Sami Tanhua

Networking Solution in Regulated Environment

Metropolia University of Applied Sciences

Bachelor’s Degree

Information Technology

Bachelor’s Thesis

20.02.2022

Abstract

Author:	Sami Tanhua
Title:	Networking Solution in Regulated Environment
Number of Pages:	34 pages
Date:	20 February 2022

Degree:	Bachelor of Engineering
Degree Programme:	Information Technology
Professional Major:	Health Technology
Supervisors:	Markus Paasi, Software Manager Sakari Lukkarinen, Senior Lecturer

The main goal of the study was to evaluate the feasibility of integrating a new medical device to the intended environment. The feasibility would be defined by the cybersecurity level of the device and its conformance to regulations. The intended implementation network for the device is hospital/clinic network. Such networks are highly regulated as the functionality of the machines and data going through the network are very sensitive. The reason behind the evaluation need was that the new Medical Device Regulation (EU) 2017/745 has come in affect in EU area and supporting standards are being published to support the regulation. Some of the standards address how cybersecurity should be taken into consideration.

The evaluation was carried out by comparing the current networking model to the regulations and other relevant sources that define cybersecurity needs of the environment. To limit the size of evaluable sources only the standard IEC 81001-5-1 was reviewed.

The main objects under the evaluation were the encryption protocol, physical components, medical device software and third-party software. Also, the processes during the production and life cycle of medical device that relate to cybersecurity were under evaluation.

Analysis of the regulation and related material produced a result that indicated the encryption protocol intended to be used in the networking model should be changed. The review of the standard unveiled that additional processes related to the security in development and the life cycle support of the device must be produced to claim conformance to the new generation of standards.

The results of the evaluation were presented to the medical device manufacturer and the modifications of the networking model and processes defined by the standard IEC 81001-5-1 were taken under advisement.

Keywords: Medical device, IEC81001-5-1, Cybersecurity, medical device regulation

Tiivistelmä

Sivumäärä:	34 sivua
Aika:	20.02.2022
Tutkinto:	Insinööri (AMK)
Tutkinto-ohjelma:	Tieto- ja viestintätekniikka
Ammatillinen pääaine:	Hyvinvointi- ja terveysteknologia
Ohjaajat:	Software Manager Markus Paasi Lehtori Sakari Lukkarinen

Avainsanat: Lääkinnällinen laite, IEC81001-5-1, Kyberturvallisuus, lääkinnällisten laitteiden säädökset

Opinnäytetyön päätavoitteena oli arvioida mahdollisuutta integroida uusi lääkinnällinen laite sille aiottuun asennusympäristöön. Toteutettavuus määritellään laitteen kyberturvallisuustason ja määräystenmukaisuuden perusteella. Laitteen suunniteltu toteutusverkko on sairaala-/klinikkaverkko. Tällaiset verkot ovat erittäin säänneltyjä, koska verkon läpi kulkeva tieto on todella arkaluontoista, ja verkossa sijaitsevien laitteiden vahingoittumisesta voisi syntyä vaurioita potilaille. Arviointitarpeen syynä oli se, että uusi lääkinnällisiä laitteita koskeva asetus Medical Device Regulation (EU) 2017/745 on tullut voimaan EU:n alueella ja asetuksen tueksi julkaistaan tukistandardeja. Osassa näistä standardeista käsitellään sitä, miten kyberturvallisuus olisi otettava huomioon.

Arviointi tehtiin vertaamalla nykyistä verkkomallia säädöksiin ja muihin asiaankuuluviin lähteisiin, jotka määrittelevät ympäristön kyberturvallisuustarpeet. Arvioitavien lähteiden koon rajoittamiseksi työssä tutkittiin vain standardia IEC 81001-5-1. Arvioinnin pääkohteet olivat salausprotokollat, fyysiset komponentit, lääkinnällisten laitteiden ohjelmistot ja kolmansien osapuolien ohjelmistot. Myös kyberturvallisuuteen liittyviä lääkinnällisten laitteiden tuotannon ja elinkaaren prosesseja arvioitiin.

Regulaatioiden ja kyberturvallisuuteen liittyvien aineistojen analysoinnin tuloksena oli, että verkkomallissa käytettävä salausprotokolla ei ole soveltuva sille tarkoitettuun tehtävään. Korvaavaa salausprotokollaa ehdotettiin. Standardin tarkastelun tuloksena oli, että laitteen kehittämisen ja elinkaaren tuen turvallisuuteen liittyviä lisäprosesseja on tuotettava, jotta voidaan ilmoittaa tuotteen olevan vaatimusten mukainen uuden sukupolven standardeille.

Arvioinnin tulos esiteltiin lääkinnällisen laitteen valmistajalle. Verkkomallin muutosehdotukset huomioitiin ja aloitettiin kehitysprosessi salausprotokollan integraatiosta tuotteeseen. Standardissa IEC 81001-5-1 määritellyt prosessien muutokset otetaan huomioon tulevaisuudessa, kun uusia standardeja noudattavia prosesseja kehitetään.

Contents

List of abbreviations

PACS Picture archiving and communication systems, used in medical data storage.

DICOM Digital Imaging and communications in Medicine standard. Regulating communication and management of medical imaging and related data.

MDR Medical Device Regulation. EU regulation 2017/745.

HTTP Hypertext Transfer Protocol, protocol used in web and browser applications to convert transferred data to the used application.

REST Representational state transfer, based to HTTP architecture model and used to connect software components between systems.

API Application programming interface, Connection between programs/computers that allows communication and interaction between the systems.

HDO Health Delivery Organisation, an organisation that deliverers healthcare service, for example Hospital or Clinic.

UI User Interface.

TLS Transport layer security, cryptographic protocol used to provide security in communication over a network.

Cybersecurity All the actions and practices committed to protecting systems networks and programs from digital attacks and unwanted use.

DICOM Client Program that can interact with and import DICOM data from PACS server

ISO Standard Internationally recognised document that defines guidelines on how certain matter should be completed.

SQL Structured Query Language, Standardized programming language that is used for database management.

DMS Data management server, a part of the networking model that handles the data management of the product.

1 Introduction

The objective of this study was to make an evaluation of a new networking solution used in a medical device. The device is used in a highly regulated environment. The main focus is on the conformance of standards IEC 81001-5-1 “Health software and health IT systems safety, effectiveness and security” and DICOM Standard ISO 12052:2017. Because of the high number of regulations and standards that affect the evaluation target, other related regulations and standards are not included in the evaluation of the networking model.

