Cyber security in healthcare systems

Prof Martti Lehto, Prof Pekka Neittaanmäki, Dr. Jouni Pöyhönen, Dr. Aarne Hummelholm.
University of Jyväskylä, Finland
martti.lehto@jyu.fi
pekka.neittaanmaki@jyu.fi
jouni.poyhonen@jyu.fi
aarne.hummelholm@jyu.fi

Abstract

Healthcare is a good example of a structure whose complexity has been shaped by the general rapid development of technology and digitalization. The digital development has made it possible to provide services in new ways and more widely than before, in particular with information networks. The healthcare information environment currently consists of a networked entity consisting of various ICT systems, medical devices, and clinical systems, which consists of an open system structure. Digitalized functions and services are becoming more common in social welfare and healthcare. Their operational reliability must be ensured during incidents and emergencies.

Although the digital world offers good opportunities to improve healthcare systems and make disease analyses more effective, we must look deeper into the issue. Devices and information systems may not work well together, and we have vulnerabilities in people, processes and technology. So, a comprehensive approach to healthcare cyber security is needed.

Key words: Healthcare, cyber security, hospital, information systems

Introduction

Securing the functioning of healthcare information systems is part of ensuring the critical infrastructure and security of supply in society, where preparedness plays a key role. Preparedness means ensuring that all activities and tasks can continue with minimum interruptions and that the required exceptional measures can be performed during disruptions occurring in normal conditions and during emergencies. Vital functions are essential for the functioning of society and they must be maintained in all situations.

The starting point should be that the required client and patient medical information must be available in all situations. Data transmission of diagnostic and other client and patient medical data, digital services and the cyber security of networked social welfare and healthcare equipment must be ensured against cyber-attacks. As more and more social welfare and health services are provided as home care, the threats to the sector are also spreading outside hospitals and healthcare centres, which must be considered in the contingency and preparedness plans of the healthcare service providers against hybrid operations and different types of cyber threats. (Security committee. 2017)

In the past two decades, information technology has been widely utilized in healthcare. Electronic health records (EHRs), biomedical database, and public health have been enhanced not only on the availability and traceability but also on the liquidity of data. As healthcare-related data is constantly growing, there are challenges for data management, storage, and processing, as follows.

1. Large Scale: With the improvement of medical informationization, particularly the development of hospital information systems, the volume of medical data has been increasing. Also, wearable health devices have accelerated the explosion of healthcare data.
2. Rapid Generation: Most medical devices, particularly wearable devices, continuously collects data. The rapidly generated data needs to be processed promptly for responding to an emergency immediately.
3. Various Structure: Clinical examination, treatment, monitoring, and other healthcare devices generate complex and heterogeneous data (e.g., text, image, audio, or video) that are either structured, semi-structured, or non-structured.
4. Deep Value: The value hidden in an isolated source is limited. However, through data fusion of EHR and electronic medical records (EMRs), we can maximize the deep value from healthcare data, such as personalized health guidance and public health warning.

(Zhang et.al, 2017)

Digital transformation gives has had a positive impact in healthcare. In this digital transformation such areas like telemedicine, artificial intelligence (AI) enabled medical devices, big data analysis, treating patients with virtual reality, wearable medical devices, and blockchain electronic health records are concrete examples of digital transformation in healthcare which are completely reshaping how we interact with health professionals, how data is shared among providers and how decisions are made about treatment plans and health outcomes. (Reddy, 2021)

A modern hospital has hundreds – even thousands – of workers using laptops, computers, smartphones, and other smart devices that are vulnerable to security breaches, data thefts and ransomware attacks. Hospitals keep medical records, which are among the most sensitive data about people. Many hospital`s electronics help keep patients alive, monitoring vital signs, administering medications, and even breathing and pumping blood for those in the most critical conditions. (Hummelholm, 2019, 648.)

The reason for the interest of criminals is that patient data is well paid for in the black market; typical patient information includes credit card numbers, email addresses, health insurance numbers, employer information, and medical history information. These have value to criminals because they usually last for years. Cybercriminals use information for phishing attacks, fraud, and identity theft. (Lehto, et.al, 2017, 18.)

In the healthcare sector, there are very specific requirements for data processing. The integrity and availability of patient data are extremely important for the safe care of patients. On the other hand, the confidentiality of data must be protected not only to ensure the protection of privacy, but also to prevent the criminal use of personal data. The functionality of the entire hospital environment is critical to patient care. In this case, the digital system and equipment environment of the hospital that connects to the Internet must be considered. An example of the wide scope is the important role of cyber security in building automation in hospital buildings. (Halonen, 2016, 19–23.)

2 Hospital as a cyber space

The healthcare sector is a large and diverse sector that provides a vast array of goods and services that are essential to the health, safety, and well-being of the nation. Critical functions of the sector include, but are not limited to:

- Primary healthcare and specialized medical care hospitals and ambulatory healthcare including the doctors, nurses, occupational health practitioners,
- Health center and Emergency medicine facilities,
- Health plans organizations, Business Associate, and Healthcare Insurance companies,
- Mortuary care,
- Enterprises that manufacture, distribute, and sell, drugs, biologics, and medical devices,
- Biobanks and Genome Centers
- Population-based care and surveillance provided by health agencies at the national, area, and local levels.

Digital healthcare tools have the vast potential to improve ability to accurately diagnose and treat disease and to enhance the delivery of healthcare for the individual. Digital tools are giving providers a more holistic view of patient health through access to data and giving patients more control over their health. Digital healthcare offers real opportunities to improve medical outcomes and enhance efficiency.

Different reports show that ransomware, data breaches and other cyber-attacks are on the rise, and healthcare is one of the biggest targets. The healthcare industry increasingly relies on technology that is connected to the internet: from patient records and lab results to radiology equipment and hospital elevators.

2.1 Hospital and cyber world layers

Martin C. Libicki has created a structure for the cyber world, whose idea is based on the Open Systems Interconnection Reference Model (OSI). The OSI model groups communication protocols into seven layers. Each layer serves the layer above it and is served by the layer below it. The Libicki cyber world model has the following four layers: physical, syntactic, semantic, and pragmatic. This model has been modified and we use five

layers: physical, syntactic, semantic, service, and cognitive. (Libicki 2007; Lehto, 2015, 21; Sartonen et.al, 2016, 5–7.).

The cyber world layers are:

1. **The physical layer** contains the physical elements of the communications network (fixed and wireless) and medical devices.
2. **The syntactic layer** consists of various system control and management software and features that facilitate interaction between the devices connected to the network.
   The layer includes the software that provides the operating commands for the physical devices.
3. **The semantic layer** contains the information and datasets in the user's computer, hospital's servers, or cloud service environment as well as different user-administered functions.
4. **The service layer** contains all those public and commercial services available in the network.
5. **The cognitive layer** is the hospital personnel's information-awareness environment: a world in which information is being interpreted and where one's contextual understanding of information is created. It can be seen from a larger perspective as the mental layer, including the user's cognitive as well as emotional awareness.

Hospital cyberspace is more than the internet, including not only hardware, software, data, medical devices, and information systems, but also people and social interaction within these networks and the whole infrastructure.
Figure 1 illustrates the cyber world layers in hospital perspective.

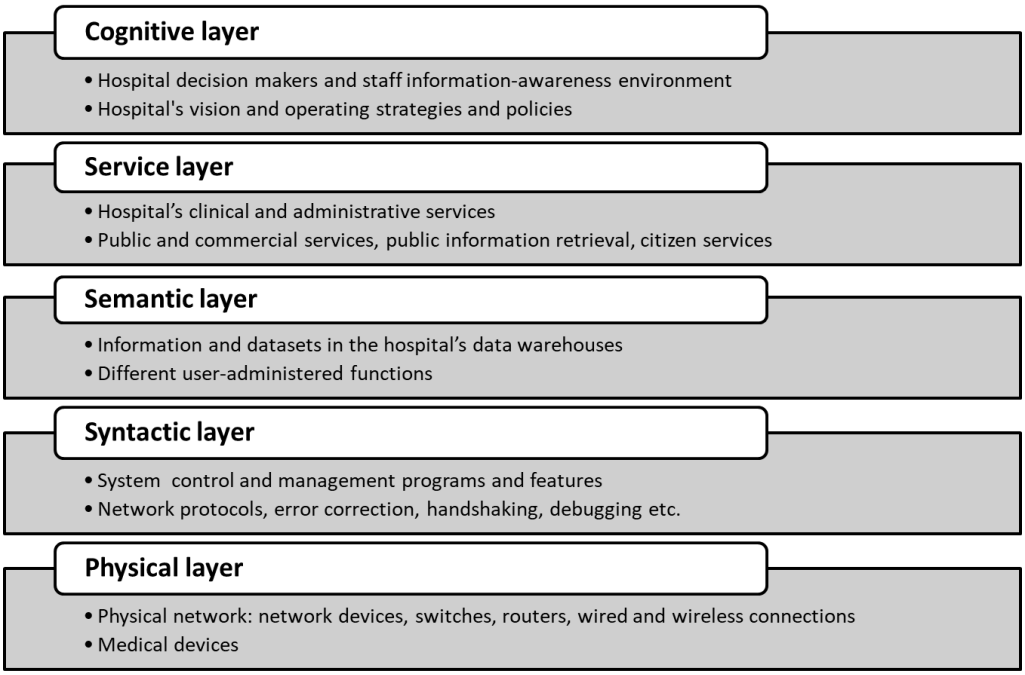


Fig. 1 Cyber world layers in hospital perspective

The International Telecommunication Union (ITU, 2018) describes, that "Cyber security is meant to describe the collection of tools, policies, guidelines, risk management approaches, actions, trainings, best practices, assurance and technologies that can be used to protect the availability, integrity and confidentiality of assets in the connected infrastructures pertaining to government, private organizations and citizens; these assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and data in the cyber-environment."

The ISO/IEC 27032 defines "Cyberspace security as the protection of privacy, integrity, and accessibility of data information in the cyberspace. Therefore, cyberspace is acknowledged as an interaction of persons, software, and worldwide technological services."

2.2 Hospital information systems

A hospital information system (HIS) is a comprehensive, integrated information system designed to manage all the aspects of a hospital's operation, such as medical, administrative, financial, and legal issues and the corresponding processing of services. The hospital environment requires the utilization of several different information system and automation system entities. They are needed at least in four different processes. The systems at a general level are:

1. Administrative information systems,
2. Hospital clinical information systems,
3. Building automation system (heating, ventilation, and air conditioning, HVAC),

4. Physical safety and security information systems.

Figure 2 illustrates generic hospital information system.

