E-Health Systems in Digital Environments

Aarne Hummelholm
Faculty of Information Technology, University of Jyväskylä, Finland
Aarne.hummelholm@elisanet.fi

Abstract: As we live in the digital world, people can be provided with more effective treatment methods that allow them to live longer in their home and to live there better. People can be provided with better home care and preventive health care. People can easily carry portable sensors and intelligent devices in their bodies and wrists that relay their vital information to hospital systems in real time, from which healthcare staff can track human vitality even in real time. Although the digital world offers good opportunities to improve healthcare systems and make disease analyses more effective, we must look deeper about that issue. Devices and systems may not work well together. Almost every manufacturer has their own technical solutions and they only work in certain environments. There is a great need for unified concepts and for IT platform solutions in healthcare systems. The technology currently in use is very varied. Standards are developing now days, but they are not yet ready. In addition, the lack of technical and functional requirements for telemedical communications systems and equipment, as well as the requirements for providing secure data transmission in remote medical care. In the news we can see and hear often that there are a lot of medical devices that have damaged the patient's health around the world. And then there are a lot of vulnerabilities and that means security risks, cyber risks and the risks of reliability of data. These risks are associated with IoT devices and sensors, and in the field of data transfer. This document describes telemedicine solutions for the future of society. Includes a brief introduction of hospital equipment in a hospital environment and a patient's home. The main overall is the communication arrangements, consisting of the bio-signal formation of the patient's sensor and the flow of bio-signals to the hospital information systems for analysis and monitoring. This study examines cyber threats and attacks against e-health systems and what that means for patients` health. This study also examines the authenticity, traceability, authentication and protection of privacy.

Keywords: healthcare systems, vulnerabilities, cyber threat, cyber-attacks, telemedicine

1. Introduction

Today, we want to exploit the potential of digitalisation, including in the services of health care, in diagnostics and in the analysis of diseases, in the precautionary and in monitoring the progression of the disease. However, the rapid technological advances underlying digitalisation set their own challenges for technical systems of health care and the whole health services, with their guidelines and regulations.

It is imperative that health services are available for 24/7, regardless of time and place, anywhere qualitatively and equitably, not forgetting that patients or the elderly may be in cities or in rural areas long distance from the hospital or from treatment point. In addition, patient spatial data may be used to indicate the person's whereabouts so that it is possible to warn them if necessary, as soon as possible and to get help to the right place.

Health care is looked at in terms of services and quality, but at the same time cost-effectiveness has become increasingly important in the decision-making process. This also affects patient care methods and solutions. The goal is to organise treatments so that patients are in hospital so as short time as possible, and then patients will be sent home if the necessary conditions for arranging home care are in place.

The one aim of digitalisation is to create the conditions for the activities described above. The aim of digital systems is to provide the patient with treatment so that they can be sent to home care without undermining the quality of care or adequate levels, even in the circumstances prevailing at home. All this requires the introduction of new technologies and the integration of different types of transportable equipment, such as IoT, various sensors and actuators, as part of health systems. Together they produce a lot of information from the patient condition, from the elderly`s condition and the environment in real time. These large data are analysed in hospital systems and analyses are leading to the necessary treatment-related measures.

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 1. This issues in turn leads to a challenging of connection of IoT devices to smart devices.

Smart devices are then 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 analysed, and the care staff take the necessary decisions based on analysed results and gives information on management measures to the patients.

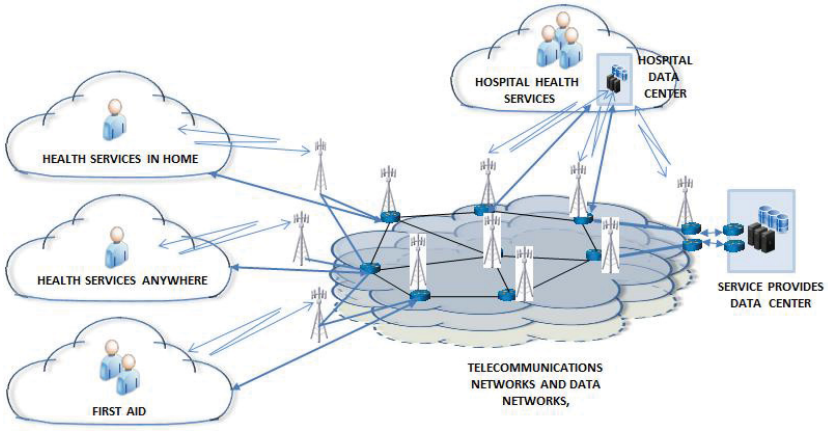

Figure 1: E-Health top level architecture

Also, for many technical specifications, the situation is variable, and the terms used vary, depending on the speaker, or depending on the time in which the term is used. We talk about the following terms, which vary slightly in importance: Telemedicine, Telehealth, e-Health and m-Health. In this document e-Health and m-Health terms are used. All this diversity of terms and undefined is also a source of challenges for security solutions, privacy and cyber security issues (EU- GDPR).