The study was commissioned by a Finnish health technology company that develops medical devices to diagnostical and therapeutical uses.

The object networking solution that the study focuses on is composed of internal connections of medical devices and connections between the medical device and devices situated in the hospital network, primarily PACS Server.

The study evaluates all parts of the networking solution, the main parts are communication protocols, physical components related to networking and configuration of the used systems/components. The implementation of the end product to the intended area of operation is evaluated and improved by analysing and altering the networking model.

The study resulted in an initial evaluation of the product and articulates possible changes that may be implemented to the final product and development process. The final product of the study was presented to the commissioner´s associates.

2 Background

This chapter goes through the medical device legislation and harmonized standards, as well as the medical device regulation (MDR). Also, background for related networking protocols and basics of networking safety are introduced. The topics are introduced in order to give an understanding of the related legislation and technology discussed in the study.

2.1 Medical Device Legislation and Harmonized Standards

Medical device market is highly regulated because of the highly sensitive operation environment and the delicate data used and generated by the devices. All the devices that work in the medical device field need to provide adequate safety, effectivity and security measures that are defined by standards and regulations. Different countries have different regulations and standards in effect. In this thesis the focus is on regulations and standards used in EU.

The standards and regulations keep changing as the field is changing and new possible defiances are detected. Currently the regulation field is at a changing period as new, more comprehensive regulations and standards are being developed and released. In the EU area the new Medical Device Regulation (MDR) came to effect on 26th of May 2021. [5] A new set of harmonised standards related to MDR are also being released to provide additional security and safety in the medical device field. [1; 6; 7]

2.2 Medical Device Regulation (MDR)

Medical device regulation (EU) 2017/745 defines how medical device manufacturers have to operate when producing and/or selling medical devices in an EU regulation area. The regulation defines what processes must be completed to make the device safe and to make the development and operational support processes transparent. The MDR defines the aspects that must be implicated but does not define the specific details how this has to be done, it uses related standards to this. Some of the MDR related standards have not yet been published.

The MDR replaces the old medical device directive used for the same purpose. The MDR only applies to new products that have been released and sold after the coming effect of the MDR. The products developed before the application of the MDR can be sold and supported using the previous regulation if no significant changes to the existing product have been made. [1]

In part the MDR has come in effect, but the manufacturers have time to apply the changes to new products.

2.3 Health System Security Standard IEC 81001-5-1

Standard IEC ISO 81001 “Health software and health IT systems safety, effectiveness and security”, is a new generation standard that is going to be added to the new medical device regulation. The standard sets guidelines and means that the health system manufacturer needs to implement to the system for adequate cybersecurity. The focus of the standard is on software security and related tasks that support the security aspects of software development. In this thesis the focus is on the standards series 5 part 1 “Security — Activities in the product life cycle”. In the future the series is going to contain more parts that set new guidelines on different security aspects.

Many aspects of the security activities stated in the standard IEC 81001 refer to standard IEC 62443-4-1 ”Security for industrial automation and control systems”, and it is also stated that implementation of the processes, activities and tasks of the IEC 81001-5-1 is sufficient to implement the process requirements of the IEC 62443-4-1 but does not achieve full conformity. [2, chapter 1.3]

The new set of standards is set to be adopted in May 2024. [1,6,7]

Some other related standards are also currently under development and the standard IEC/TR 60601-4-5 also sets technical security specifications to cybersecurity implementation.

2.4 Picture Archiving and Communication Systems (PACS)

PACS is a software solution that provides archiving solution in hospital environments. The data is stored in the DICOM format.

PACS provides a data storage solution to all the hospitals' or clinics' medical devices that use patients' data as MRI, x-ray, patient documents and other similar sensitive data. Centralized data storage makes sharing the data easier between different devices and programs.

Using a centralized storage point to store the delicate patient data makes the data storing more secure but cybersecurity is still a major issue. Hospital networks are often divided into smaller sections to make the network more secure and the PACS systems are often also divided into these sections. PACS servers can also be connected with the other PACS servers that are located in the different sections. [15]

2.5 General Data Protection Regulation (GDPR)

The general data protection regulation is a relatively new regulation that defines how personal data can be used, processed and stored. Personal data includes any data where the identity of the person can be defined and all of the data that can be identified to be patients' personal data. The most relevant task defined by the regulation in regards of this thesis is that the regulation defines that the medical data that includes identification information of the person should be secured, and the handler organisation must have defined security procedures in place. The regulation also defines that the identification data should be kept separate from the medical data as much as possible. The handler organisation should also have a way to delete persons data if the person so wants. [4]

2.6 DICOM

DICOM standard “ISO 12052:2017 Health informatics — Digital imaging and communication in medicine (DICOM)”, is a standard that defines communication protocols and related configurations options that make possible to generate a connection with other devices that also declare conformance with the DICOM standard. DICOM data format is very commonly used in medical devices as it provides a standardized way of data that can be stored and used in different devices.

The DICOM standard also defines the format of the data, including the image data and all of identification data for example patients name, date and where the file was created.

The DICOM standard defines some aspects that provide security against possible attacks, but these aspects are not sufficient on their own to protect the systems from attacks. The standard does provide references to possible methods of data transfer security protocols and security profiles that are defined in the DICOM standard. DICOM implementation can claim conformance to one or more secure use profile. DICOM conformance declaring system does not have to declare conformance to any of the provided security profiles.

There are many security aspects that the DICOM standard does not discuss and it is possible that future standards may define some methods that need to be implemented to DICOM communication protocols to claim full conformity.

DICOM data gets some of its value from the way the data contains the picture and the related patient data in the same package. This creates a problem to conformance to the GDPR as the patient data and picture data cannot be separated so extra security protocols has to be implement when storing and transporting DICOM data. [11]

2.6.1 DICOM Conformance Statement

The function of the DICOM conformance statement is to narrate how the system complies with the standard, how the system operates and how it can be implemented to a network. The conformance statement can be a quick way to determine if the system is secure enough to be connected to a hospital/clinic network and possible technical implementation difficulties can be noticed before purchase, but it does not contain any information about other cybersecurity methods that are not defined in DICOM standard. The conformance statement may include minimum cybersecurity methods that have to be implemented when integrating the conformance claiming software to a network, for example if the network is isolated or is placed behind a firewall. [11, part 2]

2.7 Networking Safety

Networking safety includes aspects such as defining who has access to the network and different systems in the network. Limiting access to the network can be done for example by not physically connecting the network to other networks, connecting the local network to the internet or limiting the connection by directing all of the traffic though a firewall that blocks the connections that are not defined to have access.

