Ethics of Cybersecurity and Biomedical Ethics – Providing Ethical Guidelines for the SHAPES Project

Heikki Hämäläinen

2021 Laurea

Laurea University of Applied Sciences

Ethics of Cybersecurity and Biomedical Ethics – Providing Ethical Guidelines for the SHAPES Project

Heikki Hämäläinen
Innovative Digital Services of the Future
Master's Thesis
May 2021

Laurea University of Applied Sciences **Abstract**
Innovative Digital Services of the Future
Master of Business Administration

Heikki Hämäläinen

Ethics of Cybersecurity and Biomedical Ethics – Providing Ethical Guidelines for the SHAPES Project

Year 2021 Pages 45

The objective of this thesis was to provide ethical guidelines from a cybersecurity ethics and biomedical ethics perspective for the SHAPES project utilizing Hevner's Design Science Research theory. Another objective was to generate a conference paper to be used in the DIGILIENCE 2021 seminar. The focus was to understand what ethical similarities but also what conflicts might occur in an environment where many different stakeholders ranging from software developers to healthcare professionals interact with the end-user group, elderly people living at home.

The theoretical framework was built on known ethical frameworks of cybersecurity ethics and biomedical ethics, but also by determining and understanding the environment that these ethical frameworks apply to. The theoretical framework together with the environment description was applied to Hevner's Design Science Research model to get the desired output, which was the ethical guidelines for the SHAPES project.

The ethical guidelines were introduced to respond to ethical questions within four main themes covering privacy, autonomy, consent and beneficence where ethical decision-making is required. When comparing known ethical frameworks for both cybersecurity ethics and biomedical ethics, many similarities but also conflicts were found.

In conclusion, from the perspective of the SHAPES project, where questions concerning cybersecurity ethics and biomedical ethics are encountered daily in relation to the well-being of the elderly people, similar comparisons still need to be performed from other ethical viewpoints. A majority of the commonly known ethical theories strive for human well-being, justice, respecting human rights and maximizing good, but clear trade-offs are found when combining different theories and inserting them into a complex environment.

Keywords: cybersecurity ethics, biomedical ethics, SHAPES, design science

Laurea-ammattikorkeakoulu **Tiivistelmä**
Tulevaisuuden innovatiiviset digitaaliset palvelut
Tradenomi (Ylempi AMK)

Heikki Hämäläinen

Kyberturvallisuuden ja lääketieteen etiikka – Eettisen ohjeistuksen toteuttaminen SHAPES -hankkeelle

Vuosi 2021 Sivumäärä 45

Opinnäytetyön tavoitteena oli muodostaa eettiset ohjeistukset SHAPES-hankkeelle kyberturvallisuuden sekä lääketieteen tunnettuja teorioita hyödyntäen. Eettiset ohjeistukset toteutettiin Hevnerin Design Science Research -mallia hyödyntäen. Eettisten ohjeistusten lisäksi, osana tätä opinnäytetyötä valmisteltiin konferenssiraportti, joka esitetään DIGILIENCE 2021-seminaarissa. Opinnäytetyötä tehdessä keskityttiin eettisten kysymysten yhtäläisyyksien ja ristiriitojen havaitsemiseen monimuotoisessa ympäristössä. SHAPES-ympäristössä useat eri sidosryhmät ohjelmistokehittäjistä hoitohenkilökuntaan ovat vuorovaikutuksessa loppukäyttäjien, eli kotona asuvien vanhusten kanssa.

Tietopohja rakennettiin yleisesti tunnettujen sekä kyberturvallisuuden että lääketieteen eettisten viitekehysten mukaan. Toisena osana toimi ympäristön määrittely. Tietopohja sekä ympäristö yhdistettiin osaksi Hevnerin Design Science Research -mallia, jonka avulla pystyttiin tuottamaan haluttu lopputulos, eli eettinen ohjeistus SHAPES-hankkeelle.

Lopputuloksena esitellyn eettisen ohjeistuksen tarkoitus on auttaa vastaamaan eettisiin kysymyksiin koskien yksityisyyttä, itsehallintoa, suostumusta sekä hyvyyttä, joissa eettistä päätöksentekoa tarvitaan.

Johtopäätöksenä esitettiin, että SHAPES-hankkeen näkökulmasta, jossa kyberturvallisuuteen sekä lääketieteeseen liittyviä eettisiä kysymyksiä kohdataan päivittäin, lisätutkimusta tarvitaan muiden eettisten viitekehysten osalta. Suuri osa tunnetuista eettisistä viitekehyksistä tavoittelee henkilön hyvinvointia, oikeutta, ihmisoikeuksien kunnioittamista ja hyvän tavoittelua. Olemassa olevien erilaisten eettisten viitekehysten sijoittaminen monimuotoiseen ympäristöön aiheuttaa tilanteita, joissa ristiriitoja syntyy ja näin ollen kompromisseja joudutaan tekemään.

Asiasanat: kyberturvallisuuden etiikka, lääketieteellinen etiikka, SHAPES, suunnittelututkimus

Contents

1 Introduction

The population of almost all developed and developing countries are ageing whilst the lifespan is increasing, and the fertility rates are low. This change in the demographic age structure puts pressure on societies to provide new innovations and solutions to be able to maintain a working society. There is an increasing demand for new technologies, products and ways of working to support the change in the age structure.

The purpose of this study is to examine cybersecurity ethics and biomedical ethics and by using Hevner's Design Science process, provide ethical guidelines for SHAPES project. The objective is to provide ethical guidelines to be utilized by different stakeholders in the environment related to SHAPES project – developers, healthcare professionals, family members and elderly people living at home. The context and findings are also provided in format of a conference paper for the DIGILIENCE 2021 conference as an attachment to this study.

The method used in this study is Alan Hevner's Design Science Research. The Design Science Research method consist of three components; knowledge base, environment and design science. Knowledge base provides the theoretical background and environment defines the people, systems and organizations involved. The design science process introduces the artifact to the environment but also continuously gathers feedback and brings new inputs to the knowledge base or environment. This study is structured to follow this composition. The theoretical background in this study is formed by a literature overview covering cybersecurity ethics and biomedical ethics.

This study is part of SHAPES project. SHAPES (The Smart and Healthy Ageing through People Engaging in Supportive Systems) is a project funded by the European Union's 2020 research and innovation programme. The aim of this study is to introduce ethical guidelines for all different stakeholders in the SHAPES project from a cybersecurity ethics and biomedical ethics point of view. This is achieved by examining and presenting known ethical frameworks from both a cybersecurity and biomedical point of view. In a SHAPEs context, examining the relations and conflicts between these two ethical frameworks are of importance, especially as a study of this subject have not been commenced before.

2 Method: Design Research Science

When introducing ethical instructions from a cybersecurity and medical viewpoint for the SHAPES project, both theory of ethics of cybersecurity and medical ethics need to be taken into consideration. With the help of Hevner's Design Science Research it is possible to connect the environment, theoretical background and the actual designing process together.

2.1 Design Science Research and Hevner's Design Science Research Cycles

Hevner's Design Science Research theory considers the practical side of the design process but also reflects new outputs to prior known knowledge and theoretical background. One of Hevner's objectives is that, the design process itself would feed knowledge back to the knowledge base as an outcome of the process.

The background of Design Science Research or DSR is in information technology and information system science. The purpose of Design Science Research is to emphasize the designer's role as a creator of innovative artifacts, which are the outcome of the process itself. Design is both a process (set of activities) and a product (artifact) and supports a problem-solving model that continuously shifts perspective between these two for the same complex problem with the aim to provide a solution as an outcome. This way, the designer will contribute new knowledge to scientific evidence with the artifact created by the process. The evaluation of the artifact provides feedback in form of information and an even more deep understanding of the problem. This aims to improve both the quality of the product and the design process itself. (Hevner & Chatterjee, 2010, 78.)