2. Chapter 1: Objective and grouping of paper

The research question is that whether e-Health systems are being used safe in digital environment.

To find the answer to the question, this study seeks to find a model that facilitates cyber threat assessment and threat comparisons and facilitates threat analysis in e-Health environment and systems. The results obtained through the model aims to facilitate the design and implementation of architectural solutions. The model implemented can help in better assessing the cyber-threat scenarios of future telecommunication environments and their impact probabilities e-health systems. The study draws on an e-Health operating environment with top-level architecture, figure 1, where services and infrastructure are grouped into different usage cases. Usage cases are divided into end-to-end communications segments. From these devices we can analyse vulnerabilities and from those we can analyse and define cyber threats to various devices, threats to services and threats to information systems. After that we can more accurately define, evaluate and analyse the cyber threats in whole system and get better overall picture of situation.

As shown in figure 1, there are several other viewpoints. Examination of threats can be made in the various usage cases with patient wearables, sensors and IoT devices including environments devices and e-Health services with them. When a patient or an elderly person is at home or outdoors using an e-Health application on their smart devices, he or she can also use other social services that are provided via telecommunications networks to him. This means that a patient or an elderly person is connected to the e-Health system in hospital or in a home and at the same time to another service or social media service that is currently being offered to people through the Internet. This will be a threat to healthcare systems and possibly to the entire e-Health service when patients or elderly persons exchange of information between the different service segments. The networks of those service providers are used to integrate health data of patients or elderly people to the hospitals systems. We must look carefully about this end-to-end communications path and all devices which are connected to that path. The above-described integration accelerates at all levels of activity, in each region both horizontally and vertically. Analysing the latest technologies and their services and applications in these smart environments will further complicate making cyber threat estimates. These considerations are considered in the selection of the target area for which the final dependency analyses, cyber-threat assessments, risk assessments and analyses are made (Aarne Hummelholm/2018).

Chapter 2 presents the ecosystems and collaborative environment formed by active nodes as well as an architecture model that describes the current operating environments of the hospital, the home, outside home,

telecommunication networks and hospital data center at the general level with their interfaces. The virtual environments management and control and telecommunication networks and data centers is part of this whole. Chapter 3 describes the cyber-threats against the future health care systems and the models which are used to make threat analysis to e-Health infrastructures and services. The chapter 4 deals with making and modelling of threat analyses and chapter 5 conclusions, our solution model and future work

3. Chapter 2: Description of the future operating environment

Even today, the situation the hospitals and healthcare centres are the key treatment points where the sick is being examined and cared for. In many situations, access to treatment takes time and frustrates patients or older people. This may be due to a shortage of healthcare personnel, but also long geographical distances may impede medical examinations or access to treatment. Long distances also increase costs and therefore it is not always possible to achieve the cost-effective solution associated with each treatment situation. People may have to travel to a care point only to check their situation, which could have been checked with digital systems without the need for entry. As a result, the development of digital methods of treatment with sensors and IoT devices is strongly developed in order 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 2.