When a device tries to connect to another device it has to know the address of the device and a specific port where the receiving device is waiting to receive a connection request. All computers include these ports, and all the ports can be configurated individually, for example to be closed or to accept only specific request. Also outside going connection from a device use similar ports. For example, a computer could be configurated to have none of the ports open to outside connections, but it could still be connected to another device if the outgoing port is configurated to accept the connection. This kind of connection would make the device relatively secure against cyberattacks, as it does not allow any connections that are started externally of the device.

Limiting access to a specific system on the network can also be done using a physical or software firewall. The firewalls can scan the received data and block if any unwanted data type is detected. Using a physical firewall to protect sensitive devices can hide the addresses of the devices behind the firewall, as the firewall blocks any unwanted connection attempt before any connections is created between the sensitive devices.

2.8 Communication and Encryption Protocols

One of the objects here is to investigate the different kinds of communication protocols feasibility of use in the intended network environment. The following sections describe a couple of different data transfer protocol types that could be used in the final networking model configuration.

2.8.1 Transmission Control Protocol (TCP)

TCP is a communication protocol that is used in most of the communication on the internet. The TCP protocol includes mechanism that observes that the data is correctly received and if data is lost the lost packets can be sent again. The TCP protocol is a transport layer protocol that only handles the data movement and therefore it does not provide security to the data transfer and needs to be used with extensions. The TCP protocol is almost always used with encrypting protocol. The DICOM communication uses the TCP protocol in sending the data through the network after the connection is established with a confirmation protocol. [9]

2.8.2 Virtual Private Network (VPN)

Virtual private network protocols are a method of providing a secure connection between hosts. VPN protocols create a connection between two different devices that can be in different networks. VPN protocols differ from other encryption protocols because in addition to the data encryption the source and destination addresses are encrypted. Hiding the addresses of the systems could provide more security because the attacker would not know the network or address where the device is situated.

VPNs could be used to provide more security to connections between the systems inside the hospital environment and to connection that are made between networks, for example if a medical device is connected to a system outside the hospital network the location of the medical device can be hidden.

There exist many different VPN protocols that have slightly different methods and algorithms to provide security and reliability. Naturally also, the security levels differ between the different protocols. [16]

2.8.3 TLS Encryption Protocol

Transport layer security (TLS) encryption protocol is the most widely used encryption protocol, for example the TLS is used in secured HTTP connections (HTTPS). TLS Encrypts the data but keeps the destination and source destinations available. The TLS protocol provides the encryption by pre shared keys that can be used to encrypt and decrypt the data. These keys are installed to the systems during the installation and the IP addresses of the devices included in the connection are also defined in the implementation process. Making the protection secure as only the systems with the defined IP addresses have the ability to access the data. The keys are not accessible to normal users and new keys can only be created with a root key. [9]

TLS encryption is used in a DICOM standard defined transfer mechanism that is used to provide more security to the connection. This makes it very potential protocol to be used in the system. [11, part 15]

3 Methods

This chapter introduces the methodology applied in the present study together with the networking model and other aspects that are under evaluation. The cybersecurity evaluation is performed for the described model.

3.1 Formative Evaluation

The chosen method of evaluation here is formative evaluation. The networking model and the relevant aspects of the systems are evaluated, and possible solutions and improvements are stated. The evaluation is done by comparing the product to relevant regulations, standards and relevant information that was learned when working with different hospitals on installing devices. [17]

3.2 Networking Model

This study uses a premade model of a possible networking solution that could possibly be used in the final product if it provides adequate security, effectivity, and safety. These aspects are defined by the regulations and tasks that are defined by relevant standards and the intended use.

The model might have more implementation configurations in the future but only the described model configuration is analysed here. Figure 1 shows the networking model.

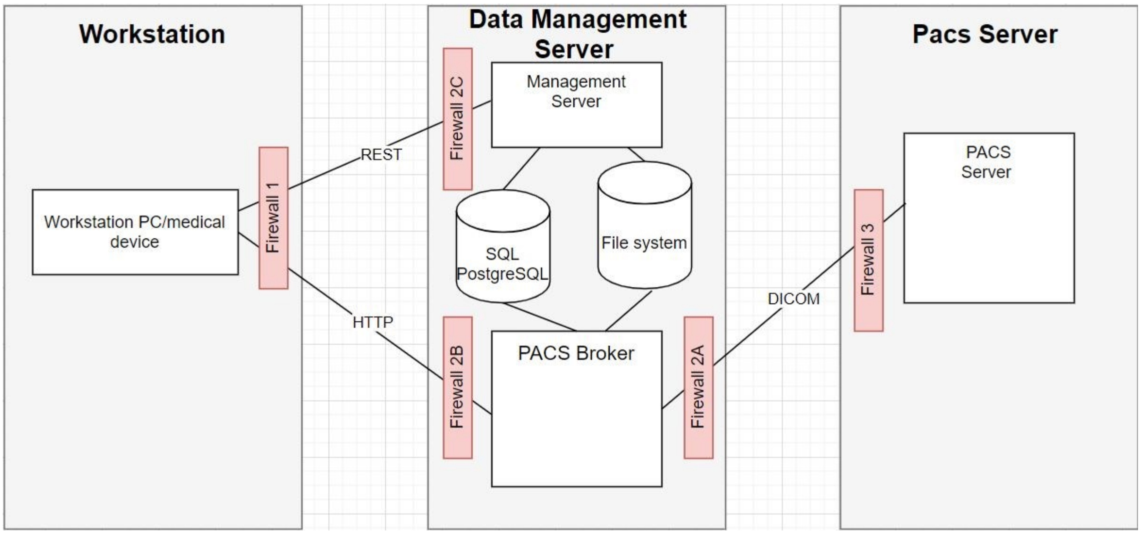

Figure 1: Networking model

The network model includes 3 devices: workstation, data management server and Hospital PACS server. The devices are connected to each other with various connection protocols. Figure 1 demonstrates how the systems are connected to each other.

The following chapters describe in more detail the architecture of the networking model seen in Figure 1. Many aspects of the device do not affect the cybersecurity, therefore the descriptions include only the aspects related to cybersecurity.

3.2.1 Workstation

The workstation is the medical device that uses the medical data in diagnostical and therapeutical purposes. Medical data is normally only stored on the workstation system during the use of the system. The system is based on a windows platform. All the network connections to the workstation come through a physical firewall component, and the incoming data comes from the data management server. The workstation does not contain any patient data on the longterm but the main threat in case of an attack would be that the systems operation could get compromised and put the safety of the patient at risk.