Design science is a paradigm based on practical problem solving and artifacts are built to solve these problems. The outcome aims to provide an artifact which then must be evaluated. The designing process itself must be evaluated by not only theoretical means but also in the real world with real use cases. The evaluation process can consist of formal mathematical algorithms, textual descriptions of "best practice" approaches or a combination of these. They demonstrate the feasibility by enabling concrete assessment of an artifact and its suitability to its intended purpose. The evaluation process also provides researchers the ability to learn how the artifact affects in the real world and how users adopt it. (Hevner & Chatterjee, 2010, 78-79.)

Information systems are often implemented in organizations to ensure efficiency in the processes of the organization. Also, people, culture and working habits impacts the process itself and how the purpose is achieved. Design Science Research aims to find solutions that make these organizational processes more efficient. (Hevner & Chatterjee, 2010, 82-83.)

Hevner introduces the Design Research Science Cycles as a part of the Design Science Research. These cycles are relevant when positioning design projects from a wider context as shown in Figure 1. The cycles bring feedback constantly back to the design process which ensures introducing new artifacts to the environment on a continuous basis. With the help of these three cycles the process can constantly evolve and bring in new content to the environment and knowledge base to be then again input back to the actual design science process. (Hevner & Chatterjee, 2010, 78-80.)

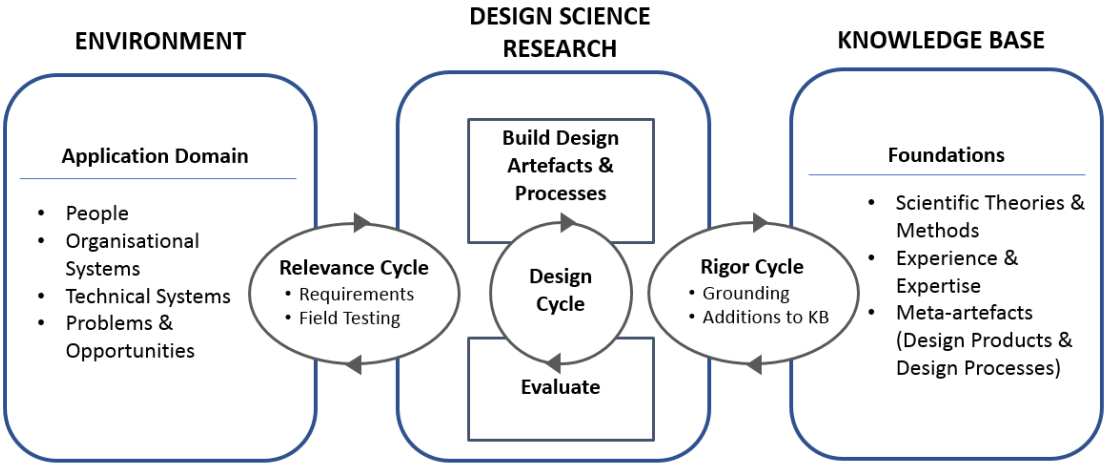

Figure 1. Hevner's Design Science Research Cycles

The knowledge base consists of foundational theories, frameworks, instruments, constructs, models, methods and instantiations which are used to develop phase for the research study. These are utilized to provide guidelines to the justification and evaluation process of the outcomes. A design process uses commonly known mathematical methods for evaluation of the artifact, but also empirical methods might be utilized. (Hevner & Chatterjee, 2010, 79-80.)

The environment describes the problem space in which the case of interest resides. For Information System research it consists of people, organizations and technology that is used. The environment defines the goals, tasks, problems and opportunities for the design process itself. (Hevner & Chatterjee, 2010, 79.)

Lastly, Design science research connects the knowledge base and the environment to the design science research process with help of Hevner's Design Science Research Cycles. This part of the model helps the continuous gathering of feedback and development of the artifacts, but also by evaluating them. (Hevner & Chatterjee, 2010, 79.)

Interacting between the environment and the design science research process, the relevance cycle provides context to the research process but also sets criteria for approval of the research results introduced. It also evaluates the research results in correspondence to the environment. (Hevner & Chatterjee, 2010, 78-80.)

On the other side of the cycles, where the knowledge base interacts with the design science research process, the rigor cycle introduces theoretical background and knowledge into the designing process. When a design process is introduced by researchers, they need to ensure that the already known theories are taken into consideration. This is to ensure that designed outputs are research contributions and not only designs based on known design artifacts or processes. (Hevner & Chatterjee, 2010, 78-80.)

The design cycle in the middle is used to continuously iterate the input from the other two cycles, the relevance cycle and the rigor cycle and feed this into the design process of building designs and evaluating them. Even if the design cycle brings information to the process from the other two cycles, it is not dependent of them but seen as an individual cycle in the process. (Hevner & Chatterjee, 2010, 79-81.)

In Information Systems research the artifacts are divided into four categories which are constructs (vocabulary and symbols), models (abstractions and representations), methods (algorithms and practices), instantiations (implemented and prototyped systems). These enable IT researchers to understand, develop and implement information systems within organizations. (Hevner & Chatterjee, 2010, 77.)

Creating an artifact for the SHAPES project in form of ethical instructions as a part of this study would be considered as a method in the SHAPES ecosystem (instantiation) for the ageing and other relevant stakeholders such as family and medical professionals.

2.2 Design research theory and Cybersecurity ethics in SHAPES

In this study Hevner's Design Science Research is used as a methodological background in order to introduce ethical instructions for all relevant stakeholders. The aim for this study is to design ethical instructions for further use in developing the SHAPES ecosystem when overseeing matters related to cybersecurity and medical activities from an ethical point of view.

The SHAPES ecosystem is an solution that collects and analyses data (also personal data) and information from various sources, such as cooperation partners and end-users, and utilizes this data to provide healthcare related solutions and assistance to elderly people living at

home. Therefore, ethical instructions based on ethics of cybersecurity and medical ethics can be considered as a relevant scope of interest for many stakeholders in the SHAPES ecosystem.

This study is structured in three parts. First, the knowledge base is covered with relevant theoretical background. The knowledge base is followed by a description of the environment from the perspective of the SHAPES project. Last, the Design Science artifact is to be introduced based on input from the knowledge base, environment and enhanced by the three different Design Science Research Cycles as shown in Figure 2.

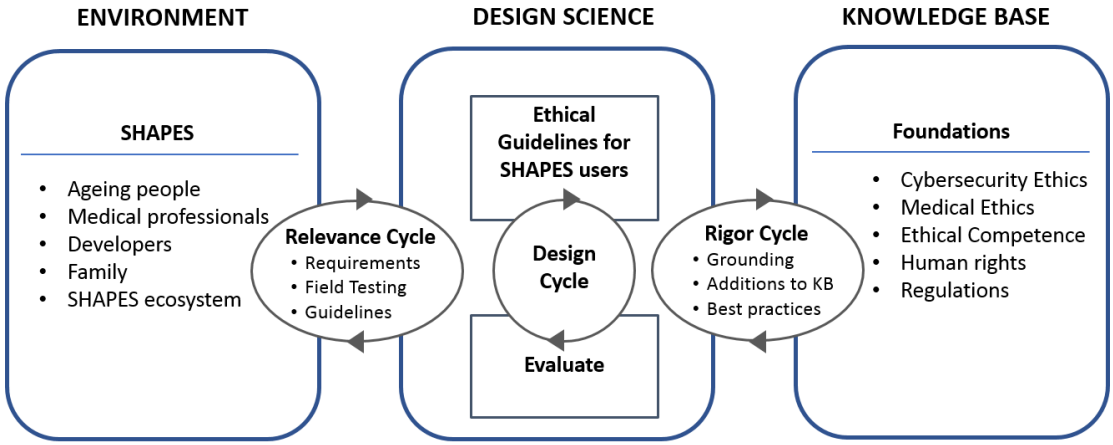

Figure 2. Hevner's Design Science Research Cycles in SHAPES environment

3 Knowledge base

3.1 Biomedical ethics

In medical ethics, often four main principles are introduced for medical procedures commenced by healthcare professionals. Principles does not provide a strict guideline for actions, but rather an ethical framework to conduct right decisions in various situations. All these principles pay a key role in ensuring optimal outcomes in patient safety and care. The four main principles are autonomy, beneficence, non-maleficence and justice. The four main principles serve a paradigm to answer moral questions in biomedical research and healthcare related matters. (Beauchamp & Childress, 2009, VIII.)