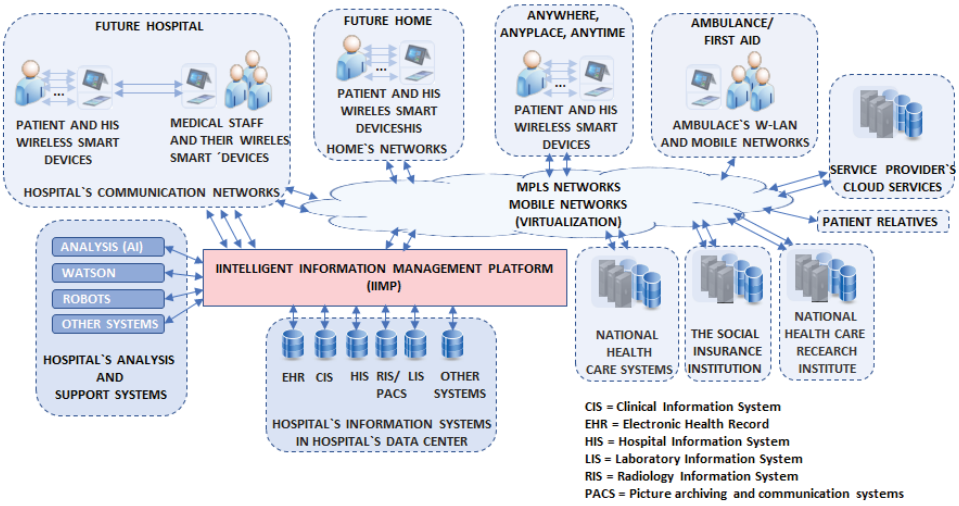

Figure 2; E-Health or m-health operating environment, top level architecture

In order to improve health care, new digital hospitals have been introduced which are more cost-effective than previous traditional hospitals and are geared towards better treatment accuracy and performance in treatment processes and are also more effective in diagnosing diseases. The Digital hospital environment utilizes the digital Hospital Patient Report Systems (EHR), which are the one main systems in this operation (figure 2). In the future hospital, the patient has several digital sensors and IoT devices attached to them to collect their health-related bio-signals, which are sent through the patient's smart device to the hospital Information systems for analysis and follow-up (figure 3).

The e-Health or m-Health system taxonomy can be described, describing the data streams and processes when the data is taken by the patient and they become a hospital medical information system where the data is analysed and draws conclusions (Robert S. H. Istepanian).

Patients e-Health or m-Health sensors and hospital healthcare systems taxonomy is composed of the following categories: Health and wellness monitoring, Diagnostic sensors, Prognostic and treatment sensors and Assistive sensors. Each of these categories have their own sub-categories. And these subcategories are further subdivided into sub-categories. Intelligent Data Management Platform (IIMP), (figure 2), types of systems are needed in order to monitor the flow of information from patient`s IoT devices and sensors to the hospital health care systems and it also gives possibilities to health care staff to analyse information fast. This also ensures that care staff can find information about patients for analysis in critical situations as well. This type of system can also help you find possible anomalies or changes of data, or if someone has attempted to penetrate or use the data in a way that is not desired.

The hospital has its own local network (LAN) and its own wireless network (W-LAN), through which medical records go to databases in the hospital's data center. The medical data in the hospital databases can be monitored by doctors and medical staff to make the necessary patient care decisions and management measures. The sensors and IoT devices belonging to the infrastucture`s automation systems can be also connected to the hospital's local area networks, as well as all the hospital's internal communications systems but this is risk.

This situation means that all clever IoT - devices, sensors and clever terminals would be in the same network systems and possibilities to connect to the hospital`s data center. From those, the hospital`s networks and hospital`s data center have also connections to the internet and to various external information systems such as National Health Care systems and National Social Insurance system (figure 2).

Communication between the patient's smart device and IoT devices and the sensors attached to them is done either through fixed wired connections or wireless connections, including different wireless technical solutions as Bluetooth in different versions, ZigBee, W-LAN, RFID and WiGig, (figure 3). These technologies allow for connection distances ranging from 1 metre to the 100 meters. When the hospital has a wide range of sensors and real estate automation systems that operate in the same frequency bands and when same frequency bands can also be used in hospital staff devices, the emergence of incidents is possible in the form of mutual interference. The new public buildings that are being built under the EU directive can also prevent the operation of wireless communications due to the large damping of the walls and windows of the building and the mobile networks are not working properly indoors (EU -2012/27/EU). In the patient`s home may be also lot of sensors and IoT devices, that uses same frequencies than patient`s smart device. The inside the patient's home may in this situation be also these frequency interferences.