In the model the workstation has two network connections to data management servers both software components. Each connection is made though a secure port in the firewall. Connection to the management server is made with a REST protocol connection, as can be seen in Figure 1. All the patient data between the workstation and data management server is sent though this connection. The connection to the PACS broker is made with HTTP protocol, the connection provides an API from the data management server to the workstation from this application interface the user can request queries and data from the Hospitals PACS server. The workstation does not have any ports open to outside connections and all connection between the workstation and data management server are initiated by the software inside the workstation.

3.2.2 Data Management Server (DMS)

Data management server contains only software and should not be identified as a physical system. The DMS software can be installed on hospital’s own system or on a developer’s reference windows 10 PC/desktop that has been installed in the network. The data management system stores all the patient data that the medical device used, created, or will use.

The object of the DMS is to transfer and store data. The server is comprised of four software parts: Management server, PACS broker, SQL Postgres database and a datafile.

Management server is software that sends the patient data from the management server to the workstation and provides a user interface where data management server can be configurated.

PACS broker is software that connects to PACS server and makes queries of the available DICOM data, imports the DICOM data from the PACS server and forwards it to the storage systems. The PACS broker also provides the user interface that is used to select the query parameters and data to be imported from the PACS server (connection 2).

The data storage system in the management server is comprised of two components. The SQL database is used to store and define all of the aspects of the data, for example data IDs and patient IDs. This information is used to control and identify the stored data. The second part is the datafile that includes all the DICOM files, the datafile is a normal windows data folder that cannot be accessed by the user. The system is based on a windows platform. The DMS server has 3 points of connections.

3.2.3 Hospital PACS

The hospital PACS server is a component of the network that cannot be modified, and the networking configuration is defined by the hospital's server configuration and the rules configuration and cybersecurity aspects that the hospital defines. Every hospital could have different specifications for the PACS. The safety and cybersecurity of the hospital's server and other components such as the routers are not taken into consideration here as the hospital is responsive of those components.

The DMS is connected to the hospital's PACS only with a DICOM format connection. The data can be moved both ways and both servers have access to each data folder.

Medical devices that require network connection for example to PACS server are usually connected to a separate network that includes only medical devices and related systems. This network can be isolated from the open internet but this can vary between hospitals/clinics. The hospital usually contains another network that is used by systems that require connection to the open internet.

3.3 Physical Parts under Cybersecurity Evaluation

Physical components included in the system can also affect the safety and cybersecurity of the system and therefore should be included in the investigation and risk assessment.

Also, the configuration of the system that uses these physical components affect the safety. For example, the settings that define when a port can be accessed and what identifications are needed before operating.

Only the physical parts of the workstation can be evaluated, as the physical parts of the data management server cannot be investigated as the physical components are not defined. Also, the data management server can be implemented to hardware that is owned by the hospital. The PACS physical components cannot be evaluated as it is owned by the hospital.

3.3.1 USB Ports

USB ports are a major security concern on a medical device as they could be used as an access point to the system if an attacker would have physical access to the system, compromising the patient data and the safe operation of the system.

The workstation contains normal USB 3.0 ports that affect the cyber security of the system. The USB ports are located mainly inside the system and cannot be accessed easily, one USB port is easily accessible. The new generation standards that define cybersecurity related aspects, e.g. the ISO 81001-5-1, define what measure the manufacturer must implement to make the USB ports secure and acceptable.

The server also could contain USB ports but the device that includes the software is not defined, therefore the mentioned part will not be included in the evaluation. The cybersecurity of the server device falls under the hospitals or clinics responsibility area.

3.3.2 DVD Drive

The workstation includes a DVD drive, the driver is situated in the PC panel that can be accessed. The DVD drive is implemented to the system because, using DVD´s as a storage platform for MRI files is still common in hospitals/clinics. The DVD drive is one of the accessing points that could be used in an attack to access the data situated in the workstation.

3.3.3 Firewalls

The network is includes one physical firewall. Two types of physical firewalls could be used. A simple hardware firewall that is configurated to allow specific connections to known destinations to get through, this kind of firewall does not scan the files. The second type of firewall is more advanced so-called next generation firewall that has some internal processing capabilities. This kind of firewall usually has a capability to receive encrypted data from different protocols, scan the data for unwanted types of data and the firewall could be modified easier to receive different kinds of connections, for example to receive VPN protocols. [8] Decision of the specific firewall model that is going to be used in the system has not been made at the time of writing the thesis.

Different models could affect what VPN protocols can be used, as some firewalls support VPN protocols and can decrypt the data as it arrives to the firewall. If a firewall does not support the used VPN protocol limits the configuration and modification possibilities during installation.

3.4 Model Configuration

The proposed model uses a VPN protocol to provide security in all the connections. The VPN protocol has not been defined.

The systems do not have any connections to external hosts and services that are outside the local network, meaning that the system is not connected to the open internet or any other device outside the local network.

4 Evaluation of Networking Model

This chapter introduces the evaluations of the networking model and the related components by comparing the model to the standards and the known safety aspects. Also, possible challenges that may affect the development and implementation are discussed.

4.1 Realization Challenges

Evaluation of the cybersecurity is very complex. All the physical and software components related to the cybersecurity need to be evaluated and possible mitigations needs to be implemented. Exposed components that are essential to the system operation need to be investigated for possible remaining risks.

Finding a suitable encryption protocol for the systems network connections. Encryption protocol is a critical aspect of the products cybersecurity, so a comprehensive evaluation of possible protocols should be completed before final decision is made.

Defining what is the adequate security level. Penetration tests and documentation are needed. These tasks have not been completed before in this security aspect and therefore tasks for testing and documentation needs to be defined.

Balancing between security and usability. When implementing new security methods, it should be kept in mind that the cybersecurity methods should not affect the usability of the system, for example implementing password confirmation or other user verification process to the system the usability should not be significantly affected.

Verification of modifications. All software or configuration changes need to be tested and verified before a device with the changes can be installed and used in the clinical use. This means that implementing a change could take a long time and a lot of working hours.

Updates and security update implementation. Applying virus protection software to workstation and data management server could improve the security but implementing third-party software to the system is a long process. Virus protection software needs to have regular updates to provide adequate security. Testing and verifying every security update on the system is not practical. Also implementing security updates to a system frequently is not practical as the updates would need to be done on site by trained personnel, as defined by the standard IEC 81001-5. Implementing a remote access to the system for such updates could be done, but such a connection could create new cybersecurity risks and the risks for the system would have to be revaluated.