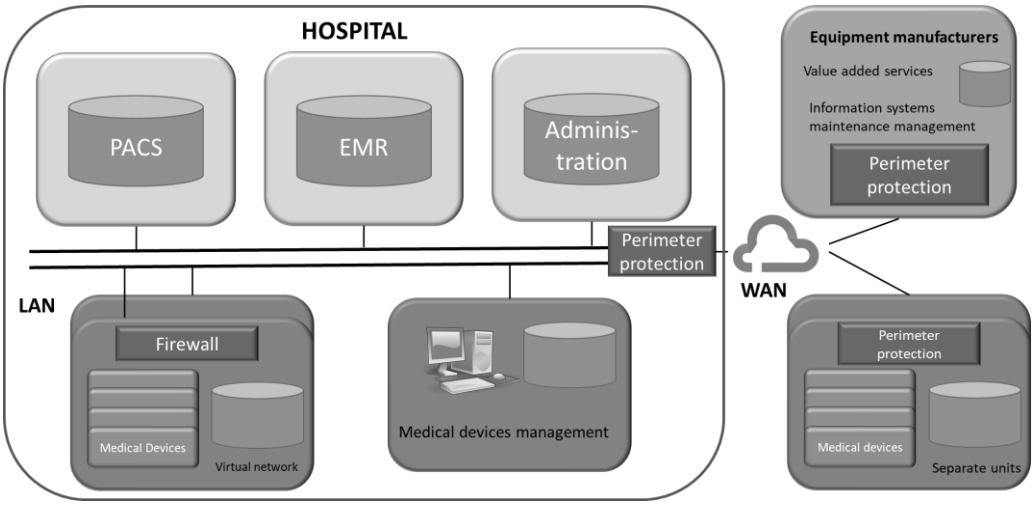


Fig. 2 Generic hospital information system. (Integrating the Healthcare Enterprise, 2015, 21)

A patient record system can be part of a hospital information system, and it is a type of clinical information system, which is dedicated to collecting, storing, manipulating, and making available clinical information important to the delivery of patient care. A patient record is the repository of information about a single patient. This information is generated by health care professionals as a direct result of interaction with a patient or with individuals who have personal knowledge of the patient (or with both).

A health information system refers to a system designed to manage healthcare data. This includes systems that collect, process, store, manage, report, and transmit a patient's electronic medical record (EMR), a hospital's operational management or a system supporting healthcare policy decisions. Health information systems also include those systems that handle data related to the activities of providers and health organizations. EMR / EHR database maintain patient's record by data like contact details, test results, treatment history, and more. It enables the sharing of information to another EMR / EHR system so that different healthcare providers can access the patient's system if compatible data models are used. (Levin, 2019; Chanchal, 2020)

The reality of hospital information systems is that they must tightly match the reality of the organization, its internal formation, care processes, medico-technical means, legal and regulatory environments, and billing procedures.

Health information systems consist of six key components, including:

1. **Resources:** the legislative, regulatory, and planning frameworks required for system functionality. This includes personnel, financing, logistics support, information, and communications technology (ICT).
2. **Indicators:** a complete set of indicators and relevant targets, including inputs, outputs, and outcomes, determinants of health, and health status indicators.
3. **Data sources:** including both population-based and institution-based data sources.
4. **Data management:** collection and storage, QA, processing and flow, and compilation and analysis.
5. **Information products:** data which has been analyzed and presented as actionable information.
6. **Dissemination and use:** the process of making data available to decision-makers and facilitating the use of that information.

(Levin, 2019)

The health information system is a complex system of systems that manages healthcare data, including many types of systems. Some of those include:

- Electronic Health Record (EHR) or Electronic Medical Record (EMR). These platforms collect, store, and share data related to a patient's health history.
- Practice Management System: This type of system manages the daily operations of a practice, such as scheduling and billing.
- Master Patient Index: This type of platform connects separate patient records across multiple databases.
- Patient Data Repository: A healthcare data system used with the patient data system. It allows centralized archiving of electronic patient data, as well as active use and storage of the data.
- Pharmacy Management System: This software includes all data related to a patient's prescriptions and is found in several pharmacy settings, including retail, hospital, and long-term care.
- Patient Portals: These systems allow patients to access their health data, including medications and lab results (MyData). They can also use it to communicate with physicians and track appointments.
- Clinical Decision Support (CDS): This type of platform analyzes data from clinical and administrative systems. The analysis can then enable clinicians to make the best clinical decisions.
- Medical Certificates Sharing System: Certificates and reports issued by healthcare professionals can be forwarded electronically to those concerned.

(Kanta, 2020; InfoWerks, 2020; Chanchal, 2020)

PHI (protected health Information) is collected or created by a healthcare provider, health plan, employer, healthcare clearing house or other entity. According to the defining criteria, data contained within a patient's healthcare record is deemed to be PHI if there is a reasonable basis to believe the information could be used to identify an individual. Examples of identifiable data elements may include but are not limited to:

- Name, address (including postal code), telephone and fax numbers,
- Email addresses,

- Medical insurance or Social Security/National Insurance numbers,
- Identity number,
- Information about named beneficiaries,
- Any (financial or otherwise) account numbers, license, vehicle, or certificate numbers,
- Medical or otherwise salient device or serial numbers,
- Any associated internet protocol (IP) addresses or URL/URIs,
- All biometric data (for example finger, retinal or voice prints and/or DNA),
- Full facial photographic images or images that have unique identifying characteristics,
- X-rays and other diagnostic images,

(Verizon, 2018, 5)

Hospitals are becoming more reliant on the ability of hospital information systems to assist in the diagnosis, management and education for better and improved services and practices. Separate systems collect research and procedure data during the patient's care chain, which the most important are laboratory systems, through which the necessary tests are ordered, the test results are entered into them and the results are handed over to the requesting unit.

Hospital information systems are among others:

- Radiology Information System, RIS
- Picture Archiving Communications Systems, PACS
- Electronic Health Record, EHR
- Electronic Medical Records, EMR
- Laboratory information systems, LIS
- Clinical Information System, CIS
- Pathology information systems
- Pharmacy information system
- Intensive care systems
- Blood bank system
- Anesthesia information systems
- Control of surgery operations
- Remote Patient Monitoring (RPM)
- Imaging systems
- Maternity ward information systems
- Nursing Information Systems (Nurse call systems)
- Central control systems
- Financial Information System
- ERP systems
- Security systems

The human generates per lifetime 1100 Terabytes (TB) of healthcare data, 6 TB of genomics data and 0.4 TB of clinical data. The data is fragmented here and there and is not easy to share or analyze. (McGovern, 2014)

Figure 3 illustrates an example of the most significant data sources in the hospital.

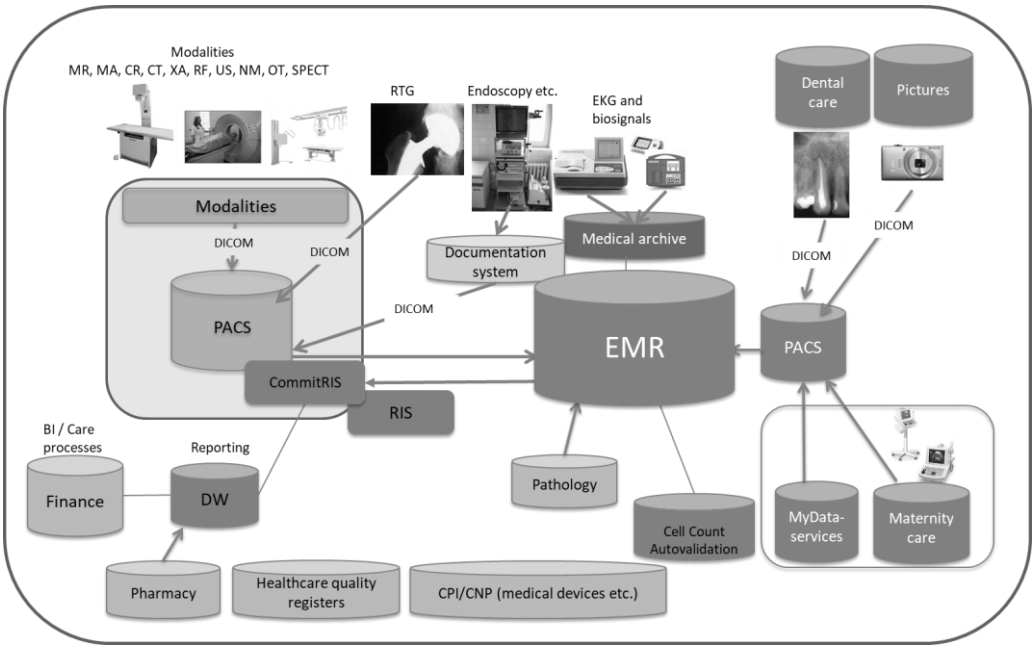


Fig. 3 Generic hospital data system

Abbreviations:

DICOM: Digital Imaging and Communications in Medicine)	PACS: Picture Archiving and Communication System)	RIS: Radiology Information System)
CPI: Clinical Physiology and Isotope Medicine)	CNP: Clinical neurophysiology)	EMR: Electronic Medical Records

2.3 Medical devices

Smart devices are connected to fixed or mobile networks and are used to transfer the patient's bio-signal data to hospital systems. In hospital systems, the information is analyzed, and the care staff take the necessary decisions based on analyzed results and gives information on management measures to the patients. (Hummelholm, 2019, 642)

Medical devices are as follows: An instrument, apparatus, appliance, implement, machine, contrivance, implant, in vitro reagent, or other similar or related article, including a component part, or accessory intended for use in the diagnosis of disease or other conditions, and/or therapeutic purposes or in the cure, mitigation, treatment, or prevention of disease:

- Radiology equipment, radiotherapy, nuclear medicine, operative room or intensive care equipment, robots for surgery, electro-medical equipment, infusion pumps, spirometry devices, medical lasers, endoscopy equipment.
- Patient implantable devices (holsters, pacemakers, insulin pumps, cochlear implants, brain stimulators, cardiac defibrillators, gastric stimulators, etc.) or wearables (external EKG or pressure holsters, glucose monitors, etc.).
- Device to be used for human beings for the purpose of:
    - diagnosis, prevention, monitoring, treatment, or alleviation of disease,
    - diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,
    - investigation, replacement, or modification of the anatomy or of a physiological process,
    - control of conception,
    - therapeutic purposes.