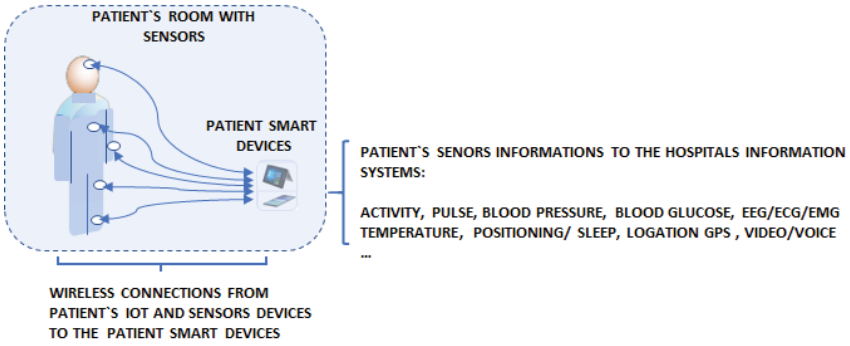

Figure 3: Patient`s IoT and sensor devices connections

One important factor in the hospital and in the treatment of patients in the digital environment, figure 2 and 3, is to ensure the proper functioning of communications. When we talk about the human spirit and related issues, it is also necessary to take into account, that digital devices do not operate without electricity.

Ensuring communication is very important when looking at the situation of the patient in rural areas where the supply of electricity may be completely cut-off for hours or even several days due to storms or snow disasters. In this situation, it is very important that the doctor receives information about the patient in one way or another. Doctors and/or medical staff should also be able to monitor the patient's condition at home in a real time situation, so that the necessary steps can be taken in time to guide the patient to necessary measures, (figure 4). Figure 4 shows the flow of patient information from his or her smart devices to the hospital system from which the medical staff receives the information and sends feedback to the patient's smart device. In this way, the exchange of information between the patient or the elderly and the care staff is carried out at a general level, whether in the patient's hospital, at home or outdoors on the town or anywhere. In table 1 we can see the bandwidth needs of the patient's sensors in the communications networks and at what transfer rate data is transferred via telecom networks. The table also shows the delay values that must be reached through communication connections. The values in the table 1 are those obtained from research results, but not yet the actual requirements or recommendations of our nursing systems.

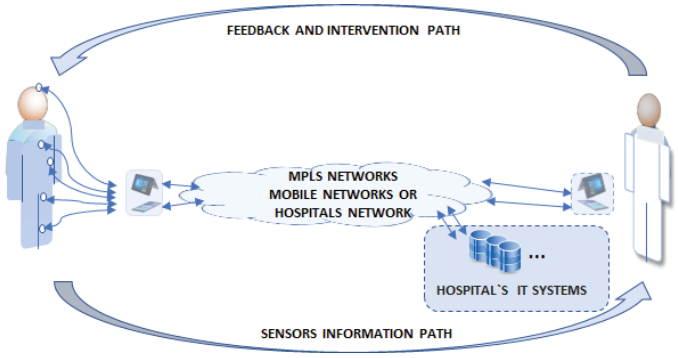

Figure 4: A general wireless and fixed m-health monitoring system

Table 1: Data rates and bandwidth of key biomedical wireless monitoring, (Robert S. H. Istepanian)

Physiological/Biomedical Parameter	Bandwidth	Rate Latency/Data
ECG (12 leads)	0.1 – 1 kHz	~144 Kbits/<200 ms
EEG (12 leads)	0.1 – 0.2 kHz	~40 Kbits/<300 ms
EMG	0 – 10 kHz	~350 Kbits/<200 ms
Body temperature	0 – 1 kHz	~0.1 kHz
Medical imaging and video streaming data	-	~ > 10 Mbps/<100 ms
Speech and voice	-	~50 – 100 Mbitps/<10 ms
Accelerometer and motion sensing	0 – 0.5 kHz	~30 Kbitps
Blood glucose monitoring	0 – 40 kHz	~1.5 Kbits
Blood pressure	0 – 1 kHz	~15 Hz

4. Chapter 3: Cyber Threats against the future health care systems

As seen in Figure 2, how does the future health care Information System form an extensive and complex package with a range of co-operation requirements and, above all, a highly critical condition for the wellbeing of the patient or the elderly environment. Many wireless technologies are used in the operating environment, and the operating systems do not form a closed set, which it would be possible to have as a separate island without connections to the outside world. In addition, the health registers include the personal data of all citizens and information about their illnesses. These systems are linked to external systems that allow people to send information to those systems. This in turn will raise hackers and cyber players' interest in penetrating one way or another into health systems, because from there is a chance to also have an economic benefit. Cyber attackers can also use system vulnerabilities to harm people who have been selected.

