: 104, Seq: 1, Ack: 1, Len: 216
v DICOM, A-ASSOCIATE request ModalitySCU --> DICOMSCP
    PDU Type: ASSOC Request (0x01)
    PDU Length: 210
  v A-ASSOCIATE request ModalitySCU --> DICOMSCP
      Protocol Version: 1
      Called  AE Title: DICOMSCP
      Calling AE Title: ModalitySCU
    > Application Context: DICOM Application Context Name (1.2.840.10008.3.1.1.1)
    v Presentation Context: MR Image Storage (1.2.840.10008.5.1.4.1.1.4)
        Item Type: Presentation Context (0x20)
        Item Length: 59
        Context ID: 0x01
      > Abstract Syntax: MR Image Storage (1.2.840.10008.5.1.4.1.1.4)
      > Transfer Syntax: JPEG Lossless, Non-Hierarchical, First-Order Prediction (Process 14 [Selection Value 1]): Default Transfer Syntax for Lossless JPEG Image Compression (1.2.840.10008.1.2.4.70)
    > User Info: Max PDU Length 16384, Implementation UID 1.2.40.0.13.1.1, Version dcm4che-2.0
```

Figure 3. DICOM Association Request.

At the end of the communication the connection is tore down in a similar method. The DICOM Association Release (A-Release-RQ) and the reply will be a DICOM Association Release Response (A-Release-RP). If the connection terminates abruptly a DICOM Association Abort (A-Abort) message is transmitted (Pianykh, 2008, p. 205).

In addition to the SOP Class which is not negotiable. The SCP either will except or reject the SOP Class. During the DICOM association the SCU and SCP will agree on an encoding format known as the Abstract Syntax. The compression ratio of which the diagnostic images will be transmitted and received is agreed upon in the association known as the Transfer Syntax. (Pianykh, 2008, p. 187-188). The Transfer Syntax plays a significant role in the DICOM network and storage. A diagnostic image that is compressed will transfer more efficiently over a network and will take less disk space so that quicker patient care is achieved and lowering the overhead to the providers, respectively. The overall process of storing diagnostic images to a DICOM compliant device is known as C-Store (Veeramani, Masood, & Sidhu, 2014). An example of a packet capture containing a C-Store request for the SOP Class UID for an MRI study is in Fig 4.

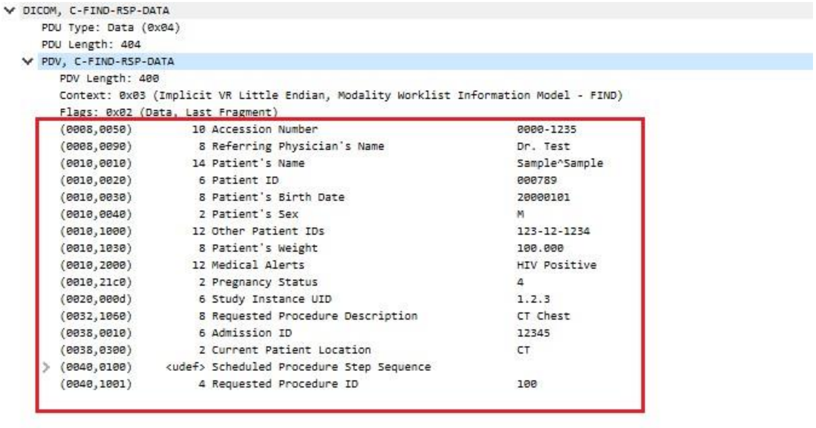


```
> Frame 123: 198 bytes on wire (1584 bits), 198 bytes captured (1584 bits)
  Raw packet data
> Internet Protocol Version 4, Src: 192.168.0.111, Dst: 192.168.0.111
> Transmission Control Protocol, Src Port: 56523, Dst Port: 104, Seq: 217, Ack: 188, Len: 158
  DICOM, C-STORE-RQ ID=1
    PDU Type: Data (0x04)
    PDU Length: 152
v   PDV, C-STORE-RQ ID=1
      PDV Length: 148
      Context: 0x01 (JPEG Lossless, Non-Hierarchical, First-Order Prediction (Process 14 [Selection Value 1]): Default Transfer Syntax for Lossless JPEG Image Compression, MR Image Storage)
      Flags: 0x03 (Command, Last Fragment)
      (0000,0000)         4 Command Group Length                    134
      (0000,0002)        26 Affected SOP Class UID                  1.2.840.10008.5.1.4.1.1.4 (MR Image Storage)
      (0000,0100)         2 Command Field                           C-STORE-RQ
      (0000,0110)         2 Message ID                              1
      (0000,0700)         2 Priority                                0
      (0000,0800)         2 Data Set Type                           0
      (0000,1000)        52 Affected SOP Instance UID               1.3.12.2.1107.5.2.31.30121.2016050511544078645250902
```

Figure 4. DICOM C-Store Request.

One crucial step in the DICOM workflow is a technology named DICOM Modality Worklist (DMWL). Consequently, the integrity of downstream data is dependent upon this step in the workflow. The primary function of the DMWL is to automate the registration of the patient on the SCU in an efficient error free process. Many providers experience high patient volumes and the data entry requires precision to prevent potential medical errors (Mann & Bansal, 2014).

The DMWL is the step prior to the acquisition of the images and should be implemented to maintain data integrity. The DMWL is hosted by the SCP and a C-FIND DICOM message is sent from the SCU. In return the SCP will send the list of scheduled examinations and patients for the technologist to select from. DICOM elements mentioned in the paragraph above help the SCP and SCU communicate the information queried for in the C-FIND message. An example of a C-FIND response containing patient data within a packet capture is seen in Fig 5.



```
v DICOM, C-FIND-RSP-DATA
    PDU Type: Data (0x04)
    PDU Length: 404
  v PDV, C-FIND-RSP-DATA
      PDV Length: 400
      Context: 0x03 (Implicit VR Little Endian, Modality Worklist Information Model - FIND)
      Flags: 0x02 (Data, Last Fragment)
      (0008,0050)       10 Accession Number                     0000-1235
      (0008,0090)        8 Referring Physician's Name           Dr. Test
      (0010,0010)       14 Patient's Name                       Sample^Sample
      (0010,0020)        6 Patient ID                           000789
      (0010,0030)        8 Patient's Birth Date                 20000101
      (0010,0040)        2 Patient's Sex                        M
      (0010,1000)       12 Other Patient IDs                    123-12-1234
      (0010,1030)        8 Patient's Weight                     100.000
      (0010,2000)       12 Medical Alerts                       HIV Positive
      (0010,21c0)        2 Pregnancy Status                     4
      (0020,000d)        6 Study Instance UID                   1.2.3
      (0032,1060)        8 Requested Procedure Description      CT Chest
      (0038,0010)        6 Admission ID                         12345
      (0038,0300)        2 Current Patient Location             CT
    > (0040,0100)   <udef> Scheduled Procedure Step Sequence
      (0040,1001)        4 Requested Procedure ID               100
```

Figure 5. DICOM C-FIND Containing Patient Demographics.

The information in these prepopulated elements contain the patient demographics and facility information that was derived from the HL7 ORM received by the SCP (Kartawiguna & Georgiana, 2014). Granted, this DMWL is the step prior to acquisition of the images it would not be possible without the help of the protocol known as HL7.

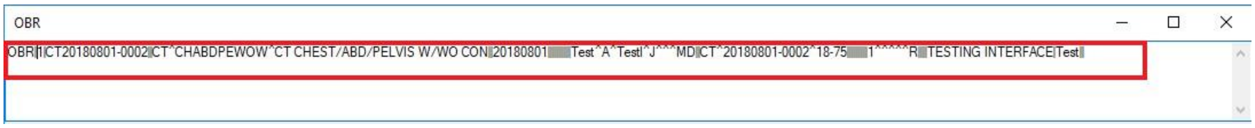
HL7

Patient safety, data integrity, and cost savings is primary factors that drive the healthcare industry to improvements in system integration. Health Level 7 (HL7) was developed to set a standard in the way information systems in healthcare can communicate. The integration between information systems in healthcare using HL7 has reduced patient errors and saves time of data entry into multiple systems (Al-Enazi & El-Masri, 2013). With the various persons, devices, and networks that interact with one another to achieve good patient care. The patient care can span across enterprise networks and multiple healthcare organizations. This is part of the reasoning behind HL7 (Oemig & Snelick, 2016, p. 1-9).

HL7 Workflow

For reference, it is important to understand what confidential information is within a HL7 message. HL7 messages are broken down into three categories, Order Message (ORM), Order

Result (ORU), and Admission, Discharge, and Transfer (ADT), that are defined in the header of the HL7 message (Branstetter, 2009, p. 89-90). The structure of a HL7 message is broken down into data fields separated by a pipe "|" and each HL7 message either it is an ORM, ORU, or ADT will have segments that contain information about the patient and examination (Pianykh, 2008, p. 302-303). This is illustrated in Fig 6.



```
OBR|1|CT20180801-0002|CT^CHABDPEWOW^CT CHEST/ABD/PELVIS W/WO CON|20180801[redacted]Test^A^Testl^J^^^^MD|CT^20180801-0002^18-75[redacted]1^^^^^^R|TESTING INTERFACE|Test|
```

Figure 6. HL7 OBR Segment.

Notice that within this OBR section of the HL7 message that the patient name and examination data is within this segment. In most instances, these messages are lengthy and contain highly confidential data. The example in Figure 6 is more to give an example of the structure of the HL7 message and the content will be discussed later in this writing.

When an order is placed for a Radiology examination the sending system in the HL7 interface will transmit what is known as an ORM to the PACS HL7 broker which contains information about the scheduled procedure. After the patient is entered into the sending system of the interface there may be the need to update the patient information or status at the medical facility and in these scenarios an ADT message will be transmitted to the PACS. After the results of the examination is completed in PACS or the accompanying reporting system an ORU message is triggered, thereby transmitting the results to the EMR. (Branstetter, 2009, p. 90-91).

At the beginning of the workflow patient demographics and private information gets entered into the information systems such as an EMR. The workflow begins when the referring physician orders a diagnostic imaging examination, whereas the data is entered into information systems during the registration process. With that in mind, this is a significant step within the workflow, mainly because this data will flow downstream to information systems, causing the electronic medical record and related databases to get populated with the registration data. In most cases, this process takes place in a Hospital Information System (HIS) and the HIS will transmit what is known as a HL7 message to the RIS or PACS.