3.1.1 Respect for Autonomy

The word “autonomy” originates from the Greek words autos (“self”) and nomos (“rule”). Autonomy in a biomedical ethic setting refers to respecting the decision-making capacities in healthcare of individuals. Decision-making in such a setting especially includes informed consent and refusal, usually related to an operation handled by a healthcare professional. Personal autonomy in biomedical ethics is at least a self-rule that is free of limitations from controlling interference by others or from limitations, such as insufficient understanding that would prevent a meaningful choice of the patient. (Beauchamp & Childress, 2009, 57-58.)

Even autonomous individuals sometimes fail to make meaningful choices due to temporary limitations caused by ignorance, illness or other conditions that might restrict their options. In such cases informed consent is important. Informed consent includes three different components, threshold elements (competence and voluntariness), information elements (recommendation, understanding and disclosure) and consent elements (decision and authorization). (Sarlio-Siintola, 2020.)

3.1.2 Non-maleficence

Non-maleficence is the principle which asserts an obligation not to do harm to others. Healthcare professionals often invoke the maxim: “I will use treatment to help the sick according to my ability and judgment, but I will never use it to injure or wrong them”. Many ethical theories recognize non-maleficence and it is often combined with the beneficence principle which is covered in the next chapter. (Beauchamp & Childress, 2009, 113.)

The principle of non-maleficence can be seen quite broadly and it supports many other more specific moral rules, such as “do not kill” and “do not cause pain or suffering”. Non-maleficence includes not only the obligation to not harm others directly, but also not imposing risks of harm. It is often combined as a single principle together with beneficence. (Beauchamp & Childress, 2009, 114-116.)

3.1.3 Beneficence

Morality entails not only that we treat other individuals with respect for autonomy and non-maleficence, but also to contribute towards their welfare and wellbeing. Even if beneficence and non-maleficence are somewhat morally overlapping, the principles of beneficence usually require more because the agents are required to take action to help others, not only avoid causing harm. Beneficence includes all kind of actions, where the intention is to help others. (Beauchamp & Childress, 2009, 165.)

Beneficence aims to contribute towards persons' welfare and the principle is divided into chapters, positive beneficence and utility. Positive beneficence refers to the agent contributing actions towards brining benefit to the individual. Utility is seen as a balance between drawbacks and benefits and the aim is to provide the best possible overall result which can be compared to the utilitarian approach. (Beauchamp & Childress, 2009, 165-166.)

3.1.4 Justice

Justice is seen as a group of norms that aims to for distributing benefits, risks and costs fairly and in a balanced way. Justice from a healthcare point of view can answer questions like "should all individuals despite of age or location have the same access to healthcare services?". Many principles of justice in a biomedical ethics setting are not distinct and independent of other principles, such as beneficence and non-maleficence. (Beauchamp & Childress, 2009, 225-226.)

Other ethical frameworks and theories such as utilitarianism, libertarianism, and communitarianism offer tools for theoretical thinking about making decisions that make justice for individuals. Even if these frameworks impact each other, none of them are necessary within health policy and allocation decisions. (Sarlio-Siintola, 2020.)

3.2 Cybersecurity

The constant increase in usage of information processing and communication technologies supports a more efficient way of operating in our modern society and increases interaction in our operating environment. However, this is also leading to the technologies being used and the ecosystems built around them becoming increasingly vulnerable to threats. No information technology system or technology is ever completely secure or independent from external threats. Cybersecurity and its ethics play an important role when launching new technologies, but also an important issue retrospectively for existing systems and databases. More complex ecosystems are built using information systems and will need to be carefully designed and have established guidelines that focus on cybersecurity to ensure a safe launch of such systems. (Christen, Gordijin & Loi, 2020, 1-2.)

The modern society can be called "the information society" because of the big role played by intangible assets such as knowledge-based economies and information-intensive services. This has led to a situation where information and cybersecurity ethics mean different things to researchers and professional in different disciplines, including business ethics, medical ethics and the philosophy of information to name a few. (Himma & Tavani, 2008, 3-5.)

Overemphasizing cybersecurity can also contribute to violating fundamental values such as equality, fairness, freedom or privacy. On the other hand, neglecting cyber security can undermine public trust in the digital infrastructure, policy makers and state authorities. One of the key functions of cybersecurity is to support individual values such as privacy and trust. In some cases, however, leveraging cybersecurity works against these values. As a result, cybersecurity intersects between two worlds of values, in some cases as a supportive function, but also as a source of conflict. (Christen, Gordijin & Loi, 2020, 1-2.)

In most cases, cybersecurity ensures that personal information is kept secure, but in certain situations it may also expose this personal information to cybersecurity professionals. These cases may include, for example, situations where a cybersecurity expert must look at databases and systems containing personal information to identify potential malicious activity or security attacks. (Christen, Gordijin & Loi, 2020, 1-2.)

Cybersecurity is yet an underdeveloped topic in technology ethics and is often discussed as a tool to protect privacy. Cybersecurity raises a excess of ethical issues such as weighting data access and data privacy in sensitive health data to name a few. For example, in medical operations where implants are installed in the patient, the implant producer may want to protect the data transfer between the implant and the receiver server with cryptology. Using of this cryptology increases the battery consumption of the implant and requires medical surgeries for battery exchange. (Christen, Gordijin & Loi, 2020, 1-2.)

3.2.1 Core Values in cybersecurity

Values are understood as dimensions which can be used to evaluate the goodness of a certain activity. Different values correspond to different varieties of goodness and to different morally problematic discussions. A value cluster in this context is established to gather different values into a cluster to be discerned in relation to cybersecurity. (van de Poel, 2020, 45-46.)

In cybersecurity, security versus privacy is the most common moral dilemma and usually mixed with each other. The moral dilemma occurs when we want to maintain good security of ICT systems by monitoring traffic and activity – and hence give up privacy data - of these systems. Privacy and security are not always in conflict but sometimes these to values might be mutually reinforced. It depends on the context whether privacy and security are supportive or conflicting. (van de Poel, 2020, 45-46.)

Van de Poel (2020) introduces four important value clusters for cybersecurity. The first one is “security” which includes more specific values such as individual and national security but

also information security. These values can conflict with each other on occasion, but they serve the same purpose of protecting something valuable from external threats (van de Poel, 2020, 47-51).

The second value cluster is “privacy”. This cluster includes values such as identity, anonymity, confidentiality, personhood and an act of self-care. Cybersecurity connects to these values in informational privacy. Informational privacy refers to concerns about what information about a person is known to or shared with others. The control conception of privacy - collecting, storing and sharing of personal data – is not always problematic. The issue lies within giving or not giving citizens control over the collected data. This issue is usually covered by utilizing “informed consent”, meaning providing information about data collection, storing and sharing to the data subject. (van de Poel, 2020, 52-55.)