In general, the security threats in wireless health networks 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
- denial of service (DoS) 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 to 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

If attackers know patient location, attacker can follow patient route, where he or she is living, what route or bus or train he or she is using, which kind of car he or she use and so on. Attacker has possibilities to find vulnerabilities in his or her smart device or hospital equipment so, that he can attack against patient`s devices or trough those devices, against his or her car and maybe cause an accident and perhaps the patient dies as a result of the accident. After the accident, accident investigators think that the patient received a disease attack

and it occurred for this reason. This can happen especially to VIPs who are in prominent positions if someone wants to inflict damage on them

One of the attackers' goals could be to use these patient Smart Devices in order to get inside the systems from which we paid people grants (figure 5). These systems contain billions of euros in money. When cyber attacker attacking to health systems and hospital systems can it be quickly paralyse the entire society and make people desperate for their future, (Russell Brandon, Sky news, ABC news).

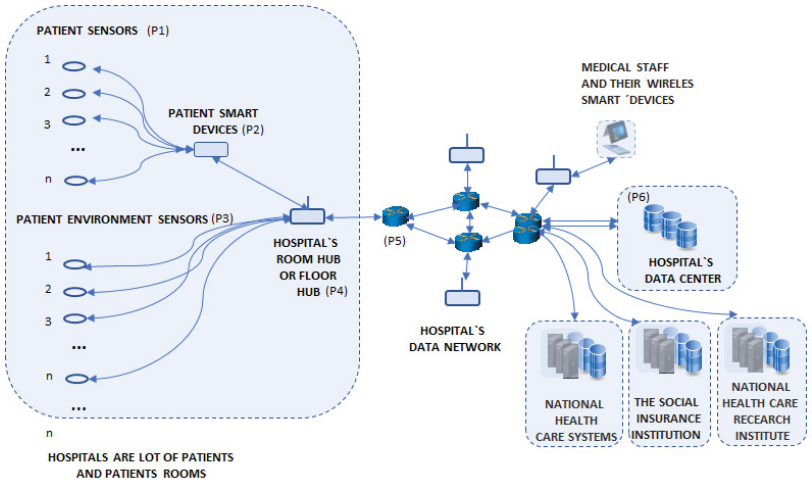

Figure 5: A general wireless and fixed m-health monitoring system with environment sensors in hospitals

5. Chapter 4: Making and modelling of threat analyses

When looking at figure 2, we see that health care systems are extremely complex and have interfaces in many directions to wireless networks or fixed networks. In addition, there are several service providers, admins and many stakeholders working on the same networks and information systems. The operating limits of the responsible actors must be able to define and instruct the functions so that interoperability is ensured between operators and those using the services. In order to be able to conduct cyber threat assessments and analyses, we must first work with architectural descriptions of the operating environments of the hospital, home, and outside home, with equipment and operating processes. In order to prevent or even reduce the risks described chapter 3, all parts of the health care systems should be segmented into their functional parts and a distinction should be made between them with enough safety mechanism which is a certain type gateway solution. These segments will then be examined also based on use cases. Then we must also look carefully attackers, their capabilities and motivations to disrupting health care systems and organisations, table 2.

Thereafter, data streams can be defined from the bio-signal produced by the patient's sensors to the servers. These data streams can be used to identify the devices and systems associated with each use case situation and to view related dependencies and vulnerabilities. Based on dependencies and vulnerabilities, risk analysis can be defined. These bases, it is possible to make an information and cyber threat, as well as to determine the probabilities of the cyber threats. The detected dependencies, risks, and vulnerabilities can be exported to a table where they are easily extracted for mathematical processing. Dependencies, risks and vulnerabilities can be given a number estimate of the probability of realisation that can be utilised in mathematical review. We can use attack tree models to count cyber threats probabilities. In addition, preliminary analyses of the tabular form can be used, which have already defined, based on sensitivity analysis, a preliminary assessment of each threat. Mathematical processing clarifies the whole and gives a better picture of the threats if they are mathematically presented. It is possible to compare the cases in parallel and to make decisions based on the results. That is worth doing both for the sake of victims and to see the effect of the measure of the test.

In Figure 2, e-Health or m-Health, we can look at the various use cases and, in these cases, to review the service chains, from which we can look for dependencies, risks, vulnerabilities and give them a probability value. These values are put in table 3 which can be used help to calculate the probabilities of each case. Examine the use case in which the patient is hospitalized, figure 5. Figure 5 shows that quite several IoT devices and sensors are connected to the patient's smart device and that the device is connected to a room or floor access point (HUB). The same base station is also connected to various heating, ventilation, air conditioning and cooling systems

(HVAC) systems, etc. Manipulation all these systems can allow an attacker to access and exploit sensitive data stored in hospitals data centers.