(ENISA, 2020, 14; Williams and Woodward, 2015; EU, 1993)

Figure 4 shows a generic model of the architecture and key components of medical devices from a cyber security perspective.

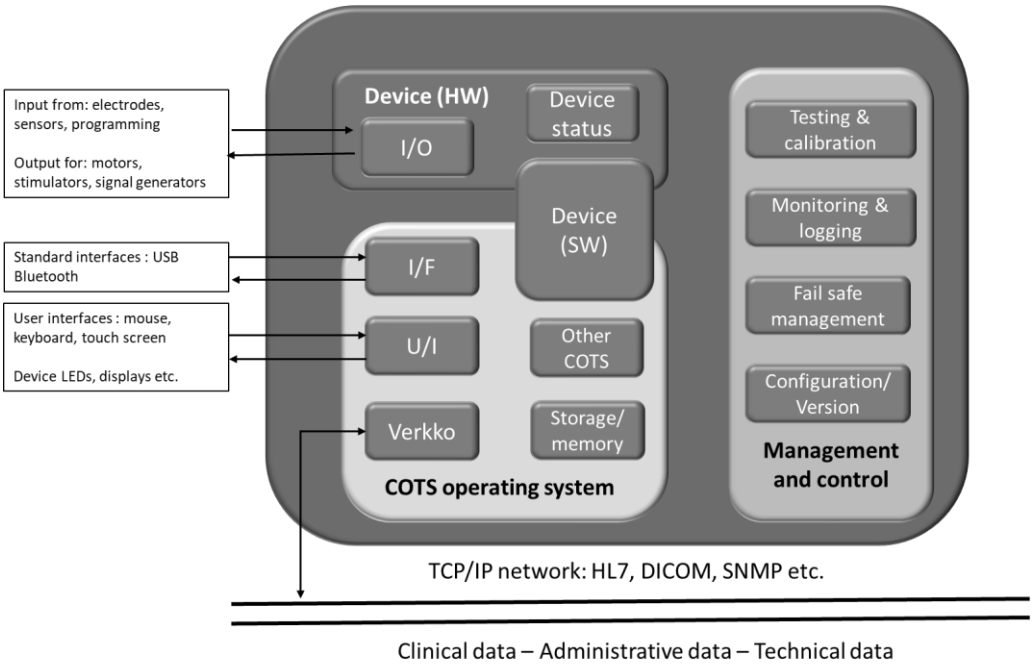


Fig. 4 Generic medical device architecture. (Integrating the Healthcare Enterprise, 2015, 16)

3 Cyber security risks related to hospital systems and equipment

The "2020 Healthcare Data Breach Report" published by HIPAA Journal notes that in the year 2020 there was a 25% year-over-year increase in healthcare data breaches. 619 major breaches were reported in 2020, affecting nearly 28.8 million individuals of those 415 were

reported as hacking incidents. Some 246 incidents were reported as involving a business associate. After hacking incidents, the next most reported type of breach involved unauthorized access/disclosure. There were about 134 such incidents. Another 28 breaches involved lost or stolen unencrypted computing devices. (HIPAA, 2021; Kolbasuk, 2021)

Table 1 illustrates top 10 breaches in 2020 by number of individuals affected in U.S. (HIPAA, 2021)

Table 1. Top 10 breaches in 2020 by number of individuals affected in U.S.

Breached Entity	Individuals Affected	Covered Entity Type	Type of Breach
*Trinity Health	3.3 Million	Business Associate	Hacking/IT Incident
MEDNAX Services	1.3 Million	Business Associate	Hacking/IT Incident
*Inova Health System	1.05 Million	Healthcare Provider	Hacking/IT Incident
Magellan Health Inc.	1.01 Million	Health Plan	Hacking/IT Incident
Dental Care Alliance	1 Million	Business Associate	Hacking/IT Incident
Luxottica of America	830 000	Business Associate	Hacking/IT Incident
*Northern Light Health	657 000	Business Associate	Hacking/IT Incident
Health Share of Oregon	654 000	Health Plan	Theft
Florida Orthopaedic Institute	640 000	Healthcare Provider	Hacking/IT Incident
Elkhart Emergency Physicians	550 000	Healthcare Provider	Improper Disposal

*Affected by ransomware attack on Blackbaud.

2020 was the third worst year in terms of the number of breached healthcare records, with 29,298,012 records reported as having been exposed or impermissibly disclosed in

2020. 266.78 million healthcare records have been breached since October 2009 across 3,705 reported data breaches of 500 or more records. Figure 5 illustrates that development.

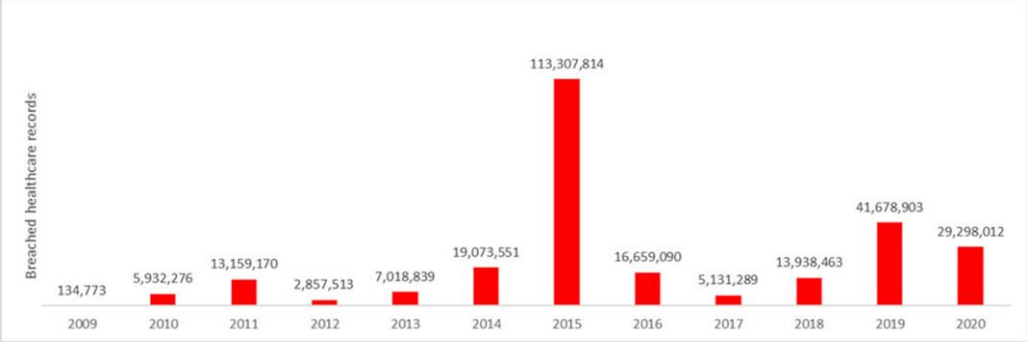


Fig. 5 Records exposed in U.S. Healthcare data breaches (HIPAA, 2021)

Threats come from a variety of different sources including adversarial, natural (including system complexity, human error, accidents, and equipment failures) and natural disasters. Adversarial groups or individuals have varying capabilities, motives, and resources. (Piggin, 2017, 6.)

Threat, vulnerability, and risk form an intertwined entirety in the cyber world. First, there is a valuable physical object, competence or some other immaterial right which needs protection and safeguarding. A threat is a harmful cyber event which may occur. The numeric value of the threat represents its degree of probability. Vulnerability is the inherent weakness in the system which increases the probability of an occurrence or exacerbates its consequences.

Vulnerabilities can be divided into those that exist in human action, processes, or technologies. Risk is the value of the expected damage. Risk equals probability times the loss. It can be assessed from the viewpoint of its economic consequences or loss of face. Risk management consists of the following factors: risk assumption, risk alleviation, risk avoidance, risk limitation, risk planning and risk transference. Countermeasures can be grouped into the three following categories: regulation, organisational solutions (management, security processes, methods and procedures and the security culture) and security technology solutions. (Lehto, 2015)

Figure 6 shows typical operational vulnerabilities in a five-layer cyber structure model.

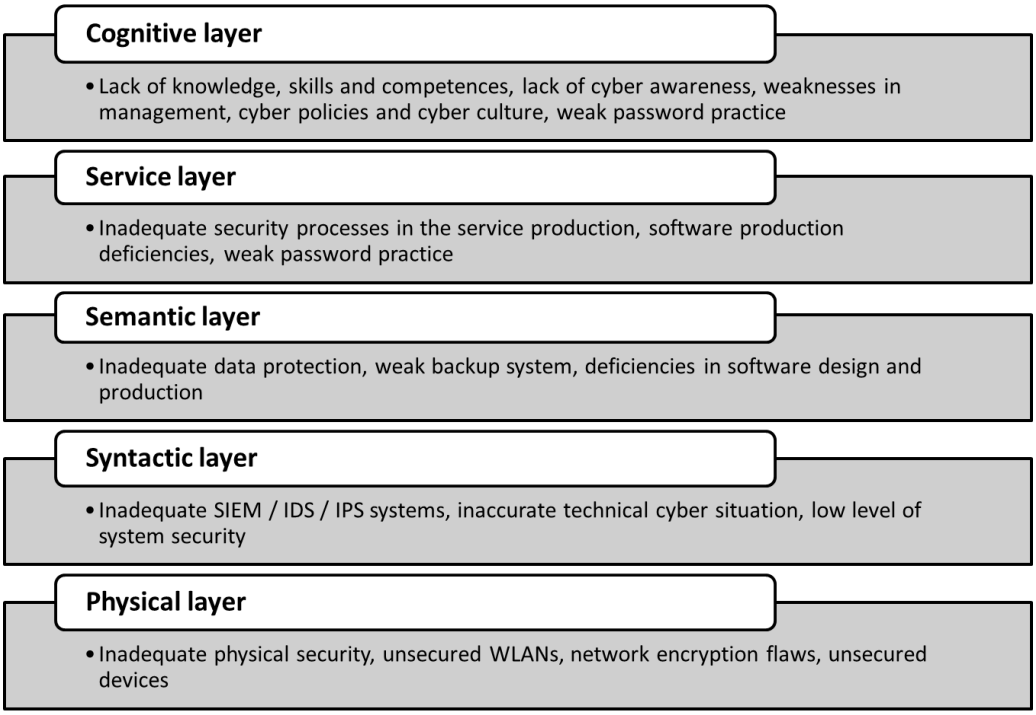


Fig. 6 Vulnerabilities in the cyber environment, (Lehto, 2014, 168.)

In general, the cyber security threats and attack vectors in health networks (wireless/fixed) include the following issues like:

- Monitoring and eavesdropping of patients' vital signs,
- Threats to information during transmission,
- Routing threats in networks,
- Location threats and activity tracking,
- Distributed Denial of service (DDoS) threats,
- Interfere with or inhibit the radio communication of IoT devices and sensors,
- Using vulnerabilities to get access to the health care services,
- Attack against the hospital health care information`s systems,
- Disrupt or impede the entire hospital's wireless communication and prevent the use of the hospital's daily activities,
- Disruption of care/service (including potential for patient deaths),
- Malware and phishing attempts: Sophisticated malware and phishing schemes that plant malicious scripts on a computer or steal login credentials.
- Deception of staff with spoof email or fake websites to obtain login credentials or install malware,
- Unintentional or intentional insider threat,
- Loss of patient information – especially electronic protected health information (ePHI)
- Data breach, information exfiltration and loss of assets
- Blackmail, extortion, and duress through exploitation of exfiltrated sensitive data
- Intellectual Property (IP) theft

(Hummelholm, 2019, 645; Piggin, 2017, 5.)