The third cluster is “fairness” and consists of values such as justice, quality, non-discrimination, freedom, democracy and civil liberties. Cybersecurity measures typically might come with unequal benefits and costs for the target group and might lead morally unfair situations whereas democratic and civil rights should be sustained. (van de Poel, 2020, 55-58.)

The fourth cluster is “accountability”. Van de Poel (2020) introduces such values as openness, explainability and transparency in this cluster. This value cluster is relevant to cybersecurity when, for example, governments or companies are held accountable for cybersecurity measures they have taken even if there is not a suspicion of undue harm. In such situations the accountability is based on power imbalances where a government might have more excessive access to large data sets or big data than the counterparty. (van de Poel, 2020, 58.)

3.3 Ethical Frameworks for Cybersecurity

The word cybersecurity itself conveys the most important ethical goal, being safe from dangers in the cyberspace. The word security is often not seen as an ethical value of its own, but rather an instrumental value to protect ethical values. The same applies to cybersecurity which is often seen as a set of technologies and policies to protect from cybercrime such as data theft. (Christen & Loi, 2020, 74.)

Cybersecurity ethics is an multisectoral practice incorporating inputs from different fields of study such as medical ethics, military ethics, legal ethics and media ethics. Therefore, cybersecurity ethics can be seen as professional ethics, providing in-depth and specific knowledge to a group of practitioners who share certain characteristics. (Manjikian, 2018, 39-40.)

Cybersecurity professionals should consider ethics as a part of their profession, not only to avoid harm, prevent illegal activity or destructive behaviour but one who understands the ethical significance of their profession. An ethical cybersecurity professional not only uses their skills to build a better product or service, but something that strives towards a better world. (Manjikian, 2018, 326.)

3.3.1 Principlism

Principlism is a set of principles – usually three to four - combined and seen as a system of ethics. From a moral perspective, we always have good reasons to respect other humans, to pursue for the good of others, to act justly and avoid harming other people. The principlist approach is a simple and modest approach to ethics, which on the other hand can leave the researchers and cybersecurity operatives with a difficult task of weighting these principles against each other when trade-offs occur. (Christen & Loi, 2020, 75-76.)

From a cybersecurity perspective, the respect principle should be observed in all cases in which data may relate to identifiable personal data, for example in communication between persons and ID addresses. Respect also involves all research done where a consent is requested from a person in some experimental research on human factors in cybersecurity. (Christen & Loi, 2020, 75-76.)

The benefit principle (to pursue for the good of others) applies generally to cybersecurity research, meaning it should maximize benefit and minimize harm. When minimizing harm, one need to consider a broad set of risks for persons, including emotional, reputational, financial and physical harm. (Christen & Loi, 2020, 75-76.)

The justice principle is aiming for distributing an equal amount of benefit for all stakeholders. Justice in research implies that a research should be designed in a way that a group of people benefit more from the research than others. (Christen & Loi, 2020, 75-76.)

3.3.2 Human Rights

Looking at human rights from a cybersecurity perspective, a balance is often used to review the trade-offs between the extent to which human rights can be respected and security achieved. Trade-offs implies that priorities need to be set. Giving priorities to different types of threats needs to be considered, for example protecting the security of personal information or preventing attacks with criminal objectives. (Christen & Loi, 2020, 77.)

Protecting the security for personal information can be seen both as a duty of cybersecurity but also as a duty of human rights. Cybersecurity can also be a threat for human rights, for

example when colleting personal data for authentication purposes. Also, cases where the goal is to enhance cybersecurity by monitoring traffic and possible cyber-attacks might violate directly with human rights. Cybersecurity might therefore conflict with human rights in some cases, and balancing between trade-offs and benefits are is needed. The core of human rights should not be compromised to achieve a small gain in cybersecurity, but other methods should be explored, even if they are highly less efficient. (Christen & Loi, 2020, 78.)

3.3.3 Utilitarianism

Utilitarianism allows for the possibility of situational ethics meaning that in some circumstances one might need to violate a society's or an individual moral code if the outcome is better for a greater amount of individuals. Utilitarianism always aims for the decision with the highest benefit or the highest utility. (Manjikian, 2018, 88-89.)

From a cybersecurity perspective the utilitarian approach can be hard to define. One might encounter the debate whether individuals should be threated on base of different norms and morals in the cybersecurity space than in normal life. Also, it should be defined if "good" in normal life equals the same in a cybersecurity ethics perspective. Doing good should always exceed doing bad, and from a utilitarian cybersecurity ethics perspective the goods could be for example ability, knowledge, freedom, resources, security and opportunities. On the negative side would be for example death, pain or disability. Maximizing the goods should also be looked at from a longer time perspective to avoid unwanted outcomes long-term. (Manjikian, 2018, 90-91.)

3.3.4 Deontological Ethics

Deontological ethics defines certain individual behaviour characteristics as moral obligations or duties with which humans should treat each other. The deontological approach means that the individual commencing the moral or ethical decision does not always need to be happy with the result of the decision or even it might not lead to the best possible solution, but it is the right thing to do at the moment. (Manjikian, 2018, 75.)

Deontological ethics suggest that ethical questions can be solved by always acting on the principle which can be universally binding and beneficial for all individuals in that current situation. Everyone should define and agree on a same set of universal standards. Deontological ethics also has the approach of "reversibility", which means one should be able to ask the question "Would I be harmed if someone made the similar decision and took action towards me – how might I get harmed?". Treat the counterparty as you would like yourself to be treated, with respect and dignity. (Manjikian, 2018, 75-76.)

From a cybersecurity perspective deontological ethics with a reversibility approach is a good starting point. When healthcare professionals are dealing with sensitive personal data of individuals, it is good to think how you would feel if a person outside your personal life had a look on this data. Cyberspace and cybersecurity are not seen as any different from the real world and both worlds should be treated in the same way, for example the duty not to lie or practice deception should be equal in both worlds. (Manjikian, 2018, 85-86.)

Deontological ethics in cybersecurity with the involvement of robotics is where it becomes tricky. Machines are not able to reflect the decision to their own being. Therefore, machines are most probably been taught maximize the outcome with utilitarian ethics. (Manjikian, 2018, 87.)

3.3.5 Cybersecurity regulation in the European Union

The European Union (EU) published the first Cybersecurity Strategy in 2013, which did rise cybersecurity as new policy area in the EU. From EU's perspective cybersecurity can be defined as a combination of cyber resilience, cybercrime, cyber defence, cybersecurity and global cyberspace issues. The aim for introducing these 5 priority areas was to make EU's online environment the safest in the world. (Christen & Loi, 2020, 99-100.)

From a user perspective, digital life can only work good enough where there is a trust towards the cybersecurity of digital services and IT infrastructure. The importance of testing, validating and auditing increases and these a supported by various security certification schemes and legal support. (European Commission, 2021.)

The human interaction with software and services is often the weak factor in cybersecurity. The EU focuses on raising awareness of cybersecurity and promoting best practices among the general public. Building sustainable and secure environments requires special knowledge from different professionals and professions. Currently, there are not enough professionals available for this purpose. Therefore, EU has launched a training program to train cybersecurity professionals and cybersecurity skills has become one part of the general digital skills agenda. (European Commission, 2021.)

3.3.6 Cybersecurity in Healthcare

Cybersecurity has become increasingly important considering healthcare data in the current world. Not only does it cost money to prevent and heal from data breaches, but the rapid growth of cybercrime in the healthcare industry makes it a hard equation. To prevent cybersecurity threats, following practices should be noted and implemented. (UIC, 2020.)