Risk Management and Security Assessment of Radiology

Hardening clinical systems while allowing fast access and transmission to the data has segmented the healthcare industry from other public sectors such as finance and manufacturing regarding how data is secured. Securing the Radiology network is one thing but keeping the software and hardware stable after the hardening is completed is another. Often the responsibility securing systems such as PACS or modalities is assumed but not defined that either the vendor or healthcare facility. This type of misunderstanding leads to vulnerabilities that are trivial for an attacker to exploit.

In recent years, several healthcare facilities have fallen victim to cyber-attacks. Since personal identifiable information (PII) within electronic medical records are worth more than banking or credit card data. It is no wonder how large health care operations such as MedStar Health, the largest non-profit health care system in the United States, is a more attractive victim than financial companies.

Another type of attack that is becoming a common buzzword in news reports is ransomware, in which the attacks have encrypted information systems and the only way to unencrypt the data was for the owner to purchase the encryption key from the hackers. With this in mind, hackers successfully installed Ransomware on information systems at MedStar Health facilities and took ten hospitals and a couple hundred outpatient clinics offline in 2016 (Ragan, 2016). Medstar was not the only healthcare facility to fall to threat actors that used Ransomware. In 2017, Erie County Medical Center was hit with what is known as the SamSam ransomware. In this case it took over a million dollars and a total of six weeks to fully recover from this attack (Davis, 2018). In fact, threat actors used the SamSam ransomware that targeted healthcare servers utilizing the protocol Remote Desktop Protocol (RDP). The attackers used brute force to gain access to the systems running RDP. On the dark web these RDP credentials were put up for sale and allowed anyone who was willing to pay would gain access to the compromised RDP systems (Gibson, 2018). Keep in mind that RDP is a method that vendors of DICOM and HL7 software provide remote support to servers and workstations to customers. This type of attack clearly compromises the structure of the support models provided by vendors.

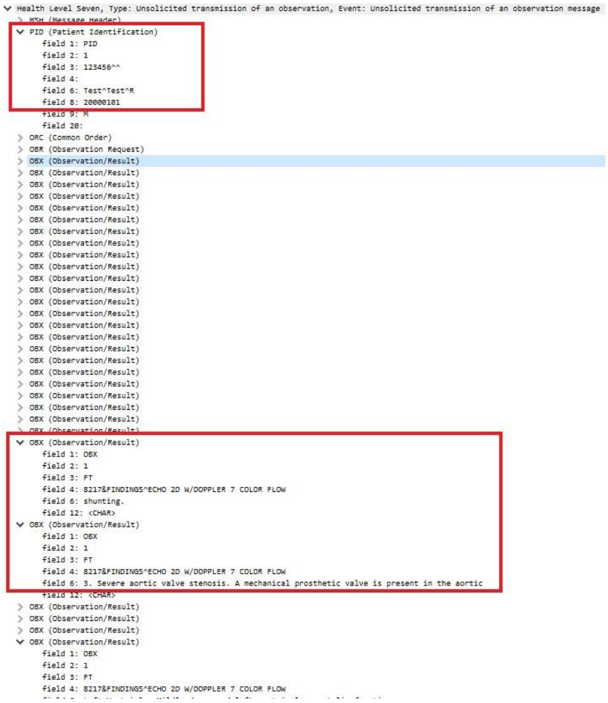
These recent attacks against healthcare have demonstrated how valuable the data on systems such as PACS is. To illustrate how common these attacks are becoming, the report by Protenus in 2016 documented over four hundred and fifty breaches were reported to HHS or to the media. These incidents compromised the integrity and confidentially of over twenty-seven million patient records that were affected by these security incidents. Surprisingly, forty three percent of the breaches were caused by unintentional actions of employees, but more than half of the breaches were deliberate attacks.

How did Radiology evolve into one of the highest revenues generating departments for the healthcare industry while simultaneously become a threat vector for cyber-attacks? For decades security has been laxed in healthcare mainly around distinct protocols such as DICOM and HL7. Both protocols are the primary data flow for a Radiology department. Securing the protocols and methods of communication is key in protecting patient data. Security through obscurity with these protocols can no longer be achieved. Hackers have realized that HL7 and DICOM is transmitted in clear text. They know that the modalities are not secure and can be easily compromised to provide a doorway into the network that runs on HL7 and DICOM.

Proper steps must be taken to protect patient data from inside and outside threats. A solid risk management framework can help prevent such attacks. Before a risk management framework can be implemented for DICOM, HL7, Modalities, PACS, and outsourced radiology services vulnerabilities and security controls must be identified. Towards this goal, we must first explore additional vulnerabilities, exploits, and mitigations.

HL7 Security

HL7 messages are transmitted over a TCP/IP network connection over a predefined port between the sender and receiver, and the connection is referred to as a HL7 interface. This type of transmission is taking place over the network in clear text and this creates a security issue for the protocol (Auger & Cardinal). Evidently, this leaves the patient data vulnerable for packet capture as noted in the figure 7 below that displays an ORU message that was transmitted from a PACS reporting module to an EMR.



```
v Health Level Seven, Type: Unsolicited transmission of an observation, Event: Unsolicited transmission of an observation message
  > MSH (Message Header)
  v PID (Patient Identification)
      field 1: PID
      field 2: 1
      field 3: 123456^^
      field 4:
      field 6: Test^Test^R
      field 8: 20000101
      field 9: M
      field 20:
  > ORC (Common Order)
  > OBR (Observation Request)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  v OBX (Observation/Result)
      field 1: OBX
      field 2: 1
      field 3: FT
      field 4: 8217&FINDINGS^ECHO 2D W/DOPPLER 7 COLOR FLOW
      field 6: shunting.
      field 12: <CHAR>
  v OBX (Observation/Result)
      field 1: OBX
      field 2: 1
      field 3: FT
      field 4: 8217&FINDINGS^ECHO 2D W/DOPPLER 7 COLOR FLOW
      field 6: 3. Severe aortic valve stenosis. A mechanical prosthetic valve is present in the aortic
      field 12: <CHAR>
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  > OBX (Observation/Result)
  v OBX (Observation/Result)
      field 1: OBX
      field 2: 1
      field 3: FT
      field 4: 8217&FINDINGS^ECHO 2D W/DOPPLER 7 COLOR FLOW
```

Figure 7. Packet Capture of an HL7 Message Containing Patient Demographics.

It is obvious why this type of was a topic of conversation at Black Hat in 2018, which will be discussed in more detail later. It is well known that data integrity of the HL7 data feed is of high importance as the information within the EMR and other information systems such as PACS and RIS contains data that is pertinent to the clinical decisions for the health of the patient. As you can see in the example packet capture above confidential information, such as patient demographics and clinical outcomes, is transmitted in clear text. A packet capture such as this illustrates that HL7 does not have encryption at the protocol level.

Within the HL7 standard it is assumed that encryption will occur behind the application layer of the OSI model. With HL7 there are no checksums to determine if the message was altered in transit (Dameff, Bland, Levchenko, & Tully, 2018). Not only does HL7 lack encryption or checksums to provide confidentiality and data integrity there is a lack of authentication, opening the door for an attacker who discovers the HL7 ports being used they could easily capture a mass amount of PHI (Haselhorst, 2017). This type of vulnerability increases the risk of a man in the middle or data exfiltration attack, due to the face that the HL7 feeds contain a plethora of patient data because every detail about the patient and care received is distributed across an HL7 interface at some point.

HL7 Vulnerabilities and Exploits.

As discussed earlier, HL7 is usually transmitted over the network in clear text and is susceptible to multiple types of attacks. By design HL7 transfers patient data between clinical systems, and once the data is received it is usually securely stored in databases. In breaches with the financial industry the databases and documents are what holds the information that hackers seek, this is not necessarily true in healthcare. With regard to HL7, the data of value is going across the network, unencrypted and without authentication, and any exfiltration of the data is near untraceable. Of course, the security mitigation offered by some in the industry is that a hacker must be on the network to accomplish these types of attacks (Auger & Cardinal, 2018). Considering this, insider threats must be reviewed.

Nation states and hacker groups are not the only threat actor to Radiology departments, employees are becoming the source of breaches. Unfortunately, these types of attacks are difficult to prevent and, at times, detect. For example, in a report by CERT seventy five percent of all insider attacks go unnoticed (HIPAA Journal, 2018). In another survey by Accenture one if five healthcare employees would sell patient data if the price was right and within that same survey showed that twenty four percent said they had knowledge of a co-worker selling their credentials to an outsider group (Accenture, 2018). Like unsecured modalities, insiders provide a threat vector onto the network where HL7 is transmitted in unencrypted form without any checksums to prevention from being exfiltrated. As detailed below, there are documented security incidents with HL7 interfaces.

Black Hat 2018.

At the Black Hat conference in August 2018 four of the speakers simulated a man in the middle attack that altered a patient's results in an ORU message leading to the patient's death. As illustrated in Figure 7, the ORU message is where the clinical diagnosis is communicated between clinical information systems.

In the simulation of the man in the middle attack the group altered the findings in the ORU message segment by altering the diagnosis and by doing so gave the perception to the ordering provider that the patient needed clinical treatment for a wrong diagnosis. Consequently, the patient in the scenario died due to the loss in data integrity in the HL7 message.

The demonstrated attack showed that HL7 can be easily changed undetected, due to the fact that the hospital systems are on a paperless system and any physical record of what the medical record was supposed to contain would already be destroyed by the time the error in the electronic data would be realized (Auger & Cardinal, 2018). Remember, the HIPAA Security clause states that

> …Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.

These findings at Black Hat directly show that the widely used protocol of HL7 no longer meets the technical safeguard requirements for HIPAA.

Even though sniffing the data is a huge risk to confidentiality and integrity of the data there are other risk factors in regard to HL7. The following two examples deal with a vendor configuration error that compromised data and how human error in data entry can incidentally cause patient safety issues.

Middletown Medical.

In early 2018 at Middletown Medical Center in New York, NY a misconfigured Radiology HL7 interface exposed over sixty-three thousand patient records, that including patient name, date of birth, internal medical record numbers, billing information, and medical history, exposed directly to the Internet. The facility nor the vendor was unable to determine how long the interface was openly exposed to the Internet and if any patient data was compromised (Davis, 2018).

In this case, the vendor failed to ensure that the configuration of a HL7 interface was secured on both the hospital and vendor sides of the connection. Although, this is not an issue with the HL7 protocol, but demonstrates the ramification of improper HL7 implementation.

Vendor related incidents such as this is considered an insider attack, either intentional or unintentional, the breach occurred because of someone who was granted access to the network and information systems within.

Downstream Data Integrity.