3.2 Cyber security risks related to medical devices

Increasing connectivity of medical devices to computer networks and the convergence of technologies has exposed vulnerable devices and software applications to incidents. The medical devices being potentially vulnerable and easy to exploit, so cyber-attack is possible and feasible. The purpose of such attacks can be wide-ranging from the intent to harm a specific patient; or an attack on a specific healthcare provider (e.g., cyber vandalism, crime); or an attack on the larger healthcare system (e.g., cyber terrorism, sabotage), or a military operation to support of a conventional or biological attack. These are serious. (Integrating the Healthcare Enterprise. 2015, 23.)

Cyber security risks are set to increase further with the adoption of the Internet of Things (IoT) by healthcare organizations and consumers. The security risk of medical devices is that they may potentially expose both the data associated with the device and the control of the device itself to an outsider. The convergence of networking, computing technology and software has enabled increasing integration of Hospital Enterprise Systems, Information Technology (IT), Operational Technology (OT) and Clinical Engineering (CE), and suppliers through remote connectivity. This will be revolutionized by cloud-based services and the use of big data analytics. This threat naturally raises the need for consideration between patient safety and cyber security. Therefore, the cyber threat will require increasingly close stakeholder cooperation in the future, especially regarding system/device design and regulation, stakeholder engagement regulators, device manufacturers, healthcare organizations, and IT providers. (Piggin, 2017, 3.)

Most medical devices are more vulnerable to cyber-attacks than normal IT endpoints (desktops, laptops, servers), whether it is a specifically targeted attack on the medical device or an unintentional infection of it by common malware. Also, technology convergence has since brought an abundance of commercially off-the-shelf (COTS) technology including common networking infrastructure, operating systems, software, smart mobile devices, computers, and embedded control systems to medical devices. Many medical devices contain configurable embedded computers that might be vulnerable to cybersecurity breaches. Often embedded systems may utilize older, vulnerable operating systems that may be unpatched or even no longer supported. The common vulnerabilities of the medical devices are among others:

- Network-connected/configured medical devices infected or disabled by malware,
- The malware access to the hospital IT/OT/ E system using wireless technology to access patient data,
- Uncontrolled distribution of passwords, disabled passwords, hard-coded passwords, or default passwords,
- Failure to provide timely security software updates and patches to medical devices and networks,
- Vulnerabilities in older medical device models (legacy devices),
- Poor design practices,

- Misconfigured or open ports,
- Lack of encryption & authentication,
- Poor vulnerability management,
- Insecure remote access,
- Poor manufacturing cyber-hygiene.

(Piggin, 2017, 13–14.)

Several factors complicate the protection of medical devices and contribute to a continued state of insecurity. These are a result of technical, management and human causes:

- Providing hackers with vital information from the device's performance and technical design,
- Legacy operating systems and software and incompatibility between systems leaves vulnerabilities,
- Lack of timely software updates and patches,
- Medical devices do not have basic security features,
- Web services are a popular solution for Interfacing to existing systems,
- Compromised medical devices can be used to attack other sections of the health care organization network,
- Lack of awareness of the cybersecurity issues, and poor security practices,
- The balance between cyber security, privacy and effective healthcare processes can create vulnerabilities in the device environment.

(Williams and Woodward, 2015)

The security risks associated with hospital equipment are also reflected at the system level. From a cybersecurity point of view, the hospital is comprised of a set of critical systems that contain both operational risks and various vulnerabilities, through device vulnerabilities, and are thus exposed to cyber threats.

The predicted rapid growth of connected devices in healthcare applications, the increasing concern over breaches of patient data and more recently the potential risks to patient safety requires security to be a critical feature in medical products and software. An advanced malware-infected device has the potential, in the worst case, to shut down hospital operations, expose sensitive patient information, compromise the operation of other devices, and harm patients. (Piggin, 2017, 5, 18–19.)

3.3 Cyber-attack vectors against hospital

There are a wide range of Internet threats and attacks from virus propagation and worms, such as; distributed denial of service (DDoS) attacks and data theft and manipulation and also hospital systems paralysis.

An attack vector is a path or means by which an attacker can gain unauthorized access to a computer, network, or information infrastructure to deliver a payload or malicious outcome. Attack vectors allow attackers to exploit system vulnerabilities, install different types of malware and launch cyber-attacks. Once the attacker has based his/her motivation

and objective they choose one or more means to achieve the goal = attack vector. (CERT-UK, 2015; Kovanen et.al, 2018)

There are many different types of actors who commit cyber-attacks. A disgruntled former employee may be aware of vulnerable attack vectors due to their role in the hospital. An individual hacker may be trying to steal personalized information. A hacktivist might initiate a cyber-attack against a hospital to make an ideological statement. Business competitors may try to attack clinical infrastructure to gain a competitive edge. Cyber-criminal groups combine their expertise and resources to penetrate hospital security systems and steal large volumes of data. The intelligence service of a foreign government wants to steal secret information. There are also many different known attack vectors that these groups can effectively exploit to gain unauthorized access to hospital IT/OT/CE infrastructure.

Inadequately tested hardware upgrades must be considered as one of the most significant risk factors for cyber security in hospital systems and equipment. The threats posed by them can be exploited by both inside and external actors. According to Piggin (2017, 6-7.) threats can be accidental or described because of non-validated changes. Cyberattack vectors among others are:

- Communication – disruption of network/device communications,
- Database injection – used to gain access to data or systems and to steal data,
- Replay – replaying data to gain access to systems or to falsify data,
- Spoofing or impersonation –fooling hardware or software making communication appear to originate from elsewhere,
- Social engineering – the attempt to obtain information by subterfuge from personnel that can then be used to attack computers, devices, or networks,
- Phishing – a form of social engineering, using forged email or websites to entice the victim to reveal information,
- Malicious code – to gather information, destroy data, provide a means to access a system, falsify system data or reports, or provide time-consuming irritation to operators and maintenance personnel,
- Distributed Denial of Service (DDoS) – this affects the availability of networks and computing resources (e.g., operating systems, hard drives, and applications),
- Escalation of privileges – a technique to increase the effectiveness of an attack by obtaining privileged access to perform actions that would otherwise be prevented,
- Physical destruction – attacks aimed at destroying or incapacitating physical devices or components. These might be direct or indirect via cyber-attack to cause actions that lead to physical damage (such as the Stuxnet worm).

3.3.1 Ransomware

Ransomware is a type of malware that threatens to publish the victim's data or perpetually block access to it unless a ransom is paid. It encrypts the victim's files, making them inaccessible, and demands a ransom payment to decrypt them. In a properly implemented attack, recovering the files without the decryption key is an intractable problem – and

difficult to trace digital currencies such as Bitcoin and other cryptocurrencies are used for the ransoms. Ransomware often spreads like other malware as email attachments, requiring the user to open the file. Another infection method is spam, which has links to websites by which malware is downloaded to the computer.
Hospitals have been the target of malware, and special attention was paid in May 2017 to the widespread WannaCry blackmail malware, which spread to 48 National Health Service organizations in the UK.

Hospitals have been the target of blackmail malware for many different reasons. One reason is that hospitals often have multiple information systems and also old operating systems in use. It is not possible to frequently update all devices that are in clinical use due to them being constantly needed. Another reason is that the operation of hospitals requires that clinical information systems be available like the patient information system, and without this information, the operation of hospitals will be significantly slowed down, which can cause problems for the patient's health.

Example:
The private mental health services firm Vastaamo has been at the center of a hacking and blackmail scandal after it emerged that highly sensitive information on thousands of patients had been stolen from its database. The total number of compromised data is 40 000.

A blackmailer demanding money from a group of psychotherapy centres has released more highly sensitive personal information about more than 200 of its patients. The perpetrator has threatened to publish more daily unless the Vastaamo psychotherapy centre firm pays a ransom of nearly half a million euros. A second batch of about 100 patient reports appeared on the anonymous Tor network, bringing the total to more than 200. They include highly intimate information about Vastaamo customers' personal lives and mental health issues, along with their names, addresses and social security numbers. The unknown extortionist has published messages in English purporting to be in correspondence with representatives of the company. The blackmailer is demanding that Vastaamo pay 40 bitcoins to halt the release of more patient data. The result was the bankruptcy of Vastamo. (YLE, 2020)

Example:
The WannaCry ransomware attack was a May 2017 worldwide cyberattack by the WannaCry ransomware cryptoworm, which targeted computers running the Microsoft Windows operating system by encrypting data and demanding ransom payments in the Bitcoin cryptocurrency. It propagates using EternalBlue, an exploit of Windows' Server Message Block (SMB) protocol. While Microsoft had released patches previously to close the exploit, much of WannaCry's spread was from organizations that had not applied these or were using older Windows systems that were past their end-of-life. When executed, the WannaCry malware first checks the "kill switch" domain name; if it is not found, then the ransomware encrypts the computer's data, then attempts to exploit the SMB vulnerability to spread out to random computers on the Internet, and "laterally" to computers on the same network. As with other modern ransomware, the payload displays a message informing the user that files have been encrypted and demands a payment of around US$300 in bitcoin

within three days, or US$600 within seven days. Many hospitals world-wide with services impacted, and medical devices hit specifically hard, like radiology modalities, contract injectors and patient monitoring systems, others. (Symantec, 2017; Kusche, 2018)

Looking at the ransomware case that have occurred in hospitals and other health services over the past years, their impact has been significant. Infections have resulted in the inaccessibility of, for example, the patient information system, appointment booking, and X-ray equipment. In some cases, patient data has also been stolen. Only a few hospitals have told the public that they have paid a ransom and many hospitals have had backups that could be used for recovery.

3.3.2 Hacking and data breach

Definition of HHS is: "A data breach is a security violation in which sensitive, protected or confidential data is copied, transmitted, viewed, stolen or used by an individual unauthorized to do so." Data breaches may involve financial information such as credit card or bank details, personal health information, personally identifiable information (PII), trade secrets of corporations or intellectual property. Most data breaches involve overexposed and vulnerable unstructured data – files, documents, and sensitive information. (HHS, 2020)

Patient records contain a large amount of personal information that is of interest to criminals. Information stolen from health care systems are name, address, date of birth, social security number, bank account number, credit card number, medication, treatments / surgeries, insurance information, and much more personal information. The information allows for a wide range of harm to the individual, and criminals can sell the information directly or use the information as part of an attack on an individual.