1. Trainings to ensure that every member of the organization or healthcare provider is responsible for protecting patient data
2. Planning for unexpected cybersecurity threats by backing up and storing patient data securely
3. Controlling the access to protected data to cover only those professionals who need to access this data to make the patient the best benefit

From an ethical perspective, healthcare professional should have an ethical guideline in place where they are forced to report suspicious activity regarding possible cybersecurity threats when interacting with patient data. The utilitarian ethical framework would also suggest to healthcare professional to educate the patients to handle their personal data with caution for and greater outcome. (UIC, 2020.)

4 Environment

4.1 People

4.1.1 Ageing citizens

The population of almost all developed and developing countries are ageing whilst the lifespan is increasing. Also, in Europe, the current fertility rates are low, which will eventually lead into decreasing amount of younger people. This change in the demographic age structure puts pressure on Europe – together with the rest of the world – to provide new innovations and solutions to be able to maintain a working society. Currently, Europe has four working citizens per one elderly citizen. By 2050, the corresponding number of working citizens has decreased to two per elderly citizen. This brings up challenges, but also opportunities for new innovations, products, technologies and ways of working to support the change in the age structure. (Cabrera & Malanowski, 2009, 1-2.)

Alan Walker (2009) states that in the so-called “golden age” after the World War II, a close relationship between the society and the ageing citizens was formed. The relation between the elderly citizens and the society brought up both positive and negative outcomes, the positive ones being increase in living standards and the negative outcomes being contribution towards a view that provided stereotypes of old age as a period of both frailty and poverty. The ageing people was seen as passive receivers of pensions, welfare and main consumers of healthcare. This led to exclusion from political and societal channels as elderly people was not seen as a part of the economic system. (Walker, 2009, 36-37.)

In the beginning of the 1990s ageing became a European policy issue when the European Commission started to study the impact of national policies affecting ageing people. This study led closer focus on active ageing and increased the importance of ageing people by decreasing social exclusion. Active ageing has since been promoted by the European Union and led to establishing a preventative strategy of age management. The aim of such preventative strategy is to create a more sustainable pension system while the demographic age structure changes rapidly. (Walker, 2009, 39-41.)

ICT solutions play an important part in achieving set goals in the strategy. ICT solutions could bring more opportunities for ageing people to participate in the economical and societal life and promote self-expression and fellowship for the ageing people towards the society. Ultimately, the outcome would be an increase in quality of life, security, autonomy and participation towards the society. ICT would enable ageing people to do this from their home. (Walker, 2009, 41-43.)

While the European Union's view on ageing people through the active ageing strategy as contributors to the economy and productivity, Walker (2009) introduces arguments that should be considered. A strong approach on increasing productivity through the active ageing strategy might establish a top-down policy rather than promoting the elderly citizens in developing their own activities to contribute towards the strategy. A top-down policy might also contribute towards a narrow view on ageing citizens being only contributors towards a small part of life rather than promoting a life-long process for all age groups. Lastly, EU's active ageing strategy should not only focus on the younger old citizens but also the older elderly, which is an age group with its special demands. Different cultural backgrounds should also be considered. (Walker, 2009, 45-47.)

For example, in Finland, by 2030 it will be beyond the capacity the national economy to provide fully serviced old people's homes in line with our traditional elderly care mode. This will lead to a situation where Finland – and other nations as well - need to find ways to offer effective online and home-based healthcare and other services for old people living at home. (Minstery for Foreign Affairs, 2021.)

4.1.2 Ageing citizens and technology

Technology and new innovations often tend to be accessible and adopted by the younger generation. The constantly and rapidly changing environment does not support the elderly citizens to adopt to these technologies fast enough. Often the requirements for embracing an innovation outpaces the adopting capabilities in the elderly citizens. This might be due to the lack of training material available, but also usually new technologies require the users to

have adopted latest technological hardware to be able take advantage of the innovation. Elderly people are not early adopters within new technological devices and hardware. New innovation should take into consideration already existing technologies and capabilities which are already adopted by the elderly. This could help in delivering and engaging elderly citizen users.

The European Union sees great opportunities in technology for the ageing population. EU estimates that introduction of ICT and telemedicine alone will improve efficiency in healthcare services by 20 percent. To be able to achieve this, universal design meaning ease of use services and technologies are crucial. (Barland & Lovett, 2015, 7.)

Kaakinen & Törmä (1999) introduces gerontechnology as a possible supportive solution for ageing people. Gerontechnology highly advices researchers to build a knowledge base about ageing people and their behaviour in order to understand and provide solutions for the elderly that supports their daily life when getting older. Gerontechnology defines five ways of promoting technological development to support the elderly citizens.

Firstly, gerontechnolgy supports the ageing people in the ageing process itself by providing support for preventing accidents such as falling. Secondly, such technological solutions should be introduced which takes into consideration individual strengths and capabilities. Thirdly, gerontechnolgy should compensate the human senses and abilities which are weakening as people get older. Fourthly, technology should not only be provided for the elderly but also for the healthcare professionals taking care of the elderly. Lastly, gerontechnolgy is seen as a great support for research done related to elderly citizens. (Kaakinen & Törmä, 1999, 6-8.)

When considering the two different elderly age groups, the old elderly and the older elderly, new technological innovations and services should note the difference between these two. The capabilities and background in using latest technologies might vary between these two user groups. On might presume that the current workforce who will need services in the future are well known to current technologies and adopting new innovations, but the old elderly might not be that adoptive.

Providing a secure environment and improvement of the overall life of the ageing should be taken into consideration when implementing new technologies. Providing new technological capabilities for the elderly citizens brings the users to a new interaction with the society, behaving as a social network. Both the elderly citizens and healthcare professionals should be taken into account when developing such services. Setting targets for innovative technologies should be considered as a process to make the work of the healthcare professionals easier by providing an efficient way of facilitating nursing processes. (Viirkorpi, 2017, 45-48.)

4.1.3 Health Care professionals

The National Institute of Health and Care Excellence in the United Kingdom have classified digital health technologies by function. Functions include system services – such as electronic prescribing systems, wearable devices to monitor health and active monitoring apps that link with sensors. These functions aim to permit health care professionals to monitor patients remotely and providing help for diagnostic decisions based on provided data and sophisticated artificial intelligence solutions. (Scott et al, 2020, 2-3.)

In the SHAPES environment the target user group is not only the elderly people living at home, but also health care professionals who are responsible for providing care to the elderly. The SHAPES ecosystem provides these health care professionals with data of the elderly people, but decisions for action or medical treatment must still be commenced by a human. Providing health care professionals with data about their patients is key in providing tailored treatment for each patient. Health care professionals must utilize this data in an ethical way, both from a cybersecurity but also from a medical ethics point of view in order to provide the best possible treatment.

Technology and new innovative solutions will have an impact on how health care professionals work. Computerized decision support systems (CDSSs) have been utilized already for a long time to support the work done by these professionals. CDSSs provides algorithmic approaches to decision-making based on decision trees and rule-based expert systems. (Mantas & Hasman, 2013, 3.)

Assisted living technologies and health-enabling technologies supports problem-solving in geriatric medicine like fall risk identification. Also, in regards of remotely provided health services, in a Whole System Demonstrator study covering patients with underlying diseases like diabetes and heart failure, it was shown that the 12 months mortality rate was lower for people receiving remote healthcare services. (Mantas & Hasman, 2013, 8.)

4.2 Technology

4.2.1 SHAPES ecosystem

Living and operating in a familiar environment is considered a good way for elderly citizens to live as it contributes to well-being, equality and autonomy. To support this mindset, nations need to provide with sufficient support for the elderly to promote this autonomy in life with help of personal assistance services, health care services but also easy-to-adopt technical tools and assets to support the everyday life of the elderly. According to THL (2021), the person’s thoughts and wishes should be taken into consideration when designing such

services. When a service portfolio is customized to meet the client's wishes, they are not only pleasant for the elderly, but also the quality increases and they are efficient to produce.