With the use of HL7 to assist in the interconnection of clinical information systems, data must be entered correctly to prevent the loss of data integrity and possible harm to the patient. According to Agrawal in a study performed by the Joint Commission in 2007, a large medical center found that incorrect registration data was entered during the admissions process for inpatient and outpatient on numerous occasions (Agrawal, 2014). So as a result, the incorrect data was transmitted into downstream clinical information systems using HL7 interfaces. What effect would this type of event have? This by definition is essentially what is known in computer science as Garbage In Garbage Out (GIGO).

An example of GIGO is when a patient gets registered with incorrect information, the result is a loss in data integrity. The loss is not only occurring at the point of registration, but the integrity loss has the potential to flow to downstream systems if the error correction has not occurred before the ORM transmission. Once the incorrect HL7 messages start transmitting, databases on downstream systems such as PACS, RIS, or reporting systems, start populating with incorrect data. Having incorrect data on multiple information systems increases the risk of an error that could affect patient safety. When incorrect data becomes populated into other information systems, rectification must take place manually in most cases. Yes, an ADT message can rectify some type of errors but, it is all according when the ADT message is transmitted. In information systems such as PACS if the DICOM files are created with the incorrect data, then the ADT will not resolve the problem. Not only are the databases incorrect but DICOM files used for clinical diagnosis is now incorrect. What happens if the PACS forwards the DICOM files with the incorrect data to a PACS system used in Teleradiology? As you can see, the number of places with the incorrect data can increase to an unmanageable amount.

This type of error was reported to be one of the top ten patient safety concerns in a 2015 ECRI Institute report. Most of these errors are caught days after the patient registration for a procedure at the healthcare facility (Relias, 2015). In the example, of a patient's DICOM files being created with data from the registration process, days later is most usually beyond the point of a wrong diagnosis and treatment plans.

Security Controls for HL7 Interfaces.

The protocol known as HL7 was developed to resolve communication issues between clinical systems and is efficient in communicating patient data between diverse information systems in Radiology and other healthcare areas. The fundamental issue is the security of the protocol. There are researchers who are calling for a replacement of the protocol after the demonstration at the security conference, Black Hat in 2018 (University of California - San Diego, 2018, August 29) but at the same time the protocol will be difficult to replace and will take many years for a replacement to be formally accepted and rolled out.

The current security posture will need to be improved during the development of a more secure replacement. The number of HL7 interfaces operational is upon a massive scale, hundreds of thousands of these interfaces are operational with new ones being brought online yearly (Haselhorst, 2017).

The steps to protect patient data must be implemented on the network and within the application configurations, and there can be several information systems such as PACS, RIS, or reporting systems that use HL7 interfaces that transmit patient data. As discussed earlier HL7 traffic travels across the network unencrypted and is easily exploitable like the DICOM traffic that is transmitted from the modality.

If the facility wants to secure the HL7 interfaces, it is possible that one if not all the vendors will not support the integration of the desired security protocols into their product. Most every information system in Radiology has a HL7 interface. PACS has multiple inbound interfaces, such as ORM, ORU, ADT, and outbound interfaces such as ORU image links, that send a hyper-link of the examination in PACS to the EMR, ORU discrete results that contain detailed clinical data used for data mining, i.e. big data. Smaller radiology departments utilize common interfaces, such as basic ORM and ORU, but at the same time complex healthcare organizations can have various types of HL7 interfaces that can span networks and enterprises. Reworking all these interfaces with coordinated vendor effort even if the vendors did support secure integration would be time consuming and costly to implement (Haselhorst, 2017).

To protect patient data HL7 interfaces must be initially secured upon installation. After upgrades are installed and configuration changes are made security controls need to be tested to ensure that regression in the hardening of the information systems did not occur. Recall that earlier, a vendor misconfigured a HL7 interface after an upgrade at Middletown Medical, resulting private data being made available on the Internet, therefore regression testing and proper change control must be part of a security plan. Of course, this is only part of protecting the data. Recall that researchers at Black Hat provided evidence that HL7 was easily sniffed and altered while in transit, proving that data in motion must be protected.

Encrypting the network traffic is the most important step in protecting the data flowing between clinical systems in a HL7 interface setup. Transport Layer Security encryption should be configured between HL7 senders and receivers. In National Institute of Standards and

Technology (NIST) publication 800-53 guidance is given to use TLS in a unique device to device trust configuration. If the HL7 interfaces connect over the Internet, then a VPN tunnel or SSH tunnel should be configured. (Haselhorst, 2017). For example, the ORU message depicted in Figure 7 should be encrypted to prevent the transmission of PII in clear text.

In addition to encryption, network isolation or segmentation should be applied to the HL7 interface endpoints. This mitigation tactic would keep the interface traffic off the main network. If an internal device was compromised by an attacker or if an insider wanted to utilize a packet sniffer, the HL7 traffic would be harder to find. However, segmenting the network could cause integration issues and the vendors of the interfacing HL7 nodes would have to work together to implement a solution such as this. In addition to segmentation, firewall rules can help keep unauthorized users from gaining access to the network that the HL7 traffic is transmitted. Keeping the HL7 isolated and encryption is part of a defense in depth approach but there are additional steps that can be used to encompass data security. Haselhorst (2017) recommends that each HL7 endpoint configure static ARP entries as another security step and by doing this the static ARP entry would allow only approved information systems to communicate within the HL7 interface.

Again, defense in depth is the best approach to protecting HL7 interfaces. As with any good information security plan, it is only as good as the weakest link. The discussion will proceed to what could possibly be the weakest link in the Radiology department.

Modality Security.

In DICOM terminology the Storage Class User (SCU) or what is referred to as a modality, is the medical imaging device that is acquiring the diagnostic images and initiating the network communication. Common modalities are Computed Tomography (CT), Magnetic

Resonance Imaging (MRI), and Ultrasound (US) and these are expensive medical imaging devices that interface with other DICOM and HL7 network resources. Ultimately, this interconnectivity can provide an adversary the backdoor into the network that is full of valuable PII. For a start, let us begin the examination of how that backdoor is opened.

In most cases, the modalities have network connections to the Internet so that vendors can have remote access to handle support tasks and so that in teleradiology configurations digital examinations can be transmitted to cloud PACS destinations. Despite the fact, that the outside connections present a threat vector for malware and attackers to gain remote access to the Radiology network, they are required to provide support to the modality. Attacks on modalities are frequent due to the low hanging fruit of legacy information systems used to operate them. As detailed in the following, in most healthcare settings, the modalities have possible security vulnerabilities that do not get patched or routinely audited for remote connections.

Modality Vulnerabilities and Exploits.

Securing the modalities is essential to the device having the availability to perform the ordered examination and keeping the Radiology network free of malware and unauthorized access. Newer modalities run Windows for an operating system, but in fact, some of these are running unpatched or unsupported versions of Windows, a few vendors do run proprietary versions of an operating system (Grimes, 2007). The most logical approach to information systems that run outdated or unpatched software is to work with the vendor of the modality to identify the risks to the device and how to mitigate them. On the other hand, this is not always possible because updates to the software can be costly and becomes overlooked in a budget (Quest, 2017). To further illustrate this point, in 2012 a report from NIST contained information on Beth Israel Deaconess Medical Center in Boston that reported an MRI was running Windows

95 while other modalities were running early unpatched releases of Windows XP (Fu & Blum, 2013). Risks to the healthcare information system infrastructure like this example is not an anomaly. In March of 2018, McAfee researchers found that a clear majority of modalities do not meet best security practices (Beek, 2018) and then Symantec reported the risk of an advance persistent threat towards devices in healthcare such as modalities in April 2018. The attacks in the recent years on medical facilities mentioned below have stemmed from unpatched modalities.

Orangeworm.

Symantec reported the risk of a persistent advance threat towards devices in healthcare such as modalities in April 2018. The attack group mentioned in the report is known as Orangeworm. The group was installing backdoors at multiple healthcare facilities and the malware from this group was found on enterprise healthcare organizations workstations that were mainly control systems for MRI and X-Ray modalities. The installation of the malware was trivial due to the nature of the devices having connections to the Internet along with unpatched operating systems. Once the attacker had the malware installed on the modality workstation they could then target other systems connected to the hospital network.

Orangeworm didn’t just target healthcare, but forty percent of the infections found were on medical devices such as MRI and CT information systems and this forty percent was larger than any other industry. Notwithstanding, the motives of Orangeworm was unclear at the times of the report and thankfully no malicious attack such as data theft or ransomware was carried out by the group. The malware installed by the group did successfully gather information about the Radiology network and devices connected to it (Symantec, 2018). In other words, the adversary was successful in mapping out the network and obtaining thumbprints of how networks such as these operate. Concerning this type of attack, although serious, it was not the first of its kind.

MedJack.

In 2016 security firm Trapx discovered malware that opened backdoors on multiple modalities at three undisclosed hospitals. The malware named Medical Device Hijack (MedJack) spread to PACS and other systems at the hospitals from the modality entry point.

The malware went undetected since anti-virus, and other security software is most usually not installed on the systems that control the modalities and thus leaving the IT teams unable to detect the intrusions. Much like Orangeworm. MedJack targeted legacy operating systems and took advantage of the limited security settings on these devices due to the nature of what functions they performed. According to the report by Trapx attackers have found that modalities have vulnerabilities that do not get patched in a timely fashion and are a prime target to gain access to a health care facility's network (Trapx, 2016). Again, this type of attack demonstrates how modalities are a likely entry point into the network. As described by Trapx vice president of marketing Anthony James in an interview for Wired Magazine,

> Most of these facilities have no clue, because no one is monitoring their healthcare devices for the presence of an attacker. No one is thinking about a CT scanner or an MRI machine and seeing a launchpad for a broader attack.

The broader attack described in the above quote has been seen recently in attention grabbing headlines and is referred to as Ransomware.

***Ransomware*.**

In May of 2017, many medical facilities in the United Kingdom and the United States were the targets of ransomware attacks that were carried out using tools stolen from the National

Security Agency (NSA). The estimates that hackers installed ransomware compromised over two hundred thousand clinical information systems running the Windows Operating system. For this reason, at one hospital in the United States, ransomware infected a medical device attached to the MRI. In this event, the Bayer Medrad system that was taken offline, halting patient care, was running an outdated version of Windows. The device was not the primary operating system for the MRI but did control the amount of contrast the patient was given intravenously during the procedure. This portion of the examination integrates with the SCU DICOM software to build the meta-data in the DICOM files (Alpine Security, 2018). Similar, to Orangeworm and MedJack the device was used as a backdoor into the Radiology network and from there into the hospital network.

Modality Worklist Errors.

