Technologies Facilitating Elderly Autonomy: Ethical and Cybersecurity Dimensions

Matti Lampinen

2022 Laurea

Laurea University of Applied Sciences

Technologies Facilitating Elderly Autonomy: Ethical and Cybersecurity Dimensions

Matti Lampinen
Safety, Security & Risk Management
Master's Thesis
May, 2022

Laurea-ammattikorkeakoulu **Tiivistelmä**

Turvallisuusjohtaminen

Tutkinto (Ylempi AMK)

Matti Lampinen

Eettiset ja kyberturvan ulottuvuudet ikäihmisten itsenäisyyttä tukevassa teknologiassa

Vuosi 2022 Sivumäärä 40

Tämä opinnäytetyö tehtiin Laurea-ammattikorkeakoulun toimeksiantona ja aiheeksi muodostui eettiset ja kyberturvan ulottuvuudet SHAPES-hankkeessa. SHAPES-hankkeen keskeisenä tavoitteena on tuottaa parempia teknologiapohjaisia kotona selviytymistä tukevia terveyspalveluja ikäihmisille.

Opinnäytetyössä tarkasteltiin miten eettiset kysymykset kuten autonomia ja tietoinen suostumus ilmenevät ikäihmisten kotona selviytymistä tukevissa teknologiaratkaisuissa ja miten eettiset ja kyberturvan ulottuvuudet linkittyvät terveysteknologiaan.

Tiedonkeruumenetelminä käytettiin kirjallisuuskatsausta sekä puolistrukturoituja asiantuntijateemahaastatteluita. Opinnäytetyön päätutkimusmenetelmä oli luonteeltaan kvalitatiivinen. Tutkimus oli samalla myös eksploratiivinen ja yritti löytää uutta tietoa olemassaolevaa tutkimustietoa sekä uutta tutkimusta hyödyntäen. Tutkimus pyrki avointen teemahaastatteluiden kautta kartoittamaan tilanteita joissa, ja mekanismeja joiden kautta eettiset ja kyberturvakysymykset nousevat esiin ikäihmisille suunnatuissa digitaalisissa terveyspalveluissa ja tuotteissa. Tutkimusta varten haastateltiin seitsemää asiantuntijaa neljästä eri organisaatiosta.

Tutkimus tukee aiempien terveysteknologian kyberturvallisuuden eettistä päätöksentekoa kartoittavien tutkimusten havaintoja siitä, että lainsäädännölliset, eettiset ja kyberturvan ulottuvuudet ovat usein ristiriidassa muodostaen arvokonflikteja. Tutkimuksessa ei noussut esille merkittävää digitaalista kuilua ikääntyneiden terveysteknologian käyttäjien suhteen.

Asiasanat: Etiikka, ikääntyminen, kyberturvallisuus, terveysteknologia, SHAPES-projekti

Laurea University of Applied Sciences **Abstract**

Degree Programme in Security Management

Master of Business Administration

Matti Lampinen

Technologies Facilitating Elderly Autonomy: Ethical and Cybersecurity Dimensions

Year 2022 Number of pages 40

This work is a part of the Smart & Healthy Ageing through People Engaging in Supportive Systems (SHAPES) project, which seeks to facilitate long-term healthy and active ageing and the maintenance of a high-quality standard of life. Mediated by technology, in-home and local community environments interact with health and care (H&C) networks contributing to the reduction of H&C costs, hospitalisations and institutional care.

The objectives of this study were, firstly, to analyse how ethical constructs are manifested in the application of technologies facilitating elderly autonomy and, secondly, what are the interlinkages of cybersecurity and health technology.

The primary source of information was empirical research, which was conducted as a case study. The study was qualitative and the information was gathered through semi-structured in-depth interviews. The cases studied were four Finnish organizations. The interviewees included seven Finnish managers from different levels of the four organizations. Earlier gerontechnology research articles and material were utilized as secondary information sources.

The study arrived at the conclusion that legal, ethical and cybersecurity dimensions significantly impact gerontechnology development and usage, creating value conflicts and requiring trade-offs between usability, ethics and security. The present study thus supports earlier research. There were, however, no indications of a significant age-based digital divide in the use of networked health technology.