The SHAPES Innovation Action (IA) aims to build, pilot and deploy a large-scale, EU-standardized open platform. Enabling and adopting a broad range of technological, organizational, clinical, educational and societal solutions aims to provide the elderly citizens tools and prerequisites to live an independent and meaningful life at home. SHAPES aim to provide an ecosystem for providing solutions, but also to gather and analyse information and data in order to develop the ecosystem and provided the ecosystem further. (SHAPES, 2020.)

One of the key goals of SHAPES is to build a European ecosystem that is attractive to health care industry and policy-makers and constructs a market for deployment of innovative digital health care solutions and services supporting and extending healthy and independent living of the aging population in Europe. (SHAPES, 2020.)

Currently, there are 36 partners from 14 different countries and the project funding started in 2019 and will last throughout a period of 48 months until 31st of October 2023. The SHAPES project introduces a methodology emphasizing co-creation between social sciences, technological development and deployment activities. All new innovations within the ecosystem should drive towards fulfilling user needs and requirements. SHAPES also adopt an ethics-based approach taking the protection of the human rights of the aging population as central focus point. (SHAPES, 2020.)

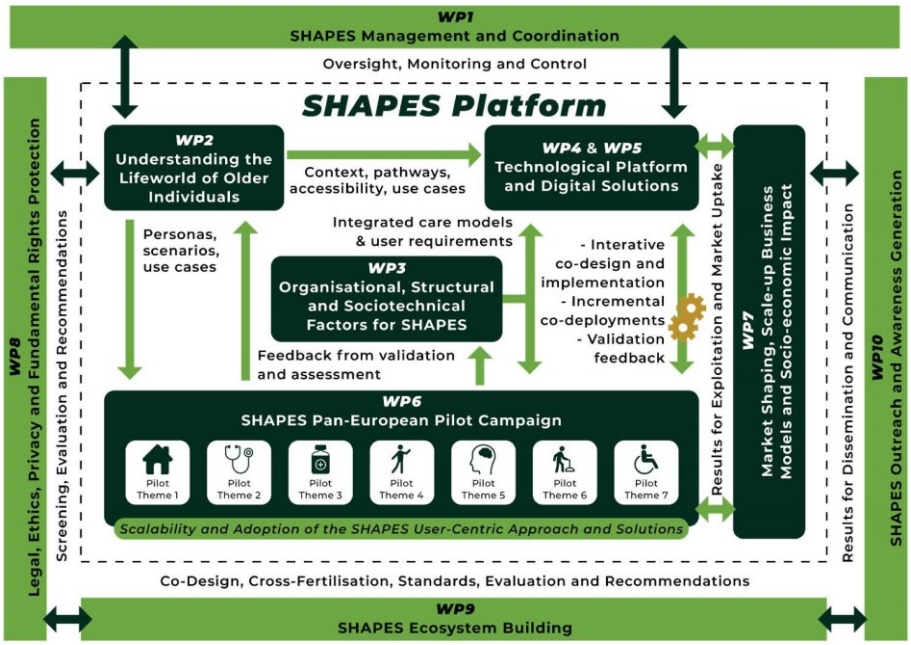

Figure 3. SHAPES structure (SHAPES 2020)

5 Design Science

5.1 The Design Process

The aim of this study was to form and create cybersecurity and medical ethical guidelines for the SHAPES project. I utilized Hevner's Design Science Research model in this study to formulate and provide ethical guidelines for both developers and users of the SHAPES ecosystem. Both cybersecurity ethics and medical ethics play a key role in the SHAPES project because of sensitive personal health data are utilized and accessed by several different counterparties such as developers, healthcare professionals and end-users. Cybersecurity ethics and medical ethics have been strong established ethical frameworks which can be utilized for each industry, but with innovative ecosystems like SHAPES the two ethical frameworks needs to be viewed from a more specific viewpoint to avoid critical trade-offs and confrontation when taking care of the elderly in scope.

Ethical guidelines combining viewpoints from ethical frameworks for cybersecurity and medical care have been studied quite little and hence I used commonly known ethical frameworks for each branch separately. Markus Christen (2020) describes the current situation as follows. "This growing complexity of the digital ecosystem in combination with increasing global risks has created the following dilemma. Overemphasizing cybersecurity may violate fundamental values such as equality, fairness, freedom or privacy". The ethical aspects of cybersecurity to some extent promotes the equivalent ones in medical ethics, but on the other hand they might confront each other depending on the situation that needs ethical decision-making.

When studying the known ethical frameworks from both a cybersecurity and medical point of view I noted that there are conflicts between these two frameworks. Even though the aim for both is good, the core values between the ethical frameworks might have goals that conflict with each other. When working in an environment with both medical and cybersecurity approaches with a human interaction, ethical guidelines need to be defined as a framework to solve ethical questions and dilemmas when working with patients.

The SHAPES project provides both developers, healthcare professionals, family members and the patients itself access to interaction with the platform. This raises many situations where for example personal health data and other sensitive data might be exposed to many different stakeholders. Personal data is seen as one of the most sensitive types of personal data which must been noted in the development process of the SHAPES ecosystem. Although, from an ethical point of view on cybersecurity privacy as a core value should not be respected

in a sense that it might prevent healthcare professionals in driving healthcare work based on ethical frameworks they work with in their daily profession.

The majority of ethical frameworks and core values presented in the knowledge base of this study does have a strong historical background. The correlations and conflicts between medical and cybersecurity ethics have not been studied more closely. As these two ethical frameworks collide in the SHAPES project, ethical guidelines must be set to provide a secure and continuously developing environment for all stakeholders.

In this study, Heavner's theory worked as a design process tool to come up with the presented guidelines. Many iteration rounds were commenced between the knowledge base, design science process and environment to bring out the artifact, which in this study refers to ethical guidelines for developing SHAPES solutions from both a medical and cybersecurity ethics perspective. From Hevner's Design Science Process, the rigor cycle connecting the knowledge base with the design process itself became more important because of the lack of actual field testing and feedback from the environment. The relevance of presented ethical frameworks and gathering feedback from the environment can be a topic for further research.

5.2 Ethical Decision-making

In order to follow a given ethical guideline when making ethical decision, a decision-making model should be introduced and followed by stakeholders, as shown in Figure 4. From a SHAPES perspective this applies mostly to developers and healthcare professionals. An ethical decision-making model ensures that the person making the ethical decision takes into consideration the given stakeholders, environment, facts and already known principles to make a commonly beneficial decision.

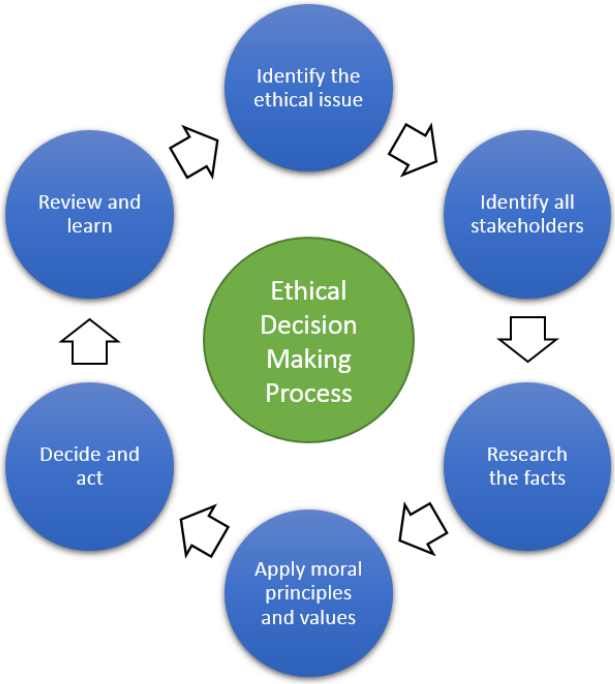

Figure 4. Ethical Decision-Making Process (The Irish Hospice Foundation 2016)

When making ethical decisions in the SHAPES context, three different layers of stakeholders need to be considered as shown in Figure 5, the human layer, the software layer and the platform layer with a focus on the elderly. All layers need to support ethical decision-making or if not possible, then usage of that function should not commence, and information brought to developers of the platform. Some ethical dilemmas might occur even if a healthcare professional could commence an ethical decision but the platform or software behind it does not allow the decision-making process to be carried through as described earlier in this chapter. For example, if a healthcare professional is commencing a procedure that requires colleting personal data that is already not collected but the platform somehow would send this personal data to unwanted stakeholders, an ethical decision has been made but reflecting on the core values of cybersecurity the outcome is negative. Similar ethical conflicts are used as examples in the following chapters alongside the ethical guidelines.