The US Department of Health and Human Services' (HHS) breach portal containing information about breaches of protected health information. According to the HHS breach portal, data breaches affected 27 million people in 2019 in U.S. Top 10 breaches by number of individuals affected, currently listed on HHS's breach portal. (HHS, 2020)

Table 1: Top 10 breaches by number of individuals affected in US.

Name of Covered Entity	Covered Entity Type	Individuals Affected	Type of Breach	Location of Breached Information	Year
Anthem Inc.	Health Plan	78 800 000	Hacking/IT Incident	Network Server	2015
American Medical Collection Agency	Business Associate	26 059 725	Hacking/IT Incident	Network Server	2019

Optum360, LLC	Business Associate	11 500 000	Hacking/IT Incident	Network Server	2019
Premera Blue Cross	Health Plan	11 000 000	Hacking/IT Incident	Network Server	2015
Laboratory Corporation of America	Health Plan	10 251 784	Hacking/IT Incident	Network Server	2019
Excellus Health Plan, Inc.	Health Plan	10 000 000	Hacking/IT Incident	Network Server	2015
Community Health Systems Professional Services Corporations	Healthcare Provider	6 121 158	Hacking/IT Incident	Network Server	2014
Science Applications International Corporation	Business Associate	4 900 000	Loss	Other	2011
Community Health Systems Professional Services Corporation	Business Associate	4 500 000	Theft	Network Server	2014
University of California, Los Angeles Health	Healthcare Provider	4 500 000	Hacking/IT Incident	Network Server	2015

3.3.3 Distributed Denial of Service attacks

Distributed denial of service (DDoS) attacks are a popular tactic, technique, and procedure (TTP) used by hacktivists and cybercriminals to overwhelm a network to the point of inoperability. This can pose a serious problem for healthcare providers who need access to the network to provide proper patient care or need access to the Internet to send and receive emails, prescriptions, records, and information. While some DDoS attacks are opportunistic or even accidental, many target victims for a social, political, ideological, or financial cause related to a situation that angers the cyber threat actors. (CIS, 2020a)

In DDoS attacks, patient data is often not at risk, but patient safety can suffer when they cannot access their data or hospital staff are unable to deliver planned actions because they do not have access to medication data, for example.

Example:
This was the case with Boston Children's Hospital in 2014. Anonymous (a well-known hacktivist group) targeted the Boston's Children's Hospital with a DDoS attack after the hospital recommended one of their patients, a 14-year-old girl, be admitted as a ward of the state and that custody be withdrawn from her parents. The doctors believed the child's ailment was actually a psychological disorder and that her parents were pushing for unnecessary treatments for a disorder the child did not have. The custody debate put Boston Children's Hospital in the middle of this controversial case, and some, including members of Anonymous, viewed this as an infringement on the girl's rights. Anonymous acted by conducting DDoS attacks against the hospital's network, which resulted in others on that network, including Harvard University and all its hospitals, to lose Internet access as well. The networks experienced outages for almost a week, and some medical patients and medical personnel could not use their online accounts to check appointments, test results, and other case information. As a result, the hospital spent more than $300,000 responding to and mitigating the damage from this attack, according to the attacker's arrest affidavit. (CIS, 2020a)

3.3.4 Insider threats

Organizations are often too preoccupied with defending the integrity of their company and network from external threats to address the very real and dangerous risk that may lie within their own organization - insiders. The insider poses a threat because the legitimate access they have or had to proprietary systems discounts them from facing traditional cybersecurity defenses, such as intrusion detection devices or physical security. They also may have knowledge of the network setup and vulnerabilities, or the ability to obtain that knowledge, better than almost anyone on the outside. While an insider may be simply careless, others cause destruction with malice. The insider threat concept encompasses a variety of employees: from those unknowingly clicking on a malicious link which compromises the network or losing a work device containing sensitive data to those maliciously giving away access codes or purposely selling PHI/PII for profit. (CIS, 2020b)

Patient data is also at risk when stored, for example, on laptops that are taken outside the hospital. Laptops have been stolen from doctor's offices, cars, and healthcare professionals' homes. What makes these situations problematic is that computers often have a password, but the hard drive itself or its data is not encrypted, so a criminal can access all the data if, for example, a password query is bypassed.

Example:
An insider victimized one Texas hospital when an employee built a botnet, using the hospital network, to attack rival hacking groups. The individual was eventually caught after he filmed himself staging an infiltration of the hospital network and then posted it on YouTube for public viewing. The video clearly shows the individual using a specific key to "infiltrate" the hospital, which revealed his identity as Jesse McGraw, a night security guard of the building. The investigation revealed that McGraw had downloaded malware on

dozens of machines, including nursing stations with patient records. Additionally, he installed a backdoor in the HVAC unit, which, if failed, would have caused damage to drugs and medicines and affected hospital patients during the hot Texas summer. McGraw pled guilty to computer tampering charges and is serving a 9-year sentence in addition to paying $31,000 in fines. (CIS, 2020b)

4 Healthcare cyber security

The technical infrastructure underlying the healthcare systems is extremely complex. It must support not only patient records but also a diverse suite of medical devices used in diagnosing, monitoring, and treating patients. Understanding and managing cybersecurity risks for this mission-critical environment is challenging as the healthcare system has a mixture of state-of- the-art applications and devices, as well as older legacy devices that use unsupported operating systems or networking protocols. In addition, it is difficult to make these systems available for updates since they often provide round-the-clock care to patients and cannot be taken out of service. Hospital environments are also challenging because staff and patients bring their own devices (BYOD) inside the facilities, as well as many different medical devices used in medical research. (Csulak et.al, 2017, 22–23.)

4.1 Best practices

National standardization bodies draw up national standards and participate in the drafting of international standards, taking into account best practice. Organizations use standards and various other guidelines and recommendations on a voluntary basis. The best practices and objectives that emerge from them are usually related to operational development, which are at best, proactive procedures. In the cyber world, they assist their users in improving the reliability, continuity, quality, risk management, and preparedness of an organization's operations. In this case, the functions may be, for example, the management and administration of cyber security or the technical development, maintenance or use of information systems, information networks and ICT services. (Pöyhönen, 2020)
Many organizations' cyber security activities continue to be characterized by a responsive approach, with hospitals being no exception. A responsive approach means that in the event of a cyber-attack, and the action are quick conclusions and urgent measures. Developing cyber security using best practices creates for the hospital proactive methods instead reactive actions. (Pöyhönen, 2020)

NIST Framework for Improving Critical Infrastructure Cybersecurity provides a common language for understanding, managing, and expressing cybersecurity risk to internal and external stakeholders. It can be used to help identify and prioritize actions for reducing cybersecurity risk, and it is a tool for aligning policy, business, and technological approaches to managing that risk. It can be used to manage cybersecurity risk across entire organizations, or it can be focused on the delivery of critical services within an organization. The Framework core provides a set of activities to achieve specific cybersecurity outcomes, and references examples of guidance to achieve those outcomes. (NIST, 2018, 6–8.).

The list below summarizes the measures of the NIST framework and their contents:

- Identify – Develop an organizational understanding to manage cybersecurity risk to systems, people, assets, data, and capabilities.
- Protect – Develop and implement appropriate safeguards to ensure delivery of critical services.
- Detect – Develop and implement appropriate activities to identify the occurrence of a cybersecurity event.
- Respond – Develop and implement appropriate activities to take action regarding a detected cybersecurity incident.
- Recover – Develop and implement appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity incident.

Categories are areas of main activities that can be divided into cyber security review groups, such as "access control" or "identification processes." The subcategories are further subdivided into technical sections and/or management activities. Informative references are parts of standards, guidelines and practices (NIST, 2018, 6–8, 13.)

Discussion in the U.S within the Health Care Industry Cybersecurity Task Force (HCIC Task Force) focused information gathering from external stakeholders and subject matter experts across the healthcare industry and other sectors. The Task Force identified six high-level imperatives that must be achieved to increase security within the healthcare industry. The imperatives are:

1. Define and streamline leadership, governance, and expectations for healthcare industry cybersecurity,
2. Increase the security and resilience of medical devices and health IT,
3. Develop the healthcare workforce capacity necessary to prioritize and ensure cybersecurity awareness and technical capabilities,
4. Increase healthcare industry readiness through improved cybersecurity awareness and education,
5. Identify mechanisms to protect R&D efforts and intellectual property from attacks or exposure,
6. Improve information sharing of cyber security threats, risks, and mitigations.

(Csulak, et al, 2017, 24–44)

Both large and small healthcare organizations struggle with unsupported legacy systems that cannot easily be replaced (hardware, software, and operating systems) and the systems have large numbers of vulnerabilities and few modern countermeasures.

The implementation of key cyber security measures include: (ENISA, 2016, 53):

- Network segmentation (smart firewalls),
- Network monitoring and intrusion detection,
- Robust encryption,
- Access control,

- Authentication and authorization.

Clinicians in a hospital setting are required to access multiple computers throughout the facility repeatedly (up to 70 times per shift) as they deliver care to patients. To authenticate their identity so that they can perform common tasks (e.g., access a patient's medical record, order diagnostic tests, prescribe medication, etc.), a clinician typically enters his or her username and a unique password. This widely used, single factor approach to accessing information is particularly prone to cyber-attack as such passwords can be weak, stolen, and are vulnerable to external phishing attacks, malware, and social engineering threats. NIST SP 800-6355 adopts alternatives to the use of passwords for user authentication, including items in the user's possession (e.g., a proximity card or token) or biometrics. (Csulak et.al, 2017, 32.)

Clinicians also interact with medical devices and the integrity of the devices used in these treatments must be assured from a bioengineering and a cybersecurity perspective. The provider operating the device must be authenticated and authorized to operate it, and the patient needs to be accurately identified as the person authorized to receive the treatment. Moreover, communications between the device and other healthcare technologies should be authenticated (i.e., devices should know what technologies they are communicating with and should only be communicating with technologies with the appropriate credentials). (Csulak et.al, 2017, 32.)

Many hospitals still follow a reactive approach to information security. Measures are frequently taken only after an incident has occurred. In the healthcare context, avoiding incidents is particularly important as trustworthiness is of very high priority. Security incidents may not only threaten personal health information but also patient safety. Hospitals should also be well prepared for the possibility of security incidents by having concrete response and recovery plans in place, like:

- Perform a cost benefit analysis for the most important IoT components in the hospital. Smart hospital is expensive to implement, it needs to be adequately protected.
- Create an information security strategy for the smart assets in the hospital. Clear roles and responsibilities as well as regular training and awareness raising activities are key elements of a proactive approach to information security.
- Create a BYOD and mobile device policy for users: as this is a component of a smart hospital ecosystem this needs to become a priority.
- Identify the assets and how these will be interconnected (or connected to the Internet). For some systems, the right move for safety and resilience might be for the manufacturer to refuse built-in network capabilities into the device.
- Define and implement security baselines on all major operating systems.