Keywords: Cybersecurity, elderly care, ethics, healthcare technology, SHAPES-project

Contents

Glossary of key concepts

Ageism	Stereotyping and/or discrimination against individuals or groups on the basis of their age. This may be casual or systemic. Digital ageism refers to the prejudices faced by the elderly in the digital world (Rosales and Fernández-Ardèvol 2020).
Bioethics	Bioethics is the study of the controversial ethical issues emerging from advances in biology, medicine and technologies. It proposes the discussion about moral discernment in society and it is often related to questions on values in medical policy and practice (Science Daily 2022).
Digital Divide	Many older persons have limited access to digital technology and lack necessary skills to fully utilise them. The physical features of smart devices do not necessarily account for the physiological challenges older adults may face, such as impaired vision or dexterity. Older adults may have equal access to digital technologies, but find them impractical to use. A digital divide is commonly considered a social inequality or injustice that a society must find ways to bridge (Wu, Damnée, Kerhervé, Ware & Rigaud 2015).
Gerontechnology	An interdisciplinary academic field combining gerontology and technology. In other words, it comprises technological solutions designed for older people. Gerontechnology can be categorized as a subset of health technology (Sundgren, Stolt & Suhonen 2019).
Internet of Things	The interconnection via the internet of computing devices embedded in everyday objects, enabling them to send and receive data (Oracle 2022).
Stereotyping	Using extreme, exaggerated forms of behaviour. Stereotyping is a result of cognitive simplification and limits the ability to understand fine differences in complex issues (Britannica 2022).

1 Introduction

1.1 Background to the study

Ageing population and the rapid technological advancement of are two megatrends driving a profound societal change. Finland ranked fifth (after Japan, Monaco, Martinique and Italy) in the world in terms of the percentage of total population over 65 years of age in 2020 (Statista 2021). In Finland, 22.7 percent of the population was over 65 years in 2020 (Tilastokeskus 2021). In most countries, older adults prefer to age in place, which entails the ability to live in one's own home and community safely, independently, and comfortably, regardless of age, income, or ability level. According to a study conducted in the United States by AARP (2016), 90% of older adults want to remain living in their homes for as long as possible. As one ages, this becomes increasingly challenging, for various reasons. Digital assistive technologies can help the older adults overcome some of these challenges, and with the advantages of digitalization, senior citizens are indeed becoming key users of technologies, such as wearable health trackers, Internet of Things (IoT) and emerging smart home solutions.

Governments, on the other hand, have a strong vested interest to support aging at home. The financial costs of elderly hospital care are well studied in Finland, and the research gives support to cost savings through prolonging aging in home environment as long as possible (Halminen 2016, Halminen et al. 2019). Besides the primary driver of cost savings, the government also has a duty of care towards its most vulnerable demographic, the elderly. Technology has been an enabler in meeting this dual-objective of both senior citizens and governments. Assistive technologies can result in significant societal cost savings in countries like Finland and Japan, but they also entail significant ethical and cybersecurity questions. Cybersecurity is an essential part of a safe, effective and reliable healthcare delivery system. However, there are privacy risks associated with wearables and home IoTs.

This paradigm technological shift has also resulted in criminals finding ways to use cyberspace for old-fashioned goals such as theft, fraud and intimidation. As a result, cyberfraud is increasingly affecting digital technology users across the globe, to the degree that avoiding cybercrime is becoming an important component of one's capacity to function independently. Senior citizens are the most vulnerable demographic prone to cybercrime, largely due to their limited cybersecurity awareness and skills combined with perceived high personal wealth (Federal Bureau of Investigation 2020, 2021). Due to the natural consequences of aging, such as, loss of eyesight and hearing along with other debilitating ailments, the elderly are unquestionably vulnerable. In addition, elderly people are more likely to suffer from mild cognitive impairments, communication difficulties and increased feelings of loneliness with

added financial pressures and are hence more susceptible to persons who prey upon such characteristics. Typically, fraud can have a devastating impact on the psychophysical and