Table 2: Capabilities and motivations for disrupting health care systems and organisations, example (based on Aurore LE BRIS, Walid EL ASRI, 2016)

	Patient Health		**Patient / Hospital Records**		**National Health Care Systems**	
Adversaries / Attackers	Targeted (Specific Victims)	Untargeted (Not Specified)	Targeted (Specific Victims)	Untargeted (Not Specified)	Targeted (Specific Victims)	Untargeted (Not Specified)
Individuals / Small Group				Yes		
Political Group / Hacktivists			Yes			
Organized Crime	Yes		Yes	Yes	Yes	Yes
Terrorism / Terrorist org.	Yes	Yes		Yes	Yes	Yes
Cyber Attackers			Yes	Yes	Yes	Yes
Nations, States	Yes	Yes	Yes	Yes	Yes	Yes

Making a threat analysis of the whole future hospital system, or just of an entity comprising of service sectors as part of the future intelligent health care systems is a challenging task. Therefore, threat analysis is made based on Figure 5. The entirety consists of Access networks, in a patient room with IoT devices (P1 1…n), patient`s smart device (P2), room HUB with HVAC systems (P3), core networks (P4) and data centers networks (P5). The following threat analysis is made for the patient`s access network as shown Figure 5, as currently it is subject to major changes and because it involves large quantities of different sensors and IoT devices. The starting point for the analysis is a smartphone interface the IoT devices connected to that, and the connection of the smartphone to the patient`s room HUB system and then to the hospital core router. The core router may be virtualized, and it also includes some services in their hospitals` systems own slices. In addition, the HUB system may include firewall functions.

Table 3: Threat and risk table model

Ref ID	**Org**	**Functions**	**Category**	**Threat**	**Threat/ Risk**	**Existing Control**	**Threat /risk level**			**Accept /reduce**	**Recom-mented control**	**Residual Threat/ Risk**			**Check Point**
							L	C	R			L	C	R	
1 / AH	MC	Indentify	Access	Foot-printing	Target Access	IDS /IPS	3	3	8	Reduce	EU- dir.	2	2	3	xx

Where L = Likelihood, C = Consequence, R = Risk

Chapter 3 gives examples of attack mechanisms. How to make aggressive attacks and how attackers try to use vulnerabilities and other mechanisms to gain access to analyse systems and achieve their goals. By doing so the attackers have the possibility to compromise a target device. In these calculations values for these vulnerabilities are got from analysis. The events must be independent and if they are not, we must go to so small entities in order to reach an independent situation with respect to the various functions. The review can be further deepened by examining the vulnerabilities of different OSI layers and by also making analyses of these vulnerabilities.

For probabilistic analysis, defender need estimate the probability of attack success for each node in figure 5, in Attack-Defence Tree (ADT). For the purposes of the review, we define the used notations (Wang, P. (2014).

Table 4: Meaning of notations

Action	Examples	Notation
Attack	Sniffing, enumeration, scanning, …,	A
Detection	Port scan, information scan, …,	D
Countermeasure	Analysing of vulnerabilities and to repairing, safeguards put in place, …,	M

Attacks, probabilistic attack success (P(t))

$P1_{1\ldots n}$(t) = $p1_{A1\ldots n}$(t) (1 – $p_{D1\ldots n}$(t)), to n Patient`s IoT devices, (1)

$P2_1$(t) = $P1_1$(t)[($p2_{A2}$(t) (1 – $p2_{D2}$(t)], IoT device to Smart phone, (2)

$P2_{1\ldots n}$(t) = [($p2_1$(t)) + ($p2_2$(t)) + … + ($p2_n$(t))], because, different IoT devices will to connect to Smart Phone in different times, (3)

$P3_{s1\ \ldots n}$(t)= P_{3As1}(t) (1 – P_{3ds1}(t)), …, to room connected sensors 1 … n, (4)

$P4$(t) = p_{4A1}(t) (1 – p_{4D1}(t)) (1 – p_{4M}t), HUB (room) with attackers, defence and countermeasures (5)

$P4_s$(t) = [(p_{3S1}(t)) (p_{3s2}(t)) … (p_{3sn}(t))] [p_{4A}(t) (1 – p_{4D}(t)) (1 -p_{4M}(t)], room sensors are connected to HUB (room), (6)

$P5$(t) = p_{5A1}(t) (1 – 5_{4D1}(t)) (1 – p_{5M}t), router (hospital) with attackers, defence and countermeasures (7)