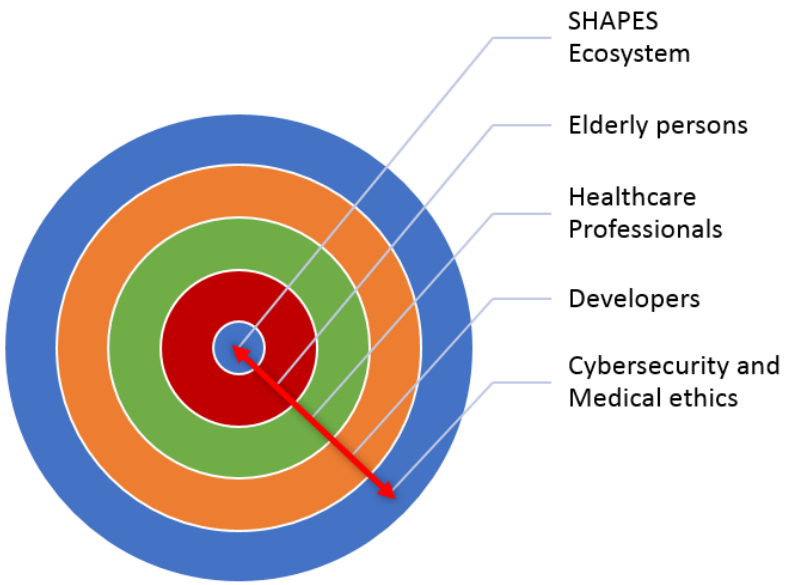

Figure 5. Stakeholder layers in Ethical decision-making in SHAPES project

5.3 Ethical guidelines for SHAPES project regarding privacy

Health-related personal data is seen as one of the most sensitive form of personal data. In a SHAPES context personal data is playing a key role and from a cybersecurity ethical point of view privacy is one of the key values. What makes privacy related issues even more important is that there are several different stakeholders in interaction with the elderly patient's personal health data. These stakeholders might include healthcare professionals, developers, family members and the end-user.

From a biomedical ethics perspective there is not a clear ethical core value that would correlate with privacy, but one might face ethical dilemmas related to privacy when utilizing the SHAPES ecosystem. The biomedical ethics aim closely on the wellbeing of the patient and drives action for the best end result for the patient's physical health. Furthermore, in cases where healthcare professionals need to take action to prevent harm of the patient, ethical viewpoints for cybersecurity might be not taken into consideration. For example, if a healthcare professional need to perform an activity on the patient that he or she needs help from a colleague and in order to get this help, he or she need to provide full health related personal data over the phone or through another platform, we can see that privacy of health-related personal data has been transmitted.

Both privacy in cybersecurity ethics and autonomy in medical ethics aim for moral autonomy for the patient. From a cybersecurity perspective, the patient needs to have control over

personal health data and trust in that this data is handled in an appropriate manner respecting dignity, identity and anonymity. Autonomy in medical ethics aims to give the patient control and that the patients dignity and humanity is respected even though medical procedure is carried through.

The ethical guidelines for SHAPES project regarding privacy:

1) Design and develop SHAPES software so that privacy is considered in every development step from design to end-user implementation
2) Promote privacy in all use cases and considering different stakeholders. Introduce privacy statements for different user groups.
3) Respect personal health data in all phases of development
4) Evaluate which personal data needs to be provided to third party vendors and strive to minimize the amount of personal data provided
5) Discuss privacy openly with the end-users

5.4 Ethical guidelines for SHAPES project regarding autonomy

Autonomy in seen as one of the main principles in biomedical ethics – the possibility for self-rule and respecting the decision-making of individuals during healthcare related measures. Autonomy especially reflects to informed consent and refusal. When looking from a cybersecurity ethical point of view, the biomedical core value autonomy finds its opposite pairs from privacy, consent, anonymity and confidentiality.

From a cybersecurity ethical perspective, autonomy can be reflected to anonymity and referred to giving the possibility to hide personal data if wanted and giving the user the self-rule to control what data are provided to developers for example. Should a person receive different care or functionalities in the platform if they refuse to provide full personal and health data? The environment in the SHAPES project includes elderly people who might not have the full technological knowledge to make decisions on what data is safe to be provided in the environment. This creates a new layer of communication needed, when requesting the consent of personal data sharing.

From a biomedical ethics perspective, healthcare professionals should be able to provide the same level of care to the elderly people regardless of the data the patient has provided and regardless of what data the developers are utilizing in order to create new functionalities or services to the ecosystem. Also, the elderly should have the feeling of autonomy when living the daily life. One example could be assistive technology such as a fall detector. When

designing ethical guidelines for autonomy in the SHAPES project, the possibility of patients not willing to share their data but rather plead to autonomy needs to be considered.

The ethical guidelines for SHAPES project regarding autonomy:

1) Give all stakeholders the autonomy to decide on whether an action is taken or not. Action might refer to collecting data, utilizing assistive technologies like
2) Continuously collect feedback from different user groups to ensure that the feeling of self-rule maintains
3) Develop and design SHAPES software in a way that autonomy is respected and consent for sharing personal data is asked
4) Utilize communication material to emphasize that technology is developed to maintain autonomy, not to take it away
5) Discuss autonomy with patients and collect feedback to bring back to the development process

5.5 Ethical guidelines for SHAPES project regarding consent

Giving consent can have different meanings depending on the situation. When looking at ethics from a biomedical point of view, giving consent might refer to giving your arm for a blood test, meaning giving consent usually refers to a particular action or procedure whereas it might get a broader perspective from a cybersecurity ethics point of view.

From a cybersecurity ethics perspective giving consent usually refers to giving permission for data collecting or utilizing already collected data for other purposes. In a SHAPES context the ethical framework for requesting consent needs to be constructed from several different angles. There might be situations where the healthcare professional commences medical advising remotely or the elderly is in interaction through the SHAPES platform to different stakeholders. Also, elderly people with not that much experience with technological devices might not be aware of the capabilities of data collecting and distributing and hence should consent be requested in several different touch points.

Different forms of requesting and giving consent should be considered as in some cases the consent might be requested not directly from the end-user (elderly) but from a family member for example. Authorization methods and verifying the consent given should be a part of the process.

The ethical guidelines for SHAPES project regarding consent:

1) Design and develop all functionalities so that consent is requested from the end-user on a regularly basis
2) Inform other stakeholders such as family members or healthcare professionals for which processes consent need to be requested from the end-sure and provide enough material for communication
3) Design processes in a way that consent is requested on a frequently basis and strive to provide information about consent in several formats such as audio and printed text
4) Quality and level of service must not be negatively affected, even if the end-user refuses to give consent. If an end-user refuses to give consent, a fallback process for re-requesting consent through another channel must be in place. Healthcare professionals should be considered in requesting consent.