Implementation environment variation. Implementation might be hard as the environments, preferred protocols and security guidelines can differ between hospitals/clinics especially when the system is implemented to a hospital/clinic situating in a country that does not have similar regulation level as the EU or USA. In this kind of situation, the network may not have adequate cybersecurity methods implemented.

Predicting how the product conforms to the future regulations. The changing regulations might force the manufacturer to change the product, medical device development is a long process and changing the product after the release is also very complicated and time consuming, so in the development the manufacturer must try to predict what kind of product could be used and sold for as long as possible. Usually, the products are supported for 7-10 years after release.

All of the aspects listed above should be taken into consideration in cybersecurity risks evaluation and when further developing the product. The aspect should also be considered when implementing new features to the product. Also, it should be noted that implementing a new feature may introduce new challenges.

4.2 IEC 81001-5-1 Conformance

At the time of the study, the final version of Standard 81001-5-1 had not gone through the approval process, therefore a draft version was used. The aspects of the standard mentioned here may not be valid in the final version. The standard was used to get an understanding on how the new standard will affect the development of the medical device. Only the aspects affecting the transfer protocols and cybersecurity critical components are investigated here as areas such as coding or some parts of quality management process are not in the scope of the present study.

The main aspect that the standard IEC 81001-5-1 defines is that the processes that have been previously used to provide security and safety in medical devices other functions, must now also be done on cybersecurity related issues.

At the moment the current device cannot claim full conformance with the standard but notes of the needed changes can be taken into advisement in the future development of the device and in establishing new processes.

The following sections describe the main rule definitions that are the most relevant to the subject, information about how the rules could be conformed and new methods implemented to the networking model.

It should be noted that the cybersecurity tasks defined in the standard do not take in consideration the MDR defined medical device class, meaning that the cybersecurity should be evaluated separate from other aspects of the medical device and the main focus should be on the implementation environment and cybersecurity vulnerability of the device.

4.2.1 Processes

The standard states that the manufacturer shall identify and characterize physical and logical interfaces of the product. The characteristics of the implementation environment could affect the cybersecurity measures and tasks that must be implemented during development and the lifetime of the product. These characteristics include aspects such as; how the system can be accessed, who has access to the product, security capabilities and mechanism used to protect the product and if the product uses third-party software. [2, chapter 5.4.3] The evaluated medical device is implemented only to locations that have restricted access and only authorised personnel can access by going to the system physically. The limited access to the system may affect the cybersecurity needs of the system.

The systems do not include an external interface outside the local network, but an external VPN connection might be implemented in the future. If the external connection is implemented, it might affect the cybersecurity evaluation of the system.

The manufacturer shall define an activity where cybersecurity design is reviewed. Reviewing shall include identifying weaknesses, security requirements that were not adequately addressed by the design and possible cybersecurity threats that could be faced. All of the software services that are used in the system shall be included in this review. [2, chapter 5.4.4]

During development the manufacturer shall establish a testing process that focuses on identifying potential security vulnerabilities in the product. [2, chapter 5.7.3] A separate testing process specifically for cybersecurity testing has not been defined.

The manufacturer shall establish an activity to provide mechanism to identify that an important file received by the product user from the manufacturer is valid and has not been altered. This file could be for example a security update for developers own software or a third-party software. The manufacturer conforms

to this by delivering all the files that the user will receive in person to the system during a service visit. The other files the system receives are files from PACS and the PACS should be considered a trusted source. If in the future this process is changed an activity to the mentioned process should be established.
[2, chapter 5.8.3]

“The manufacturer shall establish - as a part of the update activity - a policy that specifies the timeframes for delivering and qualifying security updates to product users.” At minimum, this policy shall consider the potential impact of the vulnerability, public knowledge of the vulnerability, whether published exploits exists for the vulnerability, volume of the effected products and availability of and effective external control when update is not being provided. Meaning that when a possible vulnerability is detected on a product the manufacturer has to have a policy that specifies how the manufacturer responds to the vulnerability. [2, chapter 6.1.1] This process has not yet been defined by the manufacturer.

As to the modification analysis, “The manufacturer shall establish an activity(s) to actively collect and review relevant sources of information about vulnerabilities regarding supported software”, meaning that all of the software used in the system should be monitored. The software includes possible third-party virus protection software, windows operation system and software that are integrated in the products software, for example SQL.[2, chapter 6.2]

The manufacturer shall establish an activity that estimates and evaluates the vulnerabilities and security risks of the product. These risks can be evaluated with many different tasks, for example the manufacturer may use the likelihood/severity scheme that is used by the manufacturer for other risks.
[2, chapter 7.3] The standard defines that the aspects related to cybersecurity should also be included in the products risk management process. [2, chapter 7]

If the evaluation of the risks reveals a risk that is not on an acceptable level and needs mitigation measures, the manufacturer must select a mitigation and implement it. Basically, meaning that the cybersecurity risks need to be evaluated and processed the same way other risks are evaluated in the medical device development and lifetime. [2, chapter 7.4]

As to monitoring the effectiveness of risk controls, the manufacturer should implement method/process to collect and review effectiveness of the risk controls implemented to the product. [2, chapter 7.5]

The manufacturer shall establish and document the minimum requirements of the environment the product can be installed. The requirements could define location in the network, physical or cyber security provided by the environment, isolation in the network, potential safety risks if the security is degraded and what security controls are implemented in the hardware that the health software is used. The products environment requirements could be defined for example that the physical access to the location need to be restricted or the network where the product is installed needs to be isolated from the open internet with a physical firewall. The DMS could need additional implementation requirements from the implementation environment as the DMS can be installed to hardware that is not produced by medical device manufacturer. Additional requirement to the hardware where the DMS is implemented could be a software firewall or some virus protection software installed. This security context document could be shared with the products user to ensure that the implementation environment has the needed security requirements. [2, chapter 7.1.1]

Ad to reviewing vulnerabilities, “the manufacturer shall establish an activity(s) that enables the investigation of vulnerabilities in a timely manner to determine their: applicability to the product, verifiability and related threats.” This activity could be implemented to existing processes for example in the customer complaint process. [2, chapter 9.3]

The standard defines that the manufacturer must establish an activity where detected vulnerabilities are analysed. [2, chapter 9.4] Also, another process has to be defined for determining how the vulnerability will be addressed after the analyse. [2, chapter 9.5] These activities can be completed with previously used systems/processes or new processed could be defined.