P_r(t) = [p_{5A1}(t) (1 – 5_{4D1}(t)) (1 – p_{5M}t)] ($P4_s$(t)) router (hospital) and HUB (room) connected (8)

$P6_{dc}(t) = P_{r1}$(t)P_{r2}(t) … P_{rn}(t) hospital`s data center router and all hospital router (hospital) connected together (9)

The results obtained are then exported to the Threat and Risk Table Model, table 3. The table contains the entities, the activity and category to be considered, the related threat/risk and the controls. Then the table shows the current probability, the resulting consequences and the current risk. In the future it is evaluated how the risk is addressed, what are the recommended controls and remedies with its responsible persons (including organizations). Finally, the equivalent values and checkpoints after remedies are estimated. The table can be done separately for the cyber threat and separately for the risks and furthermore add columns as needed depending on the issues being viewed and related contexts.

6. Conclusions, our solution model and future work

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. And 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.

We can say, that anything that is plugged in, whether it has a Wi-Fi connection or not, can be vulnerable to hacking, and lots of medical devices, such as pacemakers and ventilators, are connected to the internet for the benefit of the patients. Pacemakers can connect with a device at home that monitors the rhythms of the heart and are able to send that information to doctors.

Hospitals also have a wide range of support systems and different analytical systems, such as Watson or other analytics systems. In addition, hospitals are increasingly using robots, for example, to dispense medicines, etc. It is very important to protect these systems from external security breaches, data thefts, ransomware attacks, different security attacks, or even cyber-attacks against.

6.1 Solution model for smart devices

Because there are lot of security challenges in security solutions, privacy and cyber security issues in now days healthcare systems, new type of smart devices was tested, in which are new type of security solutions. In the

hospital patient room patient`s and care staff`s intelligent devices work together (D2D) and exchange information directly in real time without any other network. Smart devices can work together forming their network, to go outside, and come back again seamlessly. The device prototype works. It tested in the laboratory and on the field (Aarne Hummelholm/2013). The device security system prevents unauthorized persons accessing to the device and the data transmission and the services provided, regardless of whether the patient is traveling, at home or elsewhere outside the hospital, and so on. We must meet the requirements of what the EU-GDPR and EU-MDR directives say. IoT -devices and sensors with platforms in smart devices are not yet tested in security issues (Hanna-Leena Huttunen (2017, 2018)). Research project, Smart medical devices, will be launched soon and it takes into account also EU-GDPR, -MDR and -NIS issues.

6.2 Future work

Artificial intelligence (AI) use needs to be investigated and tested for its ability to protect e-Health's IoT devices, sensors and other health systems so that we can better protect these devices against these malicious software and cyber-attacks.

Because in health care devices are a lot of vulnerabilities and security challenges there, we need to find good architectures for healthcare equipment and systems, to give the requirements to them so that patients and the treatment staff can use them safely in this medical care environment (EU-GDPR/2016, EU-MDR/2017).

One research topic is to measure and test the frequency disturbances in the hospital and patient's home environment and check if there are any possible cases that affect the patient's treatment.
Energy efficiencies is very important research area to investigate it in the health care environment and the health care smart devices.

References

ABC News, Fears of hackers targeting US hospitals, medical devices for cyber-attacks, Jun 29, 2017.
Aurore LE BRIS, Walid EL ASRI, State of cybersecurity & cyber threats in healthcare organizations, Essec Business school, 2016.
Russell Brandom, UK hospitals hit with massive ransomware attack, May 12, 2017
EU- Energy Efficiency Directive, 2012/27.
EU-GDPR, The General Data Protection Regulation, 2016/679.
EU- MDR, The Medical Devices Regulation, 5/2017.
EU- NIS, Concerning measures for a high common level of security of network and information systems across the Union, 6/2016.
Ian Armas Foster, NIST's Security Reference Architecture for the Cloud-First Initiative, June 28, 2013
Aarne Hummelholm, Cyber threat analysis in Smart City environments, ECCWS2018, Oslo, 2018.
Aarne Hummelholm, Kari Innala, Patent N0.: US 8,606,320 B2, (45) INTELLIGENT BASE STATION, Date of Patent: Dec. 10/2013, PCT Filed: Oct. 21, 2005.
Huttunen, H. L., Halonen, R., & Koskimäki, H. (2017, September), Exploring use of wearable sensors to identify early symptoms of migraine attack.
Huttunen, H. L., & Halonen, R. (2018, September), Preferred Biosignals to Predict Migraine Attack.
Huttunen, H. L., & Halonen, R. (2018), Willingness to Use Smartphone Application Assistant to Support Migraine Treatment.
Robert S. H. Istepanian, Bryan Woodward, m-Health, Fundamentals and Applications, Wiley, 2017
ITU-T, Security in Telecommunications and Information Technology, September 2015
Samant Khajuria, Lene Sorensen, Knud Erik Skouby, Cybersecurity and Privacy Bridging Gap, River Publishers, 2017
Ramjee Prasad, 5G Outlook, Innovations and Applications, River Publishers, 2016
Wang, P. Liu, J.C. Threat Analysis of Cyber- attacks with Attack Tree +, 2014