5.6 Ethical guidelines for SHAPES project regarding beneficence

Preventing and removing harm and promoting the good can be defined as one of the basic ethical frameworks of life and one of the core values in biomedical ethics. Nonmaleficence is seen as a part of beneficence as it drives towards actions that prohibits infliction to harm, injury and death.

From a cybersecurity ethics perspective, principlism is a core value that has the same fundamental goals as beneficence. One should strive to respect others, benefit by maximizing the good and treat each other with justice.

In a SHAPES context, beneficence can be seen as the outcome where elderly people are able to stay home longer, and that the society also benefits from this. All stakeholders within the SHAPES ecosystem should maximize benefit and minimize harm of the elderly from software development to performing possible health related actions on the patient. Also, from a software perspective, beneficence should be as an active part of the designing and development perspective so that the aim of each development is to maximize good for the end-user.

The ethical guidelines for SHAPES project regarding beneficence:

1) Every action and procedure made through or on basis of information from the SHAPES ecosystem should aim on preventing harm and promoting good for the end-user
2) Collect feedback from the users to ensure that justified decisions to promote good has been done

3) When designing and developing SHAPES software, aim in all development to maximize good and minimize harm
4) Ensure that software is developed in a way that maximizing good is reached even without a human-touch
5) Collect information of possible mistakes in the SHAPES ecosystem or taken decisions and revert this information transparently back to the development process

6 Conclusions

The objective of this study was to provide ethical guidelines for SHAPES (The Smart and healthy Ageing through People Engaging in Supportive Systems), which is a project funded by the European Union's 2020 research and innovation programme. The scoping was limited to provide ethical guidelines regarding biomedical and cybersecurity ethics to different stakeholders in interaction with the SHAPES ecosystem. The findings from this study will be utilized in format of a conference paper in the DIGILIENCE 2021 conference.

The method used in this study was Hevner's Design Science research as it was suitable in the SHAPES context, where the design process reflects on already known knowledge about theories and relevant topics, but also provides the possibility to input back information into the knowledge base. Also, the environment of SHAPES is important, where many different stakeholders interact within the SHAPES ecosystem and ethical decision- making ranges from developers to healthcare professionals and end-users, elderly people living at home.

The theoretical framework was used to input context into the knowledge base. Commonly known ethical frameworks and core values was used for both biomedical ethics and cybersecurity ethics to provide a comprehensive context for performing the design process.

The output from Hevner's Design Science Research method was a set of ethical guidelines for different ethical topics covering privacy, autonomy, consent and beneficence. The ethical guidelines were formed by cross-checking similarities and conflicts between commonly known ethical theories and reflecting these findings to the environment. It is important to notice that Cybersecurity ethics and biomedical ethics are highly involved for all stakeholders and actions made within the SHAPES ecosystem. All stakeholder groups need to be identified and provided with similar ethical guidelines.

One of the challenges of this study was gathering and combining theoretical framework from two similar topics but totally different context – cybersecurity ethics and biomedical ethics. Literature was broadly available, but profession specific terminology and examples required

broad adoption and basic understanding of the context before determining which ethical approaches should be used in this study.

As a personal learning experience, this study was useful. The study taught a lot about commonly known ethical frameworks, deepened the understanding on how to compare ethical frameworks and contributed towards learning designing methods. The scope of the study could have been narrowed down even more to put emphasis on just a targeted set of ethical frameworks and providing even more deep insights on the selected ones.

Several opportunities remain for further research regarding the topic of ethical viewpoints in SHAPES context. Further research could be conducted in a form of an analysis between processes carried over by a human versus processes carried over by a machine or AI. SHAPES provide elderly people the ability to stay home for a longer time and receive efficient treatment with respect for the human life with the help of technological innovation and collaboration.

References

Printed

Barland, M. & Lovett, H. 2015. The Future of Ageing. Policy report on technology, innovation and organisation in European health care. PACITA.

Beauchamp, T. & Childress, J. 2009. Principles of Biomedical Ethics. New York: Oxford University Press.

Cabrera, M. & Malanowski, N. 2009. Information and Communication Technologies for Active Ageing. Amsterdam: IOS Press.

Christen, M., Gordjin, B. & Loi, M. 2020. The Ethics of Cybersecurity. Switzerland: Springer Nature Switzerland

Christen, M. & Loi, M. Ethical Frameworks for Cybersecurity. In: M. Christen et al. (eds.), The Ethics of Cybersecurity. Switzerland: Springer Nature Switzerland

Hevner, A. & Chatterjee, S. 2010. Design Research in Information Systems - Theory and Practise. New York: Springer.

Himma, K. & Tavani, H. 2008. The Handbook of Information and Computer Ethics. New Jersey: John Wiley & Sons, Inc.

Irish Hospice Foundation. McCarthy, J., Campbell, L., Dalton-O'Connor, C., Andrews, T. and McLoughlin, K. 2016. Palliative Care for the Person with Dementia. Guidance Document 6: Ethical Decision Making in End-of-Life Care and the Person with Dementia. Dublin: Irish Hospice Foundation.

Kaakinen J.& Törmä S. 1999. Esiselvitys geronteknologiasta – Ikääntyvä väestö ja teknologian mahdollisuudet. Tulevaisuusvaliokunnan teknologiaosasto, Teknologian arviointeja 5, Eduskunnan kanslian julkaisu 2/1999.

Manjikian, M. 2018. Cybersecurity Ethics - An Introduction. New York: Routledge.

Mantas, J. & Hasman, A. 2013. Informatics, Management and Technology in Healthcare. Amsterdam: IOS Press.

Spargo, M., Goodfellow, N., Scullin, C., Grigoleit, S., Andreou, A., Mavromoustakis, C.X., Guerra, B., Manso, M., Larburu, N., Villacañas, Ó., Fleming, G., Scott, M. 2020. Shaping the Future of Digitally Enabled Health and Care. Basel: MDPI.

van de Poel, I. 2020. Core Values and Value Conflicts. In: Christen, M. et al., The Ethics of Cybersecurity. Switzerland: Springer Nature Switzerland

Viirkorpi, P. 2015. Ikäteknologian hyvät käytännöt. Helsinki: Vanhus- ja lähimmäispalvelun liitto ry.

Walker, A. 2009. Active Ageing in Europe: Policy Discourses and initiatives. In: Cabrera, M. & Malanowski, N. Information and Communication Technologies for Active Ageing. Amsterdam: IOS Press.

Electronic

European Commission. 2021. Cybersecurity Policies. Accessed 26 February 2021. https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies

Ministry for Foreign Affairs. 2021. Enabling Active Ageing in Finland. Accessed 13 March 2021. https://finland.fi/life-society/enabling-active-ageing-in-finland/

Sarlio-Siintola, S. 2020. SHAPES Ethical Framework. Accessed 16 March 2021. https://shapes2020.eu/wp-content/uploads/2020/11/D8.4-SHAPES-Ethical-Framework.pdf

SHAPES. 2020. SHAPES Brochure. Accessed 8 February 2021. https://shapes2020.eu/wp-content/uploads/2020/10/brochure_shapes_online.pdf

THL Finnish institute for health and welfare. 2021. Older people services undergoing a change. Accessed 13 March 2021. https://thl.fi/en/web/ageing/older-people-services-undergoing-a-change

UIC. 2020. Cybersecurity: How can It Be Improved in Health Care? Accessed 26 February 2021. https://healthinformatics.uic.edu/blog/cybersecurity-how-can-it-be-improved-in-health-care/

Figures

Appendices

Appendix 1: Ethics of Cybersecurity in Digital Healthcare and Well-being of Elderly at Home

This appendix is not publicly available at the time of publishing this thesis.