Related to security expertise, all of the personnel that participate in the development, upkeeping and implementation of the system related to security should have adequate expertise of the field. [2, chapter 10.1]

In a case where the manufacturer receives software that is specifically developed for the manufacturer from a third-party supplier(s) and the software can impact security of the system, the manufacturer shall ensure that the third-party supplier(s) perform applicable security life cycle activities for each software item. [2, chapter 10.2]

4.2.2 Components

The standard defines that the manufacturer shall establish a procedure and technical controls to protect any private encryption keys implemented in the system. If any connection keys e.g. TLS encryption keys or code signing keys are implemented in the system. The manufacturer must define a way to make them not accessible and the cybersecurity of the mentioned aspect needs to be considered in the risk management process. [2, chapter 5.8.4]

Secure decommissioning has to be taken into consideration. When the system is taken of use the manufacturer should have a defined method of decommissioning. Secure decommissioning is important especially with components that store sensitive data and the medical devices software. [2, chapter 5.8.7]

The Standard defines that all of the point of entry, for example USB ports need to be evaluated. The accessing point that can be evaluated are the USB ports, ports in the firewall and the DVD driver on the workstation. Also, the physical location and security of the location needs to be considered when evaluating the cybersecurity of the medical device. [2, chapter 7.2]

The physical firewall that districts the connections to the workstation does not contain any open ports for outside connection, therefore the workstation should be safe from the attacks from the network, but the firewall could contain some deficiencies that could be exploited to access the system. If this kind of deficiency is noticed and fixed the firewall should be updated accordingly.

The most critical physical accessing point are the USB port and DVD driver in the workstation front panel. The other accessing points in the workstation are situated behind the fixed back cover of the workstation.

The cybersecurity of the mentioned ports needs to be evaluated. The accessing point should be protected against an attack as the windows configuration blocks any connections before the PC has been accessed by an account. Also, the machine cannot be booted with a removable media, meaning that the attacker cannot access the PC by opening it with an external driver. In conclusion the system does not contain any explicit cybersecurity deficiencies, but the system should still be tested comprehensively and possibly vulnerabilities should be mitigated. The system might include some vulnerabilities that are related to undiscovered deviancies in the health software and third-party software.

Previously the standards did not specify strict measures on that the ports cybersecurity should be tested and verified to be secure. The new standard does not define any process on how accessing points should be protected. Previously, often the security of the system could be stated on the basis of the location of the device being in a secure hospital environment that makes an attack very unlikely. Safety of the network is commonly based on that connection to devices in the network were districted with a firewall or that the network was not connected to other networks.

The DVD reader installed to the workstation is a safety risk, but the severity of the risk is hard to evaluate. New standards do not mention security aspects of this kind of component. It is not likely that an attacker would use this accessing point to access the medical device as it would need to be done on site in a hospital/clinic. The system does not read the data inserted to the system form any components before a user has signed into the system, also booting a software form the DVD reader is disabled. The system uses Windows security profile that provides safety by limiting the ways the windows can be used and accessed, a windows security profile is a defined windows configuration where the use of the systems components and features are limited.

In the new standard the methods that the hospital or clinic uses to provide safety and cybersecurity are going to be defined in the following parts of the standard, as stated in the standard, “The IEC/ISO 81001-5 series of standards (for which this is part 1, is therefore being designed to include future parts addressing security that apply to the implementation, operations and use phases of the life cycle for organizations such as HDOs.” [2, chapter 1.2]

The standard also defines aspects of how the software should be designed, produced, tested during production and how these processes should be documented. “Development environment security the manufacturer shall establish risk-based procedural and technical controls for protecting the IT infrastructure used for development, production delivery and maintenance from unauthorized access, corruption and deletion. This includes protecting the health software during design, implementation, updates, testing and release”. [2, chapter 5.1.2]

A protocol or method to provide a way to update the product to provide adequate security. In this case the update could be an update to the software running the product or an update to a possible cybersecurity protection software running on the products operation system. The updating could be hard as the system should not be connected openly to the internet and getting access to a hospitals network could be hard or in some cases impossible as the hospital does not allow it. If these kinds of connections would be made it should be done with a VPN protocol as the IP addresses need to encrypted to protect the hospitals network from unwanted connection attempts. [2, chapter 6.3] At the moment the manufacturer’s method for providing the updating would probably be that the update should be done on site by a trained and qualified personnel. If the updates could only be done on site by trained personnel the updates could only be done infrequently and the security level provided by the software would decrease, as the new security updates that cannot be installed to the system could include fixes for known cybersecurity vulnerabilities.

4.3 DICOM Conformance

The model has a complete DICOM connection between the data management server and the hospitals PACS server. The DICOM connection that is created by the PACS broker to the PACS server has a DICOM conformance statement that defines how the connection is created and acts as a statement that the connections comply with the DICOM standards. The DICOM connection does not declare conformance to any of the DICOM security profiles. [11, part 3.2]

4.4 Further Related Standard and Regulative Conformances

The implementation of the GDPR in the environment that uses DICOM data is complex as the patient data and identification information is stored in the same package. Providing adequate data storage safety requires extra safety means. This aspect is likely to be considered in the security requirements of the medical devices.

The networking model and related components were not evaluated against any other standards or regulations. Therefore, this thesis cannot fully provide a full picture of how the model conforms with all the related regulations.

4.5 Cybersecurity Vulnerabilities

In this section the known cybersecurity vulnerabilities of the product under evaluation are listed and discussed. The vulnerabilities are included in the evaluation and they may affect the configuration of the final networking model.

Some VPN protocols need modification to the networking components in order to be applicable, for example L2TP VPN protocols need to have an open port to access through, meaning that a port has to be opened on a firewall or a router, this open port could be used as an access point on an attack. The main issue on VPN use in medical devices is that the connection point of the VPN needs to be able to detect the incoming data transfer, as the source IP is encrypted the program that is the first one to receive the data needs to be able to access the data through the encryption or to be able to decrypt it. This can be realised by using a firewall that has capabilities to receive data with the used VPN protocol. If the firewall is not capable of accessing the data and the data can be decrypted only in a specific program that is situated inside the protective layer of the medical device the only solution to receive the data is to open a specific port in the firewall. Opening the firewall to the VPN connection opens the port to all the users who want to access the firewall thought that specific port. Opening a port in a firewall is a significant security risk and opening a port that is needed for a specific VPN protocol is even higher of a security risk as the VPN protocol ports are well known, therefore the port can potentially be targeted by attacker. [13;14]

Implementation means and methods of different protocols can vary. Usually making the connection possible for a VPN connection, the routers need to be opened in the specific ports that the protocol uses. This could make the implementation of the connection harder or in some cases impossible because if the hospital cybersecurity protocols do not allow it, as opening the ports could create vulnerability in the network.