disaster area scenarios and for rescue efforts. Thaddeus joined the University of Chester in 2015 to develop and deliver the University's new Cybersecurity programme and research.

Eric Filiol is the head of (C+V)O research lab at ESIEA, France and senior consultant in offensive cybersecurity and intelligence. He spent 22 years in the French Army (Infantry/Marine Corps). He holds an Engineer diploma in Cryptology, a PhD in applied mathematics and computer science and a Habilitation Thesis in Computer Science. He is graduated from NATO in InfoOps. He is the Editor-in-chief of the Journal in Computer Virology. He has been a speaker at international security events including Black Hat, CCC, CanSecWest, PacSec, Hack.lu, Brucon, H2HC…

Nathaniel Flack is pursuing a MS in Cyberspace Operations at the Air Force Institute of Technology in Ohio. He received his BS in Computer Engineering from Cedarville University in Cedarville, Ohio in 2012. His main research areas are cyber education, multi-domain operations, and serious games.

Noran Shafik Fouad is a doctoral researcher in international relations at the University of Sussex, and a recipient of the university's Chancellor International Research Scholarship. Her research examines the peculiarities of digital information and its implications on cybersecurity policy and theory, with a particular focus on the US as a case study.

Saïd Haddad, Ph.D in Political science (René Descartes University, Paris), is Senior lecturer in Sociology and member of the research team, Conflits in Mutation of the Saint-Cyr Research Center at the Saint-Cyr Military Academy, France. His current research focuses on the construction of cyber as a French national priority and the sociology of "cyber warriors".

Gerhard Henselmann, Dipl.-Ing. MBA, graduated Flighttest-Engineer was educated in Aerospace Engineering at Technical University of Munich/Germany and is working over 35 years in aerospace with expert experience in testing, flighttesting of airborne military platforms and has a wide experience in avionics, electronic warfare and self-defence of military platforms. He started his PhD studies in summer 2016 at the University of Jyväskylä on Cyber Security.

Aarne Hummelholm graduated from Helsinki University of Technology in 2000. Since then he has been involved in the design, development of architectures` of authorities` telecommunications networks and information systems. Key themes in his work have been critical service availability, cyber security and preparedness issues. In 2017 he started his doctoral dissertations at the University of Jyväskylä.

Gazmend Huskaj is a PhD candidate in Cyber Operations at the Swedish Defence University. He received his MSc in Information Security from Stockholm University in 2015 as a distinguished graduate. Previously, he was Director Intelligence in the Swedish Armed Forces focusing on cyber-related issues. He is also a ISACA Certified Information Security Manager (CISM).

Ion A. Iftimie is a Doctoral Candidate in Vienna, Austria. Previously, he served as the Deputy Chief for Information Operations at the United States Cyber Command. He graduated from top defense colleges in the United States, Germany, and Sweden, and is an alumnus of the Harvard Kennedy School Executive Program in Cybersecurity Policies.

Eduardo Arthur Izycki is a Student of Master in International Relations by the University of Brasília (UnB) and public servant. Eduardo Izycki worked on developing solutions for risk assessments in the cycle of major events in Brazil (2012-2016). He currently works in the Critical Infrastructure Protection Coordination of the Brazilian Institutional Security Office (GSI).

Margarita Jaitner is an analyst at the Swedish Defense Research Agency. She received her MSSc in Societal Risk Management from Karlstad University Sweden. She has authored several academic publications within the area of information warfare in cyberspace, hybrid warfare and other policy-related research within cyber security.

Dr. Victor Jaquire has been within the field of cyber and information security for over 20 years within Government and the Private sector focusing on strategy, performance management and operations. He holds