(ENISA, 2016, 53.)

The healthcare industry must increase outreach for cyber security across all members of the healthcare workforce through ongoing workshops, meetings, conferences, and tabletop exercises. Also, the healthcare industry must develop cyber security programs (including

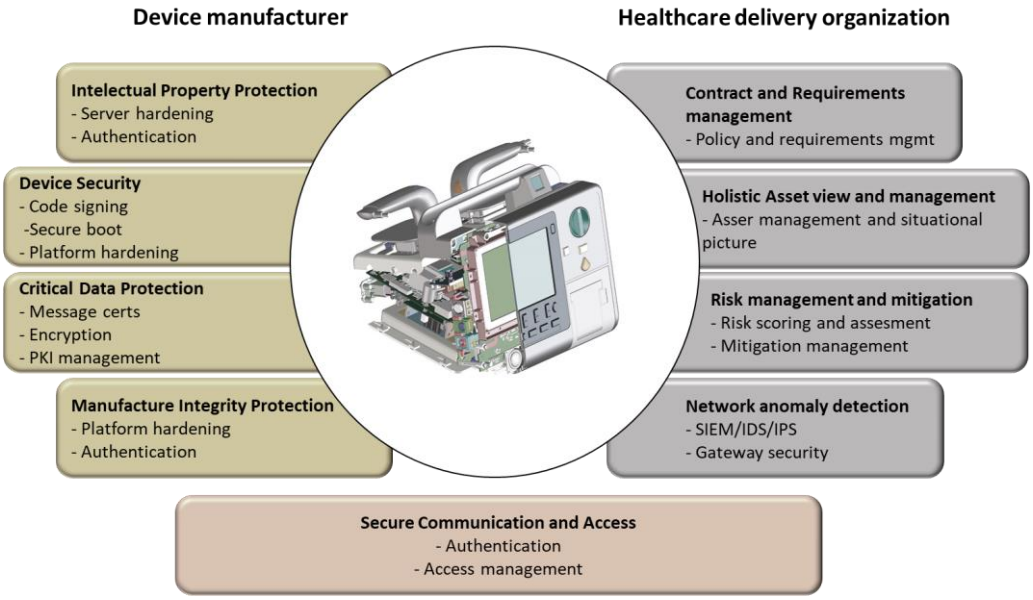
on-line education) to educate decision makers, executives, and board members about the importance of cyber security, as cybersecurity is the responsibility of top management. As part of this holistic cyber security strategy, it is critical that a thorough baseline is established whereby inherent trust can be established between patients and clinicians, technologies, and processes, and ultimately institutions and patients. (Csulak ym., 2017, 40.)

4.2 Cyber security of medical devices

The cybersecurity of medical devices has increasingly become a concern to healthcare providers, device manufacturers, regulators, and patients. Due to their long useful life, unique care-critical use case, and regulatory oversight, these devices tend to have a low security maturity, significant vulnerabilities, and an overall high susceptibility to security threats.

Lifecycle management and procurement of the medical devices need a shared responsibility. As part of their asset and risk assessment processes, actors articulate described cyber security requirements.

Figure 6 outlines the liability measures between the device manufacturer and the healthcare organization.



Fig, 6 Division of cybersecurity responsibilities for medical devices (Symantec Corporation, 2016, 2.)

Medical device providers should assign classification and priorities to medical devices based on the risk/type of device. The classifications may vary based on organizational priorities but could follow a model like the example described below. (See table 1 and table 2).

Table 1 Medical Device Priorities (Meditology Services LLC, 2017, 14)

Priority Level	Description
1	Lifesaving (defibrillator, pacemaker, ventilator)
2	Curative/Therapeutic (infusion pump, hyperbaric chamber, dialysis)
3	Patient Diagnostic (ECG, Ultrasound, X-Ray, lab equipment)
4	Analytics (fetal monitors, patient monitors)
5	Miscellaneous (medical cabinet, autoclave, scale)

Table 2 Medical Device Classifications (Meditology Services LLC, 2017, 14)

Turvallisuus-luokitus	Kuvaus
A	Over 100,000 records stored, transmitted or processed
B	Between 10,001 and 99,999 records stored, transmitted, or processed
C	Less than 10,000 records stored, transmitted or processed
D	Device does not store, transmit or process PHI

Organizations should not wait for regulators to enforce security standards. Instead, health entities should be active in conversations with regulators about needed data security standards and work collaboratively with the medical device market to ensure appropriate data security measures are factored into product design and implementations. The medical devices should be tiered based on clinical safety considerations, the volume of patient records managed by the device and platform, etc. Medical device security programs must prioritize which devices to secure first and then move on to others over time. (Meditology Services LLC, 2018)

4.3 New technologies may help

The technology revolution is creating a unique environment for all industries to grow and evolve. The healthcare and pharmaceutical industries are quickly discovering that the right tech could also be the key to delivering better care to patients. Artificial Intelligence is one of the most prominent examples of Industry 4.0 technology. With machines that can learn from the enormous amounts of data in every healthcare industry, there will be endless opportunities. (Peters, 2020)

Cyber-physical systems are ubiquitous and used in many applications, from industrial control systems, novel communication systems, to critical infrastructure. These systems generate, process, and exchange vast amounts of security-critical and privacy-sensitive data, which makes them attractive targets of attacks. Industry 4.0 and its main enabling information and communication technologies are completely changing both services and production worlds. This is especially true for the healthcare domain, where the Internet of Things, Cloud and Fog Computing, and Big Data technologies are revolutionizing eHealth and its whole ecosystem, moving it towards Healthcare 4.0. (Sadeghi, Wachsmann & Waidner, 2015, 1–2; Aceto et.al 2020)

Industry 4.0 is the combination of the automation process, manufacturing units and smart machines. It consists of digitization, IoT, internal connected network, human resources for supervision, Supervisory Control and Data Acquisition (SCADA), robots for automation of many critical functions, valves, sensors, actuators, PLC system, communication protocols and cyber security. It uses artificial intelligence to help clinical decision-making, share information digitally in hospitals and enables to create smart cyber security to hospital environment. (Javaid and Haleem, 2019)

Artificial Intelligence is intelligence exhibited by machines. Any system that perceives its environment and takes actions that maximize its chance of success at some goal may be defined as AI. For example, cognitive computing is a comprehensive set of capabilities based on technologies such as deep learning, machine learning, natural language processing, reasoning and decision technologies, speech and vision technologies, human interface technologies, semantic technology, dialog, and narrative generation, among other technologies. Artificial intelligence and robotics have steadily growing roles in healthcare. Organizations benefit from the ability of cognitive systems to improve their expertise quickly and from sharing it to all those who need it. The know-how of top experts is quickly made available to all when their subject matter expertise is taught to a cognitive system. Through repeated use, the system will provide increasingly accurate responses, eventually eclipsing the accuracy of human experts. With artificial intelligence, comprehension can be outsourced. As the intelligence of machines improve, they will use deep learning to understand the collective information. With the use of digital sensor data, equipment based on artificial intelligence can used to develop smart advisors, teachers, or assistants. (Vähäkainu et.al, 2019, 431)

The integrated framework of key security capabilities should form the core of the cyber security solutions. At the core of this structure is security intelligence and analytics. This serves as the key piece, ingesting security data across an IT environment (e.g., logs, flows, incidents, events, packets, and anomalies) as well as information beyond the organization (e.g., blogs, research information and websites) to understand threats and attacks. Security infrastructure uses its own network of integrated security capabilities to intelligently detect the symptoms of a cyber-attack, like a breach on the network, an abnormal login on a high-value server, rogue cloud app usage, and respond appropriately. (Falco, 2016)

Figure 7 below shows an example of IBM's concept of an integrated cybersecurity solution, with analytics capabilities at the heart of the solution.

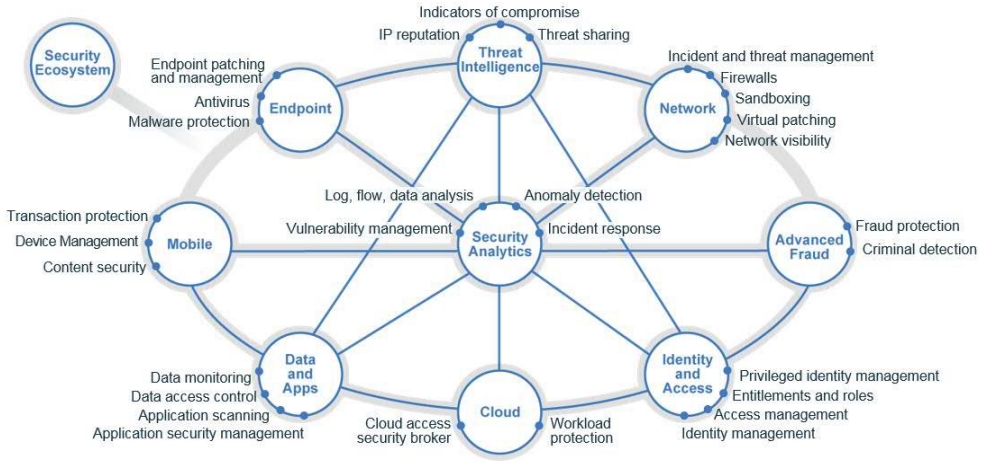


Fig. 7 IBM's integrated cybersecurity concept (Falco, 2016)

With analytics at the core, integrated capabilities deliver a level of visibility and defense that no single security solution can provide on its own.

MIT Computer Science and Artificial Intelligence Laboratory (CSAIL) and PatternEx have developed an artificial intelligence AI2 platform to predict cyber-attacks. According to Conner-Simons (2016), the AI2 platform was able to reach 86 % accuracy in detecting cyber-attacks, which is approximately three times better than results of previous studies. Tests were conducted with 3.6 billion data components (log lines), which were generated by millions of users in a three-month research period. To prevent attacks, AI2 identifies suspicious activity by applying clustering algorithms to the input data by utilizing unsupervised machine learning algorithms. Hence, the results will be presented to analysts, who confirm which incidents are real attacks. Analysts also incorporate the outcome into platform models (supervised learning) for the next set of data, which enables further learning. The system is also capable of continuously generating new models within hours, which can significantly improve the speed of its detection ability of cyber-attacks. (Conner-Simons, 2016; Veeramachaneni et.al, 2016, 49; Vähäkainu et.al, 2019, 435.)