The process of modifying or adding devices into the hospital network is usually a complex process, for example opening ports or classifying IP addresses to network components will probably need evaluation and permissions.

Using VPN to make the data transfer more secure is a good solution in some cases, for example in case the transfer is through an open network where transfer information for example source and destination IPs can possibly be observed.

The official DICOM website specifies that the use of VPNs in DICOM connections is not recommended. Because of the previously mentioned security risks and recommendations from trusted sources the use of VPN protocols in hospital networks is probably not allowed/recommended. [3]

The workstation cybersecurity risks are mostly related to physical access to the system, as the workstations firewall does not let any connections through form the outside. The workstation could be compromised by a remote attack only if the server was compromised and the workstation connected to it. The main physical vulnerability of the workstation is the open and unused USB ports.

The workstation and DMS do not include any software for scanning of the incoming data. Meaning that the data that is allowed to pass through the cybersecurity protections of the systems is not scanned for potentially harmful data/programs.

The server is the most vulnerable aspect of the network and in the future the regulation probably affects the server the most, as the server is discoverable in the network. Security methods are needed. The server is the most vulnerable to attacks as the server needs to be configurated with open TCP ports for outside connections, to make access from workstation and PACS possible. This also makes the server discoverable in the networking. To minimize the risks the server networking configuration needs to be configured to limit the connection that it accepts for example to accept connection only from a specific IP address. The DMS is always open therefore and possibly discoverable by other devices in the network.

The safety of the hospital networks also differs significantly. Some networks are completely closed from other networks, but some networks can be connected to the internet through a firewall.

Regular security upgrades are a big part of cybersecurity. Providing an update to any of the software cannot be done easily and very often, as the update can only be done by a verified service personnel and the software version has to be tested and verified as safe to use. Virus protections software on the data management server could be updated more frequently according to the hospital's needs as the hospital can be given full control of the DMS PC.

The implementation of a virus protection software to the server is not defined in the networking model, but it should be implemented to all the DMS PCs that are connected to the hospital's network. The hospital can install and configure the protection software by themselves. [10]
Ultimately the hospital's Chief Information Officer is responsible of the integration of the medical systems to the network. [3]

4.6 Feasibility to Integrate into Intended Network Environment

At the moment the hospitals and clinics demand different levels of cybersecurity protection. Some are not very strict on what cybersecurity methods are used but others want the manufacturer to provide frequent security updates. In the future the differences between sites are likely to diminish as the regulations will become stricter and more comprehensive.

Considering the network model cybersecurity, the definition of the used encryption protocol in the connection between the devices has a big effect on the cybersecurity of the system. Table 1 lists and compares the possible protocols that could be used to protect the connections in the network.

Table 1: Comparison of the encryption protocols

Protocol	Encryption	Ease of install	Security level	Conformance with regulation
Connection without an encryption protocol	None	Very easy	Low	Adequate security level cannot be reached if the transferred data is not encrypted.

VPN	Data and addresses of the devices encrypted. Encryption strength varies between VPN protocols.	Very hard to install to a network. Modifications to network needed. If not correctly installed security vulnerabilities may be created.	High	Provides adequate security if implemented right. DICOM standard does not recommend.
TLS	Provides strong encryption to the data. Widely used.	Easy. Usually, modifications to the network are not needed.	High	Provides adequate security level. Use of TLS protocol is recommended in the DICOM standard.

Table 1 above defines how the different protocols could fit in the intended environment. A data transfer protocol that has no encryption protocol could be very easy to install but cannot be implemented to the product. It would create a large vulnerability to the system as the connection would have no security against attacker trying to capture patient data moving through the network. When implementing the product with this kind of data transfer protocol the hospitals/clinics security admin would not allow the implementation to the network.

The VPN protocols have good and bad attributes. The security level provided by most VPN protocols could be high if implemented properly, the level of security is hard to define as the configuration of VPN protocols could be very complex, these possible implementation difficulties make the VPN protocols not the ideal protocols to be used.

The TLS protocol provides good results in all of the evaluation aspects. It provides high levels of security, is easily implemented to the network if the encryption protocol is integrated in the product software in production and the protocol is proven to work in the environment as it is used in a DICOM secure use profile.

Based on the provided security, ease of installation and modifiability the best encryption method is an encryption protocol based on shared encryption keys. TLS encryption is based on this method.

The product can be implemented to the intended environment if the intended encryption method is changed from VPN to some widely used sophisticated encryption protocol such as TLS. Tentative evaluation of the network solution concludes that an adequate level of cybersecurity is reached but more detailed vulnerability tests are needed. In some aspects, the product provides more security methods than is defined in the standard, for example the firewall implemented in the workstation is not strictly necessary in point of the standards. Standard 810001-5-1 section 7.1.1 notes, “If the product is expected to be protected by a user-supplied firewall that connects it to the Health-IT-network, the product would typically not require a firewall of its own.” [2]

In the future some additional tasks are needed to be defined in the development, production and lifetime support of the medical device. Most important processes to be defined are the risk and vulnerability testing of the networking components and related software.

The system has been designed to have an adequate cybersecurity. The cybersecurity could be designed to be safer, but a balance must be found between safety, costs and practicality/usability. If more safety methods were to be implemented the system could not probably be implemented on all sites and the users would not like if the use of the system became more complicated. Complicated systems could also create vulnerabilities if the user or installer does not have adequate understanding of the process.

DICOM connection can be implemented in the networks as it has a DICOM conformance statement, meaning that the manufacturer’s software can be connected to basic PACS servers as they use the same communication protocols. The connection does not use any security protocols that the DICOM standards define but this should not affect the feasibility to implement if the hospital does not implement policy to require the use of one or more of the protocols.

In many cases the product vendor does not use any of the security methods provided by DICOM standards and the main aspect of the security has been the secured environment and isolation of the network. The use of DICOM secure use profiles could become more widely used, but at the moment there is no specific reason to use the mentioned methods for additional security. [3, 10]

USB port security could be improved by closing unused USB ports and configurating them to only allow certain types of devices, for example to allow only a USB flash drive, or if wanted the configuration could be more specific and define also the model and maker of the device that will be accepted.