Not all security risks pertain to malware and hackers, there are issues with standard workflow functions used in Radiology, and this aspect of modality security pertains to the data integrity in the generation process for the DICOM files. Before the image acquisition, the patient demographics are entered by the Technologist into the modality console, and more importantly the data integrity at this step is critical. The risk to adverse events in patient care and confidentiality will occur if the data for the patient, referring physician, or examination has errors during the data entry at the registration of the patient on the modality. Maintaining data integrity at this crucial step in the DICOM workflow is achieved by a technology mentioned earlier, DMWL. The primary function of the DMWL is to automate the registration of the patient on the modality in an efficient error-free process. Most Radiology departments experience high patient volumes, and the data entry requires precision to prevent potential medical errors and maintain the integrity of the patient data. The DMWL is an integration between the Hospital Information

System (HIS) and PACS to provide the error-free data flow and help improve the overall efficiency of the Radiology workflow. The need for manual data entry of the patient demographics and examination information is done away with since the DMWL populates all the data for the Technologist. Data integrity is highly vital at the HIS registration process. If the data gets entered incorrectly, it will flow downstream to the PACS and onto other downstream information systems, passing the data integrity issues to other clinical systems. The DMWL prevents the technologist from having to enter patient demographics and study information manually into the modality, and this prevents errors that can occur by manual data entry. Another potential error created by the implementation of DMWL is the risk of selecting the incorrect patient from the DMWL and performing the examination. Currently, there is no method of detecting such an error that could cause possible patient harm other than manual detection. Similarly, to the method when incorrect data is sent downstream from the HL7 feed to the DMWL, when an examination is performed on a modality and converted into DICOM, it can get transmitted to multiple PACS destinations that have the functionality to forward the incorrect data to additional information systems. It is of high priority to correct a study performed under the wrong patient demographics on the modality prior to transmission to DICOM destinations. Due to the efficiency of PACS, the examination is quickly ready for viewing and interpretation (Kuzmak & Dayhoff, 2001). This type of risk involves the entire CIA triad. The correct patient medical record will be unavailable due to the data integrity loss along with possible loss to confidentiality if the results have transmission to the upstream and downstream systems.

Modality Data Storage Concerns.

In a study by Moggridge (2017), showed that not all methods of sanitation completely removed patient data from hard drives installed on modalities. The means of eliminating data and leaving the ability to be recovered afterward were using the operating system and vendor software to remove patient data. Even resetting the modality software back to factory settings did not prevent patient data from being recovered and the only methods that eliminated the data from the hard drive used in the study was the standards recommended by NIST and the Department of Defense (DoD).

When assessing the risk of storage of patient data not only does the servers and workstations need to be reviewed but the modalities themselves need to have security policies and procedures in place to prevent unintentional data compromises. Risk assessment plans of the modalities must also consider when a device or control workstation is decommissioned or returned to the vendor after the lease is expired. Once the device is removed from the responsibility of the healthcare facility patient data and meta-data could remain on the modality hard drives if proper data sanitation is not performed and as method before. Modalities and the attached information systems contain hard drives that could not be destroyed if the equipment is under lease or being traded back to the manufacturer for newer hardware and the vendor's software could have methods of removing the patient data from the hard drive, but it is the responsibility of the healthcare facility to validate the process.

Security Controls for Modalities.

Understanding the function of each modality and connection in the Radiology network is a key part of preventing the loss of confidentiality, integrity, and availability. A thorough inventory of the modalities must be completed before assessing the risks and vulnerabilities. The inventory must contain a comprehensive list of each modality that stores, transmits, or processes patient data. Each identified item needs to be analyzed to gather granular details of that device. The information will vary between device for example a switch between the actual CT modality and the CT workstation will have different details than the C-Arm modality. To properly gain insight into the current security posture of the Radiology network each modality within the workflow must be analyzed independently and collectively. After the asset inventory is completed the risk assessment process can begin.

Modalities have been designed to have a long-life cycle and to work without any interruption. This sort of engineering has led to the security state of the industry. The operating systems for the modalities need to be kept up to date and replaced when the operating system is end of life. According to Symantec, 2018:

> Long device lifecycles keep hardware, operating systems, communications protocols, and applications systems in service on medical devices long after they have disappeared from enterprise IT networks—so devices remain vulnerable to exploits that are of no concern to desktops and laptops.

This was documented in the study by Fu & Blum where modalities were still running Windows 95 and XP long after the operating systems were no longer supported by the software vendor, Microsoft. This does present the issue of who is responsible for upgrading the operating system. The vendor is fully responsible if the support contract defines them as such. Due to the cost and long device lifecycle the modality will be in service long after the operating system is at the end of life and in fact the cost to replace the medical device is too high just for the security of the operating system software. Stipulations in the support contract must state that the operating system must be maintained and updated to prevent vulnerabilities that will arise as time passes and the operating system comes to the end of life. Another stipulation in securing the modality is who performs the updates. Modalities are considered a medical device and per the U.S. Federal Food and Drug Administration (FDA) the vendor not the owner must be the party that installs and validates patches. Not only does this hinder the installation of security patches but the usage of third path software such as anti-virus, firewall, and Host Intrusion Protection System (HIPS) and this slows down the pace of installation of patches and eventually leads to breaches as previously described.

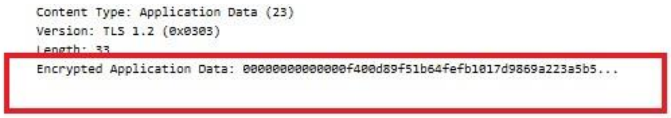
Authentication to the modalities need to be audited and restricted to users with least privilege configured. Authentication to the modalities and devices in emergent care are difficult to manage. The study by Mahlaola and Dyk, 2017, showed that in emergent care and authentication policies that burden patient care will add to human error and unintentional security events. Modalities are like the workstations in the Emergency Room. They are used by a specific group of users, they are in restricted areas of the facility, and have multiple users that can access them. Biometric authentication is one possible solution to the problem. However, the problem lays within the type of authentication the modality is configured with. Local host authentication methods are common with modalities. In an interview with Wired, Security Researcher, Scott Erven discovered that modalities had weak hard coded passwords such as admin or 1234 (Zetter, 2014). This highlights the fact why hackers target modalities, they are vulnerable to being unpatched and have week password schemes that are used across the board.

The modalities are often overlooked when a healthcare facility performs an asset inventory. Modalities are medical devices where access to the administrator functions are left to the vendor for that device and not the IT department. These devices have inner networks for the device to function properly and connect to the Radiology network to transmit the DICOM files to PACS or some type of DICOM destination. As previously discussed modalities have been used as a threat vector to enter a Radiology network for an attacker. Performing an asset inventory of the modalities is an essential step in the hardening process. There are many functions to secure on a modality to maintain confidentiality, integrity, and availability. The overall operating system, the network, DMWL, and data storage for the modality must be secured from insider and outsider attacks.

Modalities have already been proven to the be low hanging fruit that is plagued with unpatched operating systems and can be easily accessed by attackers **(Symantec, 2018).** A secure method of trust must be formed between the modality and all systems that it communicates with and any communication outside this trust should be restricted. Likewise, any device that is outside the modality trust should not be communicated with. Both Orangeworm and MedJack infected modalities and by doing so created a door into the rest of the network. Trustworthiness of modality information systems needs to be configured using the core security principles listed in NIST publication 800-53. These are simplicity, modularity, layering, domain isolation, least privilege, least functionality, and resource isolation/encapsulation. This type of approach using defense in depth is the best approach to defending against advance persistent threats and internal threats (Ashford, 2011). If the modalities infected with Orangeworm and MedJack were isolated to a Virtual Private Network (VLAN) in which other systems was not connected the malware would not spread across the network. Of course, the devices and network being isolated is not a reason to leave the information systems unpatched.

Veterans Affairs uses the NIST approach to security and provides a Medical Device Isolation Architecture guide. The guide provides the solution to a modality limitation of receiving operating system patches and anti-malware software installation. The solution is by placing each modality in a VLAN behind a firewall that will limit access bi-directionally. Inbound and outbound ports are limited to the VLAN in which the attack surface is smaller. Access control lists (ACS) are used on the routers and firewalls to add an extra layer of protection to the devices inside and outside the isolation VLAN. Again, this is an example of a defense in depth approach that mitigates the limited operating system patches and anti-malware software usage on the modalities.

The communication channels between the modalities and DICOM destinations must be secured. Due to the unsecure nature of DICOM it is passed over the network in clear text. Methods described in NIST publications and other security frameworks must be integrated into the communication of DICOM data. The metadata within DICOM contains PII and PHI and without question should be protected. DICOM includes CMS that would encrypt portions of the DICOM header, and naturally both sides would have to agree on this method and some vendors may not support it. Alternative measures are to encrypt on the network level such as the use of Transport Layer Security encryption between DICOM endpoints is highly recommended in a defense in depth strategy. In NIST publication 800-53 guidance is given to use TLS in a unique device to device trust configuration. This primarily is what the Radiology network is, unique devices communicating with each other, but vendor buy in is required for such a configuration. Security will improve if the vendors can communicate using TLS. Recall, how the DICOM association request was transmitted in clear text? Below is the same communication sent using TLS.



```
Content Type: Application Data (23)
Version: TLS 1.2 (0x0303)
Length: 33
Encrypted Application Data: 00000000000000f400d89f51b64fefb1017d9869a223a5b5...
```

Figure 8. Encrypted DICOM Association Using TLS.

Discussions on security is highly important when negotiating contracts or releasing a Request for Quote or Request for Product. Security requirements need to be made upfront in a confidential non-public manner. Documents that discuss the security design of a network should never be made public. Modalities can transmit to cloud based DICOM systems and again, the security of this type of network should be reviewed independently as it will have different risks.

For remote modalities sending to an on-site primary PACS or cloud based PACS a secure network connection is needed. NIST provides guidance for the secure implementation of the VPN tunnel that gives security assurance. By creating a VPN tunnel the endpoints of the communications are encrypted and the devices on both ends have formed a trust. The VPN connection must be monitored for unauthorized traffic and malicious code on a regular basis.

To achieve secure communications with PACS or other DICOM resources on the network the modality should only have connections to trusted systems, so in other words, setting up a trust between modalities and DICOM destination should extend beyond registering AE titles. Due to DICOM handshakes being transmitted in clear text the risk of that data being spoofed is high. In addition to registration of AE titles steps to protect the data being sent between the DICOM devices needs security functionality and security assurance. How can this be configured? This can be accomplished using firewall rules to allow only systems who have a trust to communicate with only the required ports in the workflow, all other ports should be closed. Once the communication with the proper ports are configured the next steps in the workflow should be reviewed to protect data integrity.

According to Kuzmak and Dayhoff, the risk mitigation to DMWL workflow vulnerabilities, such as selecting the incorrect patient from the DMWL list, is to implement controls such as patient verification steps that include minimizing the number of examinations displayed on the DMWL at a time, set up the modality to query by patient ID instead of date range or add a verification step to the modality. The Veterans Affairs (VA) hospital system made it a requirement for all modalities to have a second verification step within the DMWL. The reasoning behind the VA making such a requirement is that they found it easy to select the incorrect patient or study from the DMWL (Oosterwijk et al., 1999). It is mitigations such as this that will reduce the number of errors that can lead to data integrity loss.

A single modality can have the capability of having outbound connections to multiple DICOM destinations, inbound connections from the vendor, and interfaces to HL7 brokers that provide DMWL functions. Within that single modality there are several risks that can be exploited by an attacker. The modalities are only a portion of the communications in Radiology that seem to be secured with the obscure protocols used alone. The vendor configuration on a modality could include an internal network that connects various components in the workflow for the medical device. For example, there could be an internal switch that connects the modality to the workstation and internal components such as the MRI contrast agent that was infected by Ransomware at Bayer Medrad Health (Alpine Security, 2018). Then the workstation connects out to the Radiology network where other modalities, workstations, and PACS is located. In that single modality there are two connections, one internal and one external. This type of configuration presents a risk since an attacker could compromise and then attack devices on either side if they were not secured properly. Proper switch security and updates to the OS and installed software must be deployed on a scheduled basis. Applying to the updates to the systems that are on the internal side of the network will have to be planned for by the vendor. Security in layers is the recommend approach. Keeping software updated and having unnecessary services disable is adding additional layers of security. This as well would of help prevent the breaches in the Orangeworm and MedJack cases since unpatched systems was the method of exploitation in the attacks. If the attack surface is low on the modalities, then the likelihood of an attack is lower.

Outsourced DICOM Services Security

In the growing industry of cloud-based services healthcare has adapted to the models of Software as a Service (SaaS). With that in mind, due to high speed Internet connections, three SaaS platforms are utilized by Radiology departments, Teleradiology, Cloud PACS solutions, and Cloud Reporting. All three of the SaaS solutions are similar but differ slightly. To explain more, Teleradiology is the outsourcing of interpretation of Radiology examinations. Either the modality or PACS will transmit the DICOM files to the remote SCP located on the Teleradiology network. From there the Radiologist will interpret the examination and the results will be transmitted back in some form of reporting and this reporting could be a simple fax or within the Cloud Reporting software that will be discussed later. Lastly, the Cloud PACS is a SaaS solution that removes the physical footprint of a PACS from the medical facility and moves it of the cloud, think of Google Drive or Drop Box for PACS. These solutions offer the storage and viewing software all via the cloud. All these solutions sound good to reduce overhead but as with anything being placed on to the Internet, the risk increases for attacks from adversaries.

Outsourced DICOM Services Vulnerabilities and Exploits

Innovations in the past few decades have cut costs and improved the effectiveness of technologies that use DICOM and HL7. The ability to transmit DICOM and other patient data into the cloud or across the country is commonplace in the Radiology department. Partnerships with teleradiology groups, PACS vendors, and reporting software vendors have formed but security is not always an area of focus when the contracts are signed.

Since the data is flowing across the Internet other factors such as how the Internet Service Providers (ISP) are regulated. The impact of Internet regulations such as Net Neutrality threatens the foundation of which much of the innovation in this industry has created.

Teleradiology Security.

Not only should the modalities be secured from remote access and vulnerabilities that an attacker can exploit but the end to end DICOM data flow. Radiology networks are complex and have multiple potential risks associated with the devices that are communicating with the DICOM protocol. Another risk factor is a common network destination where patient data is transmitted outside of the local network. In teleradiology DICOM files are sent to a destination on an outsourced networked where the studies are stored and possibly transmitted to multiple destinations. Each destination could be point of entry for an attacker to obtain private health information of a patient. Teleradiology is a form of cloud computing and should be treated with caution when establishing partnership with companies that offer these services. According to Kharat, Safvi, Thind, & Singh, 2012, challenges exist in privacy but can be mitigated by an encrypted storage and transmission of the DICOM data. Audit trails and the use of biometric authentication methods need to be mandatory in the teleradiology environment. Another factor that was documented is the loss of availability to teleradiology nodes due to a network outage.

With teleradiology the connection has the possibility of crossing multiple providers. An Internet outage, network failure, or loss of a DICOM device on the teleradiology side could result in delayed patient care. All external network connections into the Radiology network should use a VPN or some type of network encrypting device, have redundancy, and a contingency plan. There should be firewalls implemented along with network segmentation. A multi-layered approach is best practice when securing the outside network access. The risk for loss of the availability to timely DICOM data transmission has been heighten with the repeal of the Net Neutrality rules. After decades of innovation under net neutrality rules, the healthcare information technologies have expanded into high-speed networks that have improved patient care. Teleradiology has allowed STAT examinations in rural hospital emergency rooms a prompt turnaround in interpretation. Sending hundreds of gigabytes across the country to other DICOM servers while physicians download the digital images from the PACS vendor's server. All of this is accomplished over an Internet that doesn't throttle, block, or charge additional costs for high utilization. Without the net neutrality rules, rural hospitals could lose the affordable infrastructure and the low cost of the connections to provide affordable healthcare (Brazzoli, 2017). If throttling is used by the ISPs and paid prioritization offered to profitable companies such as Facebook, YouTube, and Netflix then hospitals may not be able to afford the cost of being in the fast lane. This will result in the teleradiology services in the rural hospitals would suffer the most (Leaf, 2017). The hospitals will have to make difficult decisions to cut services or pass the cost on to the patient. Teleradiology has reduced the cost of healthcare and improved overall care (Luong, 2017). Net neutrality endangers the loss of the advances that have been made in the past two decades and future innovations by allowing the ISPs to throttle teleradiology network traffic and charge healthcare providers for something they have used to create cost savings.

Teleradiology is not the only cloud-based function in Radiology. DICOM data must be backed up to comply with regulations such as HIPAA, HITECH, and SOX. PACS vendors and manufacturers of DICOM devices offer off-site disaster recovery for patient data. The same rules that applied to Teleradiology should always apply to cloud services that backup data.

Cloud PACS.

Cloud computing is a growing technology used in healthcare. There are many uses for cloud computing in Radiology. These are Software as a Solution (SaaS) and Infrastructure as a Service (IaaS). There are other types of cloud offerings in Radiology, but the focus will be on these two main offerings. Two of the challenges in a cloud DICOM system are security and availability of the data in the cloud (Selvamani & Jayanthi, 2015).

When placing patient data such as DICOM into the hands of a cloud provider either it be for off-site long-term storage or for a SaaS PACS viewing solution security incidents can occur. One of the obstacles of having a cloud solution is how to upload the data in to the cloud quickly for retrieval. Similarly, to teleradiology the bandwidth and amount of data being uploaded is far greater than a standard customer of the ISP. With the repeal of Net Neutrality rules the availability of DICOM data going into the cloud could face a new threat that was not present prior to the repeal. Costs savings is the reason behind most facilities moving to a PACS vendor that offers a cloud platform. A smaller facility does not have to purchase, update, secure, or maintain hardware or networking. For larger companies the question of how to achieve an off-site backup of DICOM data is answered. The cost is enough to justify paying service contacts and per usage fees for cloud hosting (Pratt,2017). These services, however, rely on quality and robust connections (Arndt, 2017). According to Sullivan:

> The cloud is a highly effective platform for healthcare organizations to leverage, made more relevant by the industry’s evolution toward a consumer-driven approach to care and its need for greater collaboration to serve long-term growth.

With the repeal of net neutrality ISPs that are no longer under the regulation that prevented them from charging extra for data that a subscriber, such as a healthcare facility sending and receiving terabytes of data daily, it is possible that the cost savings from going to the cloud could be in jeopardy. According to Adams & Kuhnen:

> ...costs could go up for providers, either directly or indirectly. ISPs could charge hospitals, or more likely their cloud-based vendors, additional fees to deliver reliable service for their mission critical applications. Application vendors will likely pass these costs on to their customers.

The increase will have noticeable effects on all parties, patients, vendors, and providers. Data that is in the cloud could be locked into a slow lane when being retrieved. Uncertainty of low-cost Internet and reliable service is bad news for healthcare IT since the repeal of net neutrality (Adams & Kuhnen, 2017).

Sending x-rays between providers and vendors to rely on a quality Internet service All the innovation within cloud-based services for digital imaging is all built upon net neutrality and that the assumption that the traffic was created equally with their high bandwidth applications (Spitzer, 2017). Cloud-computing within Radiology has thrived within the structure of the Internet that allowed all traffic equal treatment. The shift from internal resources to cloud-based services has the basis of cost savings and performance. (Sullivan, 2017) With the repeal of net neutrality, these benefits have potential to be removed.

Nuance Interface Upgrade.

In January 2018 Nuance, who was acting as a transcriptionist vendor for the Orlando Orthopedic Center upgraded software for the remote reporting service. During the upgrade an error on the public facing interface server was made that resulted in over nineteen thousand patient records being made available on the Internet without any authentication method for the period of two months (Donovan, 2018). The scenario clearly demonstrates how a security misconfiguration on the external services information systems can place a Radiology department in a situation where patient data is compromised and leaving the responsibility of rectifying the breach in the hands of the provider.

Security Controls for Outsourced DICOM Systems.

External service providers present a risk that will require security controls. Radiology networks have become reliant on external services such as teleradiology, off-site DICOM storage, and vendor support. A level of trust is placed with these external service providers and there should always be contract agreements between the healthcare facility and the external service provider to set the bounds of how information and information systems should be protected. By outsourcing a service, it will be assumed that risk is either transferred or accepted at an acceptable level. Legal ramifications can occur if the contract does not clearly specify who is responsible for securing the data at times when the data is in the possession of a party within the contract.

Two key components of the trust between the Radiology department and the external service provider are security functionality and security assurance according to publication 800-53. Security functionality is the overall information security structure applied to the systems and workflow while security assurance is the certainty that proper security measures are in place to protect information and information systems. The trust is formed by security assurance activities such as audits or accreditations. The Department of Defense established a standard known as DoD Information Assurance Certification and Accreditation Process (DIACAP). The standard was replaced by RMF recently. The accreditation process remained largely the same from the change to RMF. In short, a vendor had to be accredited before they could operate within a DoD network. Similarly, if a manufacture of a modality or PACS system wanted to implement their product within a Radiology department operated by the DoD then they had to go through the accreditation process to prove that security functionality was intact and security assurance was proven. If Radiology departments ran by the private sector adapted the DoD accreditation model for external service providers there would be less room for lapses in security and overall breaches of patient data. In the instance of the Nuance and Orlando Orthopedic Center upgrade that left thousands of patient records vulnerable to attacks an accreditation for the Nuance software would have prevented such mishaps from occurring. Nuance would have to provided security assurance of that their upgrade did not degrade the security posture of the information and information system.

Security controls need to be selected to maintain the CIA triad for the information and information systems within the workflow for external service providers either an outsourced transcription service, vendor remote support capabilities, or a DICOM off-site storage. NIST publication 800-53 provides guidance on how to select relevant security controls. Prior to the selection of the relevant security controls the security categorization outlined in NIST publication 199 that was discussed earlier and is required for each information object and information system. Applying such tactics will assist in the identification of possible vulnerabilities and security lapses that could occur when system configuration changes are made.

External service provider vendors are not the only vendors to be held to security functionality and security assurance but the vendors for the modalities, HL7 interface systems, and PACS as well. Each vendor offers some type of functionality in the Radiology workflow. Multiple vendors play a role and as in the early days of digital imaging there had to be a standard in how the information systems communicate. This is how DICOM become the standard for medical imaging. If RMF was required by the Radiology department then vendors would have to conform to a security standard as they did with DICOM and HL7. The vendors for these systems are universal at times. For example, General Electric manufactures modalities and PACS. Even if the DICOM and HL7 information systems on the network were from various vendors, in which, most circumstances they are, they can be communicate in a secure and efficient manner.

DICOM Storage Security.

Securing the transmission of the DICOM data is only one step of many in securing a Radiology network. DICOM files are stored unencrypted natively. The risk of having PI in multiple unencrypted files on long- and short-term storage opens the door for a breach in patient confidentiality. DICOM file storage takes place on a large storage device such as a SAN or NAS but is often downloaded to PACS workstations that store the DICOM files for a configured time frame that usually varies between one to thirty days. Data at rest risk mitigation steps need to be applied to both servers and client workstations within the Radiology network.

Dicom Storage Vulnerabilities and Exploits

There are many events that can cause adverse effects to the confidentiality, integrity and availability of stored DICOM data and some of these events are not realized until an amount of time has passed, and the results are irreversible. In this, there are several items to consider when storing DICOM data. One is the method of how the data is stored. PACS and modality vendors, despite being DICOM compliant, there are differences in how DICOM data is processed and stored. The data loss comes from compression settings and how the DICOM tags in the files are processed.

Before going into the problems that could occur with DICOM storage the process for storing the data will be explained.

The service built into DICOM that handles moving DICOM to a storage device is called C-Store and was noted above in figure 4. The SCP is the storage device such as a PACS or VNA and as a review the SCU is the medical imaging device itself that is acquiring the diagnostic images and initiating the network communication. These roles can be reversed and are interchangeable and for that the SCP is not always the storage device and the SCU is not always the imaging device (Mildenberger, Eichelberg, & Martin, 2001).

As mentioned before, the SOP Class which is not negotiable, due to the fact that the SOP Class defines the modality type, so either, the SCP either will except or reject the SOP Class. All of this is based upon if the SCP can process and store the SOP Class being sent. In other words, it is similar to talking a language. Does the SCP talk MRI? Does the SCP talk Mammography? Remember that during the DICOM association the SCU and SCP will agree on an encoding format for the images to be transmitted with and this is known as the Abstract Syntax and the compression ratio of which the diagnostic images will be transmitted and received is agreed upon in the association known as the Transfer Syntax. (Pianykh, 2008, p. 187-188). Of course, the Transfer Syntax plays an important role in the C-Store process as a diagnostic image that is compressed will take less disk space to store (Veeramani, Masood, & Sidhu, 2014).

Regarding image compression, the acceptance between vendors can greatly vary, again, distorting the lines in integration. According to Oglevee and Pianykh there are eighteen versions of JPEG compression and most PACS vendors could use variations that could led to loss of data when migrating to a another PACS vendor. It is within these DICOM options where data integrity and possibly availability of the DICOM files get lost. If the configuration for the DICOM workflow is not validated properly then adverse events can occur.

Massachusetts General Hospital.

In an article by Oglevee and Pianykh an issue with vendor incompatibility led to a loss of PET images and the data was unrecoverable since the Radiology department did not find the problem until years later (Oglevee & Pianykh, 2014). In this case, the data loss began when the archive vendor was altering the DICOM tags for the PET images. The tags were DICOM VR tags and although the change was a violation of the DICOM standard the vendor made these changes during the C-Store process. However, since the DICOM files were being viewed in the vendors PACS product the loss was not noticed as the vendor software compensated for the lost DICOM tags. It was only after the DICOM was attempted to be viewed in another vendor's PACS product that the loss was discovered. Needless to say, the removal of valuable DICOM tags is not the only manner that data loss can occur.

Failure in C-Store Process.

In 2008 at an undisclosed hospital a patient had a CT examination that was scheduled by his physician because the patient had been complaining of pains in his lower abdomen. Weeks later the patient showed up at the ER because the pain had increased to higher levels. During the emergency surgery to fix an aortic aneurysm the patient died.

In the malpractice lawsuit it was discovered that the CT examination was not properly stored to the newly installed PACS system at the hospital. A PACS consultant was brought into investigate why the CT examination that was performed was never transmitted to PACS and interpreted by the Radiologist. If the CT had been reviewed by the Radiologist on PACS then the patient would have survived because the aneurysm would have been found prior to his death. The PACS consultant found that the examination was labeled under the incorrect name and patient ID, leading to the results of the CT examination never making back to the referring physician and patient (Smith & Berlin, 2008). Recall the issues with data integrity and patient safety issues with the DMWL. It is cases such as this, that highlight the fact that there are serious fundamental patient safety issues within the DICOM and HL7 workflows. Here we have a patient who died due to a data integrity error. One must ask, how did the patient examination fail to be transferred and was on the modality under the incorrect name? That answer is within how DICOM and PACS is configured. For instance, if the PACS already had the examination that was under the original examination, the one that was not the wrong patient, then the PACS may have rejected the C-Store request to store the DICOM files under the incorrect patient due to already having that Study Instance UID. According to Pianykh, the Study Instance UID is the unique identifier for a DICOM study and is in most cases the primary key used to store study data in a PACS or VNA database. In figure 9 below is a workflow of the rejection of the C-Store process due to the fact that the PACS database already has that Study Instance UID.

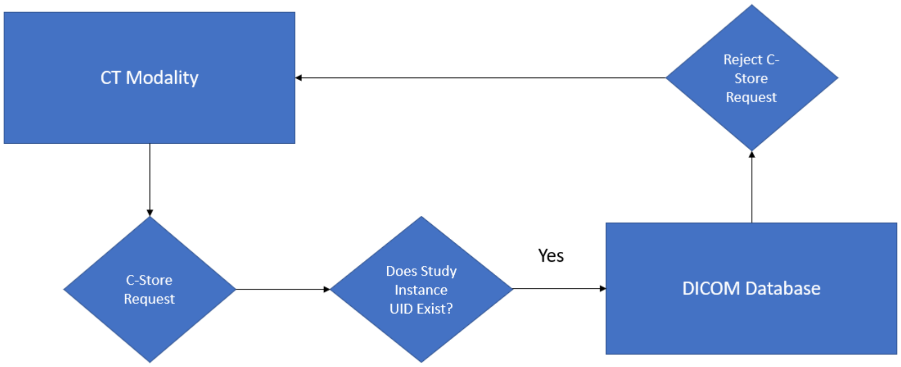
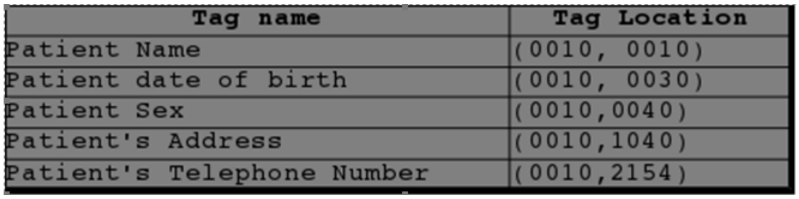


Figure 9. DICOM C-Store Workflow.

DICOM Stored Unencrypted.

According to Moggridge (2017), “DICOM meta-data is generally stored as clear text, meaning any standard text editing software can be used to open a DICOM file and view available fields.” This metadata is known as the DICOM tags. The data is categorized and broken down into group, element using a hexadecimal numbering system for identification. For example, the information about the patient are in these DICOM tags:



Tag name	Tag Location
Patient Name	(0010, 0010)
Patient date of birth	(0010, 0030)
Patient Sex	(0010,0040)
Patient's Address	(0010,1040)
Patient's Telephone Number	(0010,2154)

Figure 10. Patient Demographics DICOM Tag Location.

This type of information about the patient will always be found in these locations in the DICOM header (Pianykh, 2008, p. 42). The DICOM tags are populated with information about the patient that was sent downstream from clinical systems as where the data is entered into the EMR, passed to clinical systems in Radiology, the modality pulls the patient data from the DMWL, and this is what populates the DICOM tags. At times there is an alternative patient ID passed from the EMR and in some cases, the alternative patient ID can be a social security number. If the interfaces are configured to allow the alternative patient ID then the DICOM tag (0010,1002) could have the patient’s social security number along with full name, address, and date of birth in the meta-data of multiple DICOM files. In reference to multiple DICOM files, a single MRI examination could have hundreds of files that make up the DICOM study.

In a normal PACS configuration it is normal to have multiple terabytes of unencrypted data stored. It is best practice to store the DICOM data on a dedicated file storage device that does not share access with other departments or hospital operations. Access to these data stores must be restricted to approved users or services only. As stated earlier data should be backed up using a secure cloud services backup. If all possible the backup of the data should be in real-time. (Pianykh, 2008).

Security Controls Dicom Storage.

DICOM data at rest should be encrypted using accepted algorithms like RSA and AES as these are accepted by the DICOM standard and will convert DICOM files into encoded data and back into DICOM without any loss to the integrity of the diagnostic image (Pianykh, 2008, p. 256-260).

It is recommended that the DICOM storage device has a Host based intrusion detection system (HIDS). Using a HIDS to monitor the DICOM storage would be an effective defense in depth approach to securing DICOM data. In addition to the security that encryption provides, the HIDS would monitor and alert proper personnel, block possible unauthorized connections, and the HIDS would detect if any anomaly data requests that an attacker might launch from an internal compromised device (Moon, Pan, & Kim, 2016).

Access to the data at rest must be audited. These audits must be reviewed on a routine basis and additionally the implementation of these logs should be extensive enough to meet HIPAA auditing compliance and not interfere with patient care. There should be at least a couple of different audits for the DICOM data at rest. One is when PACS retrieves a digital examination upon a request by a user but the other should be when the DICOM data is access directly (Liu, Zhou, and Huang, 2006).

In addition to the security mechanisms that prevent unauthorized access from occurring further controls must be implemented to keep data confidentiality, integrity and availability intact. Validation at the implementation and routine checks would prevent data loss that spans years as in the case of Massachusetts General Hospital and the incorrect storage of DICOM PET images mentioned earlier. The routine checks are not automated but would have to be logged.

Any changes to the configuration between the SCU and SCP would need to go through the proper change control process.

Any data that is transmitted from a modality requires auditing to verify that the patient information is correct and that it stored correctly onto PACS. The technologist that performs the examination should verify this information is correct. A process between the EMR, modality, and PACS should be implemented to provide a cross-reference of the data. Any integrity issues discovered must be rectified quickly to prevent a potential event that could lead to patient harm.

PACS Security.

With transmission and storage of the data being secured the access to the DICOM data must also be restricted to authorized personnel and audited on a regular basis. Access to the data on a PACS system is most usually through a software application from a PACS vendor called a DICOM viewer. The application is built on top of databases and the DICOM data store. Access to PACS allows users to be able to review digital images transmitted and stored into the system and most of the time other clinical data such as reports and clinical history. In a hospital most if not all physicians have access to PACS along with other clinical staff, Technologists and Nurses. With more individuals having access to the system the greater the risk of a breach occurring. Due to the critical nature of the data within PACS the need to deploy more clients is required, meaning more points of entry for an attacker to exploit. According to Conaty-Buck a nurse at one facility did not the follow the policy of Internet usage and jeopardized the facility and every patient that has received treatment there. After browsing to an Internet site that was infected with malware the workstation was breached along with information systems including PACS. The attackers installed Ransomware which encrypted the data making it unavailable.

PACS Vulnerabilities and Exploits.

There are many varieties of PACS and multiple vendors offer PACS workflow solutions. From these solutions there are vulnerabilities that require mitigation before they are exploited by an attacker. Above all else, it is the responsibility of the medical facility to validate that the PACS functions without problems that might lead to data loss or system compromise. Quick access to PACS data can lead to exclusions in password and auto locking policies. However, the balance between security and functionality seems to be a struggle with PACS.

Authentication to PACS should be administrated by personnel in the Information Technology department and handled per security policies and procedures for other systems such as the EMR. As detailed below, accounts need to be audited and disabled after users are no longer active with the facility. In the same respect, networking, antivirus, and backup of PACS should always follow security policies. Any compromise in the security policy is compromising the CIA triad.

Availability to PACS.

Availability to the data in PACS is critical for quick patient care. PACS has created an environment in healthcare that has allowed patient care decisions to be made within seconds. Access to current and historical diagnostic images is a key component in the workflow for PACS. DICOM files are large and require storage that ranges in terabytes. Quick access to this data is a constant requirement. As the technology grows in digital imaging so does the image size. As quality goes up the storage and bandwidth requirements follow. Common storage issues are how and how much to compress the DICOM files. If too much compression or the incorrect compression is applied, data integrity could be compromised because the image could lose diagnostic qualities and influence patient care. The data storage of the files is critical to the functionality, legal requirements, and care provided to patients. It must be stored correctly, backed up, and have rapid retrieval times (Elm, 2008). In addition to security there is an overall issue with DICOM data storage. Security concepts such as data integrity, data availability, and disaster recovery all play a role in the storing of DICOM data. As patient visits increase, and the quality of data increase the necessity of storage size on both onsite and offsite locations.

Current studies being transmitted and retrieved from PACS are not the only data in the DICOM data flow. Prior DICOM studies need to be retrieved to compare to the current DICOM study. HIPAA requirements vary from state to state for the length of time that a healthcare facility must legally obtain these DICOM studies. For example, the state of Kentucky requires the retention of records for 5 years after the discharge date for adult patients. If the patient is a minor, under the age of 21, then the records must be retained 5 years from the discharge date or 3 years after the minor patient reaches the age of 21. No state has the same regulation which making it difficult for vendors to offer a solution. This creates a quickly growing need for storage. Most PACS installation have a RAID configuration. Some have moved to SAN and NAS configurations that allow a VNA approach to storing DICOM files. The data on these storage devices will need to be backed up. One common offering of PACS vendors is to offer a cloud backup solution. The cloud solution opens additional security vulnerabilities.

Password Issues in PACS.

When security policies are not entirely intact, and the stress level is high, humans are bound to allow enough error for a breach to occur. The fine line between patient confidentiality and patient safety gets divided by the security of the information systems in the Radiology department. In emergency rooms where PACS has become a lifesaving tool by allowing access within seconds to digital imaging data. Access to PACS must require complexity password policies but unlike other systems PACS requires instant access to data. Having the standard screen lock and complex password hinders patient care on certain clinical systems and PACS is included in this group. If such policies are implemented, then training on password policy is not enough to prevent system misuse or workaround such as writing passwords down and placing them under the keyboard. Human error will occur and possibly lead to unintentional breaches. The reason for the human error is due to a stressful work environment, time restraints, and overall system design. A password policy plays into another issue with security of information systems such as PACS. The compliance for such policies as complex passwords requires the end user to have some knowledge in the field of information security. Therefore, information assurance training needs to be implemented. (Mahlaola and Dyk 2017). The effective strategy for username and passwords in PACS would be the use of biometric or a PIV two factor authentication. These would reduce the risk of unauthorized access and give the provider quick access to the pertinent information in PACS.

In a survey from 2018 twenty one percent of healthcare workers admitted to writing down their username and password near their computers. The same surveyed group had ninety seven percent to agree that they understand the information assurance policies from their workplace (Accenture, 2018). This type of data provides some insight into reasons why password policies, no matter how strict do not fully mitigate unauthorized access.

Conficker.

In 2008 a worm known as Conficker was being reported on healthcare networks. Radiology departments were the hardest hit with these attacks. According to Rodney Joffe who was a senior technologist at NeuStar that Conficker infected PACS diagnostic workstations that was running unpatched version of a Microsoft operating system. His reports from the vendor was that the workstations should have not been connected to the public network due to that reason (Keen, 2010).

Griffin Hospital

In 2010 a contracted Radiologist that was previously working at Griffin Hospital accessed over nine hundred patient records after his contract had ended. The Radiologist accessed the PACS remotely. Although the former employee's access had been disabled in PACS he was able to log in with usernames and passwords of other Radiologists. During his contracted employment the Radiologist was able to obtain the credentials of his colleagues and use them later (Domino, 2010).

Security Controls for PACS.

PACS is the centralized hub for diagnostic imaging within a medical facility and therefore quick access to the data is required by a majority of the physicians and clinical staff. Protecting the PACS software is key to protecting the DICOM data stored either in a local storage device or in the cloud. In either case, unauthorized access can cause repercussions that can degrade the system integrity and confidentiality of patient data.

Like any other information system, patch management, security templates, and anti-malware software is required to prevent attacks from adversaries who seek unpatched systems to exploit. Information Technology departments should always have the ability to implement security changes to PACS but also, they should consult with the administrators over the PACS software to ensure that patient care is not affected by the changes (Chee,2018).

Routine audits of logins to PACS and who is accessing what data should be performed to help mitigate such events at the one that occurred at Griffin Hospital. Logs should include IP, data/time, user account, and what data is being accessed. For optimal discovery of potential unauthorized access, the use of a heuristic analysis software should be used. This solution would obtain a baseline of user's activity and if events outside the baseline occur it would notify the proper personnel to investigate.

Conclusion

The medical industry has been revolutionized by innovations such as DICOM, HL7, PACS, and cloud-based technologies, in hindsight, prior to the implementations of these protocols and information systems security of the data was not a factor. As Radiology departments added newer imaging technology the requirement for efficient methods to transmit clinical data between physicians followed. Decades of developing protocols and information systems that lack modern day security controls has caught up with the industry. In reality, the need to protect systems in radiology has never been greater. There is not a system or workflow that has not been exploited by some type of threat and this is obvious by events such as Orangeworm, MedJack, the issues with HL7 brought to the attention of attendees of Black Hat, and the multiple security incidents described in this writing. Even though no system will ever be completely secure, insider attacks, zero-day exploits, and overlooked security holes will always catch the most diligent security team off guard. Yet security controls can assist in mitigation of such risks.

In the final analysis the security controls that employ the usage of network level encryption to protect data in motion, disk encryption to protect data a rest and controls to prevent unauthorized access, alteration, and data loss always should be implemented. Verification steps must be configured to ensure that all diagnostic images are stored successfully to the DICOM destination. Most importantly, the patient data on both HL7 and DICOM endpoints must maintain integrity to keep patient safety intact. Above all else, due diligence is required to preserve the CIA triad.

References

Accenture. (2018, March 01). One in Five Health Employees Willing to Sell Confidential Data to Unauthorized Parties, Accenture Survey Finds. Retrieved October 9, 2018, from https://newsroom.accenture.com/news/one-in-five-health-employees-willing-to-sell-confidential-data-to-unauthorized-parties-accenture-survey-finds.htm

Adams, J., & Kuhnen, G. (2017, December 14). Why ending net neutrality will likely be bad news for health care. Retrieved from https://www.advisory.com/research/health-care-it-advisor/it-forefront/2017/11/net-neutrality

Agrawal, A. (2014). *Patient Safety a Case-Based Comprehensive Guide*. New York, NY: Springer New York.

Al-Enazi, T., & El-Masri, S. (2013, October 25). HL7 Engine Module for Healthcare Information Systems. Retrieved August 21, 2018, from https://link.springer.com/article/10.1007/s10916-013-9986-8

Alpine Security. (2018, March 29). Most Dangerous Hacked Medical Devices. Retrieved October 10, 2018, from https://www.alpinesecurity.com/blog/most-dangerous-hacked-medical-devices

Arndt, R. Z. (2017, December, 14). How will telemedicine be affected by the repeal of net neutrality? Retrieved from http://www.modernhealthcare.com/article/20171214/NEWS/171219943

Ashford, W. (2011, June). How to combat advanced persistent threats: APT strategies to protect your organization. Retrieved November 11, 2018, from https://www.computerweekly.com/feature/How-to-combat-advanced-persistent-threats-APT-strategies-to-protect-your-organisation

Auger, G. & Cardinal, S. (Host). (2018, August 15). *Biomedical Integrity Attacks, Jeremiah Grossman Interview, and Asset Inventory Reflection* [Audio podcast]. Retrieved August 25, 2018, from https://podcast.musc.edu/podcast/infosec/e37-infosecicu/

Baxter, B., & Zeleznik, M. (1983). Communication and storage Protocols for PACS. *Computer, 16*(8), 31-36. doi:10.1109/mc.1983.1654466

Beek, C. (2018, July 03). McAfee Researchers Find Poor Security Exposes Medical Data to Cybercriminals. Retrieved August 22, 2018, from https://securingtomorrow.mcafee.com/mcafee-labs/mcafee-researchers-find-poor-security-exposes-medical-data-to-cybercriminals/

Branstetter, B. F. (2009). Practical imaging informatics: Foundations and applications for PACS professionals. New York: Springer.

Brazzoli, F. (2017, December 15). Healthcare organizations voice worry over end of net neutrality. Retrieved from https://www.healthdatamanagement.com/news/healthcare-organizations-voice-worry-over-end-of-net-neutrality

Chee, A. (2018). Rethinking PACS security -- the unusual suspects. [online] Diagnostic Imaging. Available at: http://www.diagnosticimaging.com/pacs-and-informatics/rethinking-pacs-security-unusual-suspects [Accessed 22 Oct. 2018].

Dameff, C., Bland, M., Levchenko, K., & Tully, J. (2018, June 6). Pestilential Protocol: How Unsecure HL7 Messages Threaten ... Retrieved October 9, 2018, from http://acsweb.ucsd.edu/~mbland/pestilential_protocol.pdf

Davis, J. (2018, April 19). SamSam ransomware hackers still targeting healthcare, HHS warns. Retrieved October 10, 2018, from https://www.healthcareitnews.com/news/samsam-ransomware-hackers-still-targeting-healthcare-hhs-warns

Davis, J. (2018, April 12). 63,500 patient records breached by New York provider's misconfigured database. Retrieved October 9, 2018, from https://www.healthcareitnews.com/news/63500-patient-records-breached-new-york-providers-misconfigured-database

Domino, D. (2010, March 31). Radiologist hacks hospital PACS to access patient records. Retrieved November 11, 2018, from https://www.auntminnie.com/index.aspx?sec=sup&sub=pac&pag=dis&ItemID=90114

Donovan, F. (2018, August 08). 19K Orlando Orthopaedic Patients At Risk from Lax Vendor Security. Retrieved November 11, 2018, from https://healthitsecurity.com/news/19k-orlando-orthopaedic-patients-at-risk-from-lax-vendor-security

Elm, H. (2008). Do we really need standards in digital image management?. Biomedical imaging and intervention journal, 4(4), e20.

Fu, K., & Blum, J. (2013). Controlling for cybersecurity risks of medical device software. *Communications of the ACM, 56*(10), 35. doi:10.1145/2508701

Gibson, S. (2018, October 2). Security Now - Episode #683 [Audio blog post]. Retrieved October 10, 2018, from https://media.grc.com/sn/sn-683.mp3

Grimes, H. J. (2007). Security Sickness in the Health Networks. *Information Systems Security, 16*(6), 355-356. doi:10.1080/10658980701752864

Haselhorst, D. (2017, September 12). HL7 Data Interfaces in Medical Environments: Understanding the Fundamental Flaw in Healthcare. Retrieved October 9, 2018, from https://www.sans.org/reading-room/whitepapers/vpns/hl7-data-interfaces-medical-environments-understanding-fundamental-flaw-healthcare-38005

HHS Office of the Secretary, Office for Civil Rights, & OCR. (2013, July 26). Summary of the HIPAA Security Rule. Retrieved October 9, 2018, from https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html

HIPAA Journal. (2018, April 26). How to Defend Against Insider Threats in Healthcare. Retrieved October 9, 2018, from https://www.hipaajournal.com/how-to-defend-against-insider-threats-in-healthcare/

Kartawiguna D and Georgiana V. (2013). Implementation of DICOM Modality Worklist at Patient Registration Systems in Radiology Unit. EPJ Web of Conferences, 68 (28), 1-8

Keen, C. E. (2010, January 29). Conficker worm invades U.K. hospital IT network. Retrieved November 11, 2018, from https://www.auntminnie.com/index.aspx?sec=sup&sub=pac&pag=dis&ItemID=89274

Kuzmak, P. M., & Dayhoff, R. E. (2001). Minimizing Digital Imaging and Communications in Medicine (DICOM) Modality Worklist patient/study selection errors. Journal of Digital Imaging, 14(S1), 153-157. doi:10.1007/bf03190323

Leaf, C. (2017, December 14). Brainstorm health: medical devices, net neutrality and health research, alphabet anti-aging startup. Retrieved from http://fortune.com/2017/12/14/brainstorm-health-daily-12-14-17/

Lui, B., Zhou, Z., & Huang, H. (2006, January 19). A HIPAA-Compliant Architecture for Securing Clinical Images. Retrieved November 11, 2018, from https://www.ncbi.nlm.nih.gov/pmc/articles/PMC3045193/

Luong, H. (2017, December 13). Net Neutrality and Healthcare. Retrieved from https://pha.berkeley.edu/2017/12/13/net-neutrality-and-healthcare/

Mahlaola, T. B., & Dyk, B. V. (2017). Password compliance for PACS work stations: Implications for emergency-driven medical environments. *South African Journal of Bioethics and Law, 10*(2), 63. doi:10.7196/sajbl.2017.v10i2.00600

Mann, K. S., & Bansal, A. (2014). HIS Integration Systems Using Modality Worklist and DICOM. Procedia Computer Science, 37, 16-23. doi:10.1016/j.procs.2014.08.007

Medema- Philips, J., Horn, R., & Tarbox, L. (2018). DICOM Security. Digital Imaging and Communications in Medicine (DICOM), 247-261. doi:10.1007/978-3-540-74571-6_11

Mildenberger, P., Eichelberg, M., & Martin, E. (2001). Introduction to the DICOM standard. European Radiology, 12(4), 920-927. doi:10.1007/s003300101100

Moggridge, J. (2017). Security of patient data when decommissioning ultrasound systems. *Ultrasound, 25*(1), 16-24. doi:10.1177/1742271x16688043

Moon, D., Pan, S. B., & Kim, I. (2016, September 03). Host-based intrusion detection system for secure human-centric computing. Retrieved from https://link.springer.com/article/10.1007/s11227-015-1506-9

NEMA DICOM. (n.d.). History. Retrieved October 9, 2018, from https://www.dicomstandard.org/history/

Newman, L. H. (2017, June 03). Medical Devices Are the Next Security Nightmare. Retrieved October 20, 2018, from https://www.wired.com/2017/03/medical-devices-next-security-nightmare/

Oemig, F., & Snelick, R. (n.d.). Healthcare Interoperability Standards Compliance Handbook - Conformance and Testing of Healthcare Data Exchange Standards | Frank Oemig | Springer. Retrieved August 21, 2018, from https://www.springer.com/us/book/9783319448374

Oglevee, C., & Pianykh, O. (2014). Losing Images in Digital Radiology: More than You Think. Journal of Digital Imaging, 28(3), 264-271. doi:10.1007/s10278-014-9748-2

Oosterwijk, H. (1999, October 1). DICOM Update: VA issues updated DICOM requirements ... Retrieved November 11, 2018, from http://www.diagnosticimaging.com/article/dicom-update-va-issues-updated-dicom-requirements

Pianykh, O. S. (2008). Digital imaging and communications in medicine: A practical introduction and survival guide. Berlin: Springer.

Pratt, M. K. (2017, June 6). Healthcare CIO advocates a faster move to the cloud. Retrieved from https://www.computerworld.com/article/3199649/it-management/healthcare-cio-advocates-a-faster-move-to-the-cloud.html

Quest (2017) Protecting data in the healthcare Industry. [White Paper]. Retrieved August 22, 2018, from https://www.quest.com/whitepaper/protecting-data-in-the-healthcare-industry8128353/

Ragan, S. (2016, March 28). Ransomware attack hits MedStar Health, network offline. Retrieved October 9, 2018, from https://www.csoonline.com/article/3048825/security/ransomware-attack-hits-medstar-health-network-offline.html

Relias. (2015, September 1). Incorrect registration data is a significant patient safety worry. Retrieved October 9, 2018, from https://www.reliasmedia.com/articles/136101-incorrect-registration-data-is-a-significant-patient-safety-worry

Selvamani, K., & Jayanthi, S. (2015). A Review on Cloud Data Security and its Mitigation Techniques. Procedia Computer Science, 48, 347-352. doi:10.1016/j.procs.2015.04.192

Smith, J. J., & Berlin, L. (2008, December 1). PACS and the Loss of Examination Records. Retrieved November 11, 2018, from https://www.radiologytoday.net/archive/rt_120108p44.shtml

Spitzer J. (2017, December 14). 3 way the net neutrality repeal could affect healthcare. Retrieved from https://www.beckershospitalreview.com/healthcare-information-technology/3-ways-the-net-neutrality-repeal-could-affect-healthcare.html

Sullivan, T. (2017, May 26). Cloud computing will change the nature of hospital IT shops. Retrieved from http://www.healthcareitnews.com/news/cloud-computing-will-change-nature-hospital-it-shops

Symantec. (2018, April 23). New Orangeworm attack group targets the healthcare sector in the U.S., Europe, and Asia. Retrieved October 10, 2018, from https://www.symantec.com/blogs/threat-intelligence/orangeworm-targets-healthcare-us-europe-asia

Trapx. (2017, August). Healthcare - Real Healthcare Security. Retrieved October 10, 2018, from https://trapx.com/wp-content/uploads/2017/08/Case_Study_TrapX_Healthcare_MEDJACK_X-RAY.pdf

University of California - San Diego. (2018, August 29). How unsecured medical record systems and medical devices put patient lives at risk. ScienceDaily. Retrieved October 9, 2018 from www.sciencedaily.com/releases/2018/08/180829115554.htm

Veeramani, S., Masood, M. N., & Sidhu, A. S. (2014). A PACS alternative for transmitting DICOM images in a high latency environment. 2014 IEEE Conference on Biomedical Engineering and Sciences (IECBES). doi:10.1109/iecbes.2014.7047657

Zetter, K. (2017, June 03). It's Insanely Easy to Hack Hospital Equipment. Retrieved November 11, 2018, from https://www.wired.com/2014/04/hospital-equipment-vulnerable/