Doctors at the University of Tokyo reported that they diagnosed with IBM Watson a 60-year-old woman with rare leukemia that had been identified incorrectly a month earlier. Watson needed only 10 minutes to compare the patient's genetic changes to the 20 million cancer study publication database. Watson provided an accurate diagnosis, instructions on treatment, and medication to achieve the desired treatment outcomes. (Fingas, 2016)

4.4 Hospital cybersecurity architecture

The starting point for a hospital's cyber security architecture can be formed by utilizing the definitions and recommendations of the Health Care Industry Cybersecurity Task Force (HCIC Task Force) to organize policies (Csulak et.al, 2017, 1.). They relate to organizational

leadership and management, hospital resilience, staff competence, and research and information sharing. Measures should also identify cyber security challenges, which consist of the different life-cycle stages of equipment and are reflected at system level in the deployment, management, and maintenance of new devices.

As the pace of development has been very rapid and new technology has been introduced very quickly, the international standard work has not been involved in the development process. We often have manufacturer-specific solutions for IoT devices, different sensors, and data storage systems in some of the service providers' Data Center, shown in Figure 8. This issue in turn leads to a challenge of connecting IoT devices to smart devices. (Hummelholm, 2019, 641-642.)

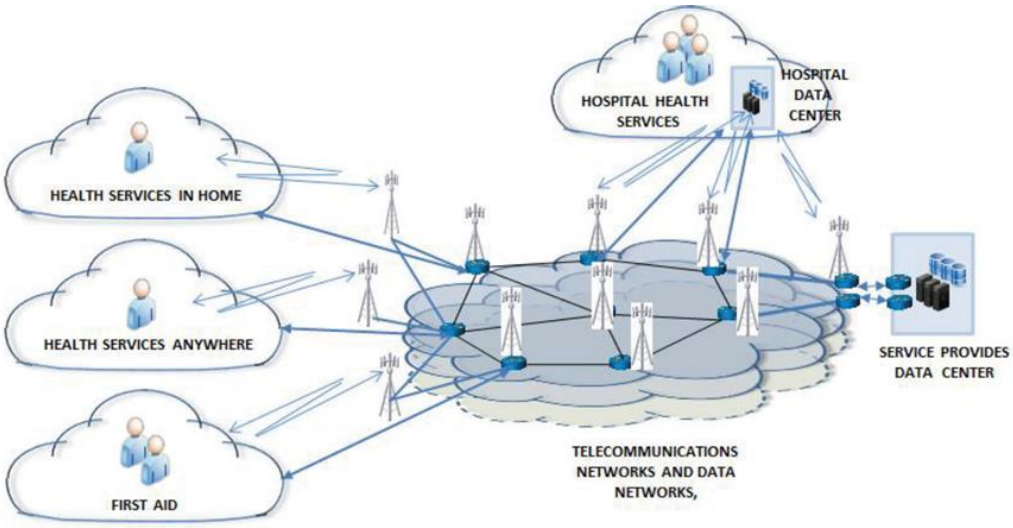


Fig. 8 E-Health top level architecture (Hummelholm, 2019, 642)

The publication of the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" can also be applied in a hospital operating environment. The starting point is to identify the processes in the hospital and the devices and systems. This is particularly related to an organization's ability to understand and manage cyber security risks in them. Security measures can then be developed and implemented with appropriate cyber security products and services that specifically address device risks. The situational picture and the situational awareness are the basic resource to create effective cyber security in hospital. (Lehto et.al, 2018, 62; NIST, 2018)

4.4.3 Development of system level protection in a hospital

In cyber-physical systems, networked devices, and their software control physical processes. The operation of the hospital involves a significant number of technical devices and functional entities consisting of systems that are cyber-physical systems. The hospital is technically a system of systems and is in turn part of a large healthcare complex. Functions are thus networked at many levels in healthcare.

The development of digital methods of treatment with sensors and IoT devices is strongly developed to improve patient care, to look at their condition remotely at home or wherever they are moving in real time. The future healthcare operation environments are presented in figure 8. (Hummelholm, 2019, 643.)

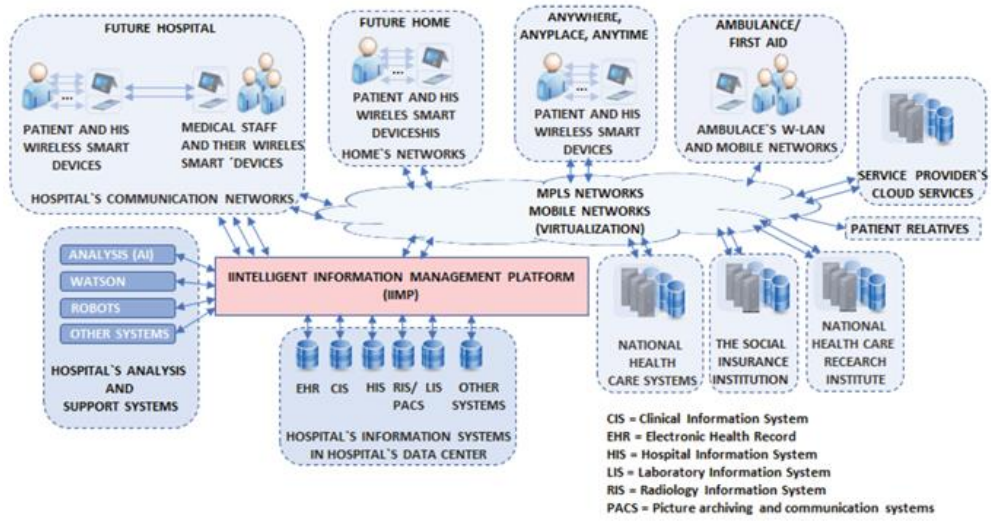


Fig. 8 E-Health or m-health operating environment, top level architecture (Hummelholm, 2019, 643.)

So, system-level protection can be developed by applying new technologies to solutions.

Conclusion

The most critical components in digital healthcare environments are mainly patient healthcare systems and devices, whose cyber security needs to be analyzed and functionalities monitored because they are critical systems in the patients' treatments.

Cyber security can be an enabler for the healthcare industry, supporting both its business and clinical objectives, as well as facilitating the delivery of efficient, high-quality patient care. However, this requires a holistic cybersecurity strategy. Organizations that do not adopt a holistic strategy not only put their data, organizations, and reputation at risk, but the welfare and safety of their patients.

If visions, strategies, scenarios and use cases are lacking in healthcare operations, then we do not have sufficiently precise architectural descriptions of ICT systems used in healthcare, and it is difficult to perceive the entities and its included service chains. It is difficult and even impossible to carry out risk and threat analyses of the services provided by service providers with sufficient accuracy. It may not be possible to identify and analyse healthcare service chains and to carry out related risk and threat analyses. The case Vastaamo, in

Finland, is a good example of what happens when healthcare-related services are outsourced. Due to outsourcing, the implementation and checking of services, the systems and applications required for them, are no longer the responsibility of healthcare organizations. In such situations, there may be deficiencies in inspections and audits of critical healthcare systems and applications. If we are unaware of the vulnerabilities in our systems and applications and then we are unable to fix them, it will allow hackers and cyber attackers to attack our system. In the case of Vastaamo, it is difficult to find the organizations or people who will have to answer in court for these consequences of the information leak. Unfortunately, it is difficult for victims of information leakage to receive adequate and correct compensation, because after that leakage, their entire lives can contain long-term suffering and pain.

Often because of service outsourcing, cloud services may become use and their actual location may not be known and service chains cannot be defined. In critical services where 1 + 1 protection and backup are necessary, signals time delays are critical, making service chains definitions and their analyses relevant to functionality. In a 1 + 1 protected operating environment, the exchange of services for the protection system must occur in milliseconds. This means that continuity management must also be considered in the design and development of healthcare systems and services based on different scenarios. Design and developments based on scenarios also provide better opportunities for cyber security risk and threat analyses of healthcare systems. In addition, there are also many integrations between healthcare systems. In the healthcare areas outlined above, we need more research to develop better and cyber-secure systems.

At present, several cyber security solutions and tools are available for healthcare organization's needs. The challenge is the fragmentation of solutions and tools, as well as the problems of the implementation and maintenance of new systems, which cause management difficulties and increase complexity within the whole system. The complexity of systems requires the development of integrated systems that identify both external and internal threats, and which have comprehensive, built-in cyber security systems. Integrated and holistic solutions provide the required visibility for all levels of the ICT system, which means protection and preventing of cyber-attacks can be implemented as a whole rather than as individual procedures.

We recommend that healthcare organizations and hospitals do and develop visions, strategies, scenarios, and use cases from their healthcare environment, and develop systems and application architectures based on this information. They then have a clear picture of their operating environment, systems, and applications, and can conduct cyber risk and threat analyzes for the systems there.

References

Aceto G., Persico V., Pescapé A. 2020. Industry 4.0 and Health: Internet of Things, Big Data, and Cloud Computing for Healthcare 4.0, Journal of Industrial Information Integration, Volume 18, June 2020.

Chanchal S. 2020. What is Hospital Information System & Our Top 15 Picks, blog in Software Suggest, Jun 1, 2020.

CIS. 2020a. DDoS Attacks: In the Healthcare Sector, blog, https://www.cisecurity.org/blog/ddos-attacks-in-the-healthcare-sector/

CIS. 2020b. Insider Threats: In the Healthcare Sector, blog. https://www.cisecurity.org/blog/insider-threats-in-the-healthcare-sector/

Conner-Simons A. 2016. System predicts 85 percent of cyber-attacks using input from human experts. MIT News Internet page. http://news.mit.edu/2016/ai-system-predicts-85-percent-cyber-attacks-using-input-human-experts-0418

Csulak E., Meadows T., Corman J., DeCesare G., Fernando A., Finn D., Jarrett M., Laybourn L., McNeil M., McWhorte D., Mellinger R., Monson J., Radadoos R., Rice,T. Sardanopoli V., Suarez R., Stine K., Sublett C., Thompson L., Ting D. & Trotter F. 2017. Report on improving cybersecurity in the health care industry. Health care industry cybersecurity task force-report. https://www.phe.gov/preparedness/planning/cybertf/documents/report2017.pdf

ENISA. 2016. Smart Hospitals: Security and Resilience for Smart Health Service and Infrastructures. https://www.enisa.europa.eu/publications/cyber-security-and-resilience-for-smart-hospitals

ENISA. 2020. Procurement Guidelines for Cybersecurity in Hospitals - Good practices for the security of Healthcare services, February 2020

EU. 1993. EU Council Directive 93/42/EEC of 14 June 1993 concerning medical devices

Falco C. 2016. Unleashing the Immune System: How to Boost Your Security Hygiene. IBM Internet page. https://securityintelligence.com/news/unleashing-the-immune-system-how-to-boost-your-security-hygiene/

Fingas J. 2016. IBM's Watson AI saved a woman from leukemia, blog in Engadged, 08.07.2016.

Halonen P. 2016. Kyberturvallisuus terveydenhuollossa. Viestintäviraston kyberturvallisuuskeskuksen PowerPoint-esitys. https://docplayer.fi/25743256-Kyberturvallisuus-terveydenhuollossa-perttu-halonen-helsinki.html

HHS. 2020. U.S. Department of Health and Human Services - Office for Civil Rights, Breach Portal. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HIPAA. 2020. Healthcare Data Breach Report, Jan 19, 2021. https://www.hipaajournal.com/2020-healthcare-data-breach-report-us/

Hummelholm A. 2019. E-Health Systems in Digital Environments, 18th European Conference on Cyber Warfare and Security, 4 - 5 July 2019, University of Coimbra, Portugal, pages 641-649

Infowerks. 2020. What Is a Health Information System? Blog in InfoWerks, January 6, 2020.

Integrating the Healthcare Enterprise. 2015. IHE Patient Care Device (PCD) White Paper 10 Medical Equipment Management (MEM): Medical Device Cyber Security – Best Practice Guide. Integrating the Healthcare Enterprise report. http://www.ihe.net/uploadedFiles/Documents/PCD/IHE_PCD_WP_Cyber-Security_Rev1.1_2015-10-14.pdf

ISO. 2012. ISO/IEC 27032 Cyber Security Trainings.

ITU. 2018. Guide to Developing a National Cybersecurity Strategy.

Javaid M., Haleem A. 2019. Industry 4.0 applications in medical field: A brief review, Current Medicine Research and Practice 9(3), April 2019

Kanta. 2020. Kanta system homepage, https://www.kanta.fi/en/what-are-kanta-services, retrieved 28.1.2021.
Kolbasuk McGee M. 2021. Analysis: 2020 Health Data Breach Trends, HealthcareInfoSecurity, Jan 4, 2021.
Kusche K. 2018. Getting Ready for the Next International Cyber-attack, HIMSS, March 5, 2018
Lehto Martti. 2014. Kybertaistelu ilmavoimaympäristössä. Teoksessa T. Kuusisto (toim.), Kybertaistelu 2020, (157–178). Taktiikan laitos Julkaisusarja 2, No. 1/2014. Helsinki: Maanpuolustuskorkeakoulu.
Lehto Martti. 2015. Phenomena in the Cyber World. In M. Lehto & P. Neittaanmäki. Cyber Security: Analytics, Technology and Automation, (3 - 29). USA: Springer.
Lehto M., Limnéll J., Innola E., Pöyhönen J., Rusi T., Salminen M. 2017. Finland's cyber security: the present state, vision and the actions needed to achieve the vision, Publications of the Government´s analysis, assessment and research activities 30/2017.
Lehto M., Limnéll J., Kokkomäki T., Pöyhönen J., Salminen M. 2018. Strategic leadership of cyber security in Finland, Publications of the Government´s analysis, assessment and research activities 28/2018
Levin D. 2019. What is a Health Information System? blog in Datica, Feb 4, 2019
Libicki M. C. 2007. Conquest in Cyberspace – National Security and Information Warfare. New York: Cambridge University Press.
McGovern L., Miller G., Hughes-Cromwick P. 2014. The Relative Contribution of Multiple Determinants to Health Outcomes, Health Affairs, Vol 33, Issue 2, Aug 21, 2014
Meditology Services LLC. 2017. Hijacking Your Life Support: Medical Device Security. https://www.meditologyservices.com/fullpanel/uploads/files/whitepaper-medical-device-security-2017.pdf
Meditology Services LLC. 2018. Healthcare's Space Junk: Medical Device & IoT Security. https://www.meditologyservices.com/healthcares-space-junk-medical-device-iot-security-part-3/
NIST. (2018) National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity version 1.1. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
Peters J. 2020. How is Industry 4.0 Affecting Healthcare, blog in Intetics Inc. Jun 9, 2020
Piggin R. 2017. Cybersecurity of medical devices - Addressing patient safety and the security of patient health information. BSI report. https://www.bsigroup.com/LocalFiles/EN-AU/ISO%2013485%20Medical%20Devices/Whitepapers/White_Paper___Cybersecurity_of_medical_devices.pdf
Pöyhönen J. 2020. Cyber security management and development as part of a critical infrastructure organization – System Thinking. University of Jyväskylä, dissertations 270.
Reddy M. Digital Transformation in Healthcare in 2021: 7 Key Trends, blog in Digital Authority Partners, January 4, 2021.

Sadeghi A. R., Wachsmann, C. & Waidner, M. 2015. Security and privacy challenges in industrial internet of things. Proceedings DAC '15 Proceedings of the 52nd Annual Design Automation Conference, 54 (1 - 6).

Sartonen M., Huhtinen A-M., Lehto M. 2016. Rhizomatic Target Audiences of the Cyber Domain. Journal of Information Warfare, 15(4), 1 - 13. https://toinformistoinfluence.com/2016/12/31/journal-of-information-warfare-volume-14-issue-4-fall-16-is-out/

Security committee. (2017). The Security Strategy for Society, Government Resolution / 2.11.2017. https://turvallisuuskomitea.fi/wp-content/uploads/2018/04/YTS_2017_english.pdf

Suomen Automaatioseura ry turvallisuusjaosto. 2010. Teollisuusautomaation tietoturva. Verkottumisen riskit ja niiden hallinta. 1. painos. https://zapdoc.site/queue/teollisuusautomaation-tietoturva-verkottumisen-riskit-ja-nii.html

Symantec. 2016. Symantec, Industry Focus: Medical Device Security. Symantec Corporation Internet page. https://www.symantec.com/content/dam/symantec/docs/data-sheets/symc-med-device-security-en.pdf

Symantec. 2017. What you need to know about the WannaCry Ransomware, Symantec Security Response. 23 Oct 2017, https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/wannacry-ransomware-attack

Veeramachaneni K., Arnaldo I., Cuesta-Infante A., Korrapati V., Bassias C. & Ke L. 2016. AI2: Training a big data machine to defend. Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing (HPSC), and IEEE International Conference on Intelligent Data and Security (IDS), 2016 IEEE 2nd International Conference, 9 - 10.

Verizon. 2018. Protected Health Information Data Breach Report, White Paper.

Viestintävirasto. 2016. Terveydenhuoltoalan kyberuhkia. https://www.viestintavirasto.fi/attachments/tietoturva/Terveydenhuoltoalan_kyberuhkia.pdf

Vähäkainu P., Lehto M. 2019. Artificial intelligence in the cyber security environment, the 14th International Conference on Cyber Warfare and Security, 28 February - 1 March 2019, Stellenbosch University, South Africa, pages 431-440

WHO. 2011. Core Medical Equipment, https://apps.who.int/iris/bitstream/handle/10665/95788/WHO_HSS_EHT_DIM_11.03_eng.pdf?sequence=1

Williams P. and Woodward A. 2015. Cybersecurity vulnerabilities in medical devices: a complex environment and multifaceted problem, Med Devices, Auckland, Issue 8: 305–316.

YLE. 2020. Extortionist publishes more sensitive data on psychotherapy centres' patients, https://yle.fi/uutiset/osasto/news/extortionist_publishes_more_sensitive_data_on_psychotherapy_centres_patients/11608960

Zhang Y., Qui M., Chun-Wei T., Hassan M. M. & Alamri A. 2017. Health-CPS: Healthcare Cyber-Physical System Assisted by Cloud and Big Data. *IEEE Systems Journal, 1* (88 - 95).

ANNEX 1 Core Medical Equipment

Core medical equipment refers here to technologies that are commonly considered as important or necessary for specific preventive, diagnostic, treatment or rehabilitation procedures carried out in most health care facilities. Today, there are more than 10,000 types of medical devices available. The selection of appropriate medical equipment always depends on local, regional or national requirements; factors to consider include the type of health facility where the devices are to be used, the health work force available and the burden of disease experienced in the specific catchment area. It is therefore impossible to make a list of core medical equipment which would be exhaustive and/or universally applicable. (WHO, 2011)

Table 2. Core medical equipment

Analyzer, laboratory, hematology, blood grouping	Electrocardiograph, ECG	Peritoneal dialysis unit
Anesthesia Unit	Electrosurgical Unit	Pulmonary function analyzer
Apnea Monitors	Fetal Heart Detector, Ultrasonic	Radiographic, Fluoroscopic System
Aspirator	Fetal monitor	Radiotherapy Planning System
Auditory Function Screening Device, Newborn	Glucose Analyzer	Radiotherapy Systems
Bilirubinometer	Hematology Point of	Remote-after loading brachytherapy system
Blood Gas/pH/Chemistry Point of Care Analyzer	Hemodialysis Unit	Scanning System, CT
Blood pressure monitor	Immunoassay Analyzer	Scanning System, Magnetic Resonance Imaging, Full-Body
Bronchoscope	Incubator, Infant	Scanning System, Ultrasonic
Cataract Extraction Units	Information	Transcutaneous Blood Gas Monitor
Clinical Chemistry Analyzer	Laser, CO2	Ventilator, Intensive Care
Colonoscope	Laser, Ophthalmic	Ventilator, Intensive Care, Neonatal/Pediatric
Cryosurgical Unit	Mammography unit	Ventilator, Portable
Cytometer	Monitor, Bedside, Electroencephalography	Videoconferencing system, Telemedicine
Defibrillator, External, Automated; Semi-automated	Monitor, Central Station	Warming Unit, Radiant, Infant
Defibrillator, External,	Monitoring System,	Whole Blood Coagulation

Manual	Physiologic	Analyzer
Densitometer, Bone	Monitor, Telemetric, Physiologic	