Some customers might want the DMS to be installed to a different network. This could affect the safety of the system, but the HDO carries the responsibility of the connection points between the networks. In such situations, the connection addresses should be encrypted.

The final implementation feasibility cannot be defined as there is no definitive answer. Testing installation is needed, but even after providing proof of concept in a single site, the compatibility to other sites cannot be proven. Slight modifications will always be necessary, and the systems should be designed to be as adjustable as possible.

5 Conclusion

The following chapters go through the final conclusions of the evaluation and suggested implementation changes, as well as the actions that have been done based on the evaluation of this study. The conclusions of this study are based on very confined material and not all of the related legislation were included in the scope of this study.

5.1 Final annotation

If the suggested encryption protocol change is done to the networking model this concise study concludes that the model has adequate safety methods and the product can be implemented to the environment, but every time the product is installed the implementation environment needs to be evaluated and confirmed to have adequate safety procedures. There should be a document that clearly defines the minimum requirements of the network, these aspects are defined by the manufacturer and the requirement should be defined carefully to make the system as safe as possible.

In the future, changes and addition safety methods may need to be implicated when new parts of relevant standards are published. The changes may include implementing some DICOM security profiles to the connection between the DMS and PACS. The biggest change in the future could be that the hospital could force the manufacturer to provide frequent software updates to the systems software. To comply with this, major changes in the product would need to be made as at the moment there is no method to provide frequent updates without an on-site visit. Providing the updates with frequent on-site visits is not feasible.

At the moment there is no defined process for any regular security update service. This process should define for example how often the updates are done. The security update process must be established.

Best method to provide cybersecurity on the connection between the system in the network would be encrypting the data with an encryption protocol.

The product network solution should be made relatively modifiable, meaning that the encryption protocol should be changeable, and the product should not use any methods dependant on any individual component to provide flexibility to change with the regulation and at the same time avoid safety risk or production difficulties caused by a third-party component/software change.

Risk management processes regarding security/cybersecurity need to be implemented and a process to observe and keep up with new possible weaknesses found in the software used in the product including third party software.

5.2 Actions Taken

Based on the evaluation a decision to dismiss the use of VPN protocols in the encryption was made. The development moved in the direction of using encryption protocols such as TLS. An inquiry about a possible method was made to a consulting company and the proposed method was accepted and the development begun. The consulting company has experience in the field and therefore the encryption should be adequate, as the implementation has been proven with previous clients. However, the field is constantly changing, and the security provided by this method could not be enough or some other method could be preferred in the future when stricter guidelines and regulations come in to affect. Still there are a lot of aspects to be investigated, for example how often a security update should be released and how long the encryption key lifetime should be.

The medical device manufacturer will be taking into consideration the applying of the processes that the new standard defines the manufacturer should apply to claim conformance to the standard IEC/ISO 81001-5-1.

Sources

1. The European Parliament and of the council, “Regulation (EU) 2017/745 of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC”,[Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017R0745. [Accessed 20th July 2021].

2. International Organization for standardization. “IEC 81001-5-1:2021 Health software and health IT systems safety, effectiveness and security — Part 5-1: Security — Activities in the product life cycle”. ISO. [Accessed 20th July 2021]

3. The Medical Imaging Technology Association. “Digital Imaging and Communication in Medicine – Security”. [Online]. Available: https://www.dicomstandard.org/using/security. [Accessed 20th July 2021]

4. The European Parliament and of the council. “Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)”. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj#d1e2051-1-1. [Accessed 1st September 2021]

5. The European Union Medical Device Regulation. [Online]. Available: https://eumdr.com/. [Accessed 1st September 2021].

6. European Commission. “M/575 Commission Implementing Decision of 14.4.2021 on a standardisation request to the European Committee for Standardization and the European Committee for Electrotechnical Standardization as regards medical devices in support of Regulation (EU)

2017/745 of the European Parliament and of the Council and in vitro diagnostic medical devices in support of Regulation (EU) 2017/746 of the European Parliament and of the Council". [Online]. Available: https://ec.europa.eu/growth/tools-databases/mandates/index.cfm?fuseaction=search.detail&id=599#. [Accessed 20th October 2021]

7. MD101 Consulting. "Cybersecurity standards: IEC 81001-5-1 and IEC/TR 60601-4-5". [Online]. Available: https://blog.cm-dm.com/post/2021/07/09/Cybersecurity-standards%3A-IEC-81001-5-1-and-IEC/TR-60601-4-5. [Accessed 20th October 2021]

8. PhoenixNap Global it services. "8 Types of firewalls: Geide for IT securirty Pros". [Online]. Available: https://phoenixnap.com/blog/types-of-firewalls. [Accessed 20th October 2021]

9. Wikipedia. "Transmission Control Protocol". [Online] Available: https://en.wikipedia.org/wiki/Transmission_Control_Protocol [Accessed 20th October 2021]

10. Marco Eichelberg, Klaus Kleber, Marc Kämmerer MD. 2020. "Cybersecurity Protection for PACS and Medical Imaging: Deployment Considerations and Practical Problems" [Online] Available: https://www.sciencedirect.com/science/article/pii/S1076633220305213 [Accessed 20th October 2021]

11. International Organization for standardization. "ISO 12052:2017 Health informatics — Digital imaging and communication in medicine (DICOM) including workflow and data management". ISO. [Accessed 20th October 2021]

12. Interner Society. "TLS Basics". [Online]. Available: https://www.internetsociety.org/deploy360/tls/basics/ [Accessed 20th October 2021]

13. Richard Bagdones, MI7. “Why are hospitals still using VPNs” [Online] Available: https://www.mi7.io/blog/why-are-hospitals-still-using-vpns [Accessed 20th October 2021]

14. Healthcurity. “Why you might think twice about VPNs on your network”. [Online]. Available: https://www.healthcurity.com/why-you-might-think-twice-about-vpns-on-your-network/. [Accessed 20th October 2021]

15. Megan Charles, SearchHealthIT. “PACS (picture archiving and communication system)” [Online] Available: https://searchhealthit.techtarget.com/definition/picture-archiving-and-communication-system-PACS. [Accessed 20th October 2021]

16. Cisco. “What is a VPN? – Virtual Private Network”. [Online]. Available: https://www.cisco.com/c/en/us/products/security/vpn-endpoint-security-clients/what-is-vpn.html [Accessed 20th October 2021]

17. Nielsen Norman Group. “Formative vs. Summative Evaluation”. [Online]. Available: https://www.nngroup.com/articles/formative-vs-summative-evaluations/ [Accessed 13th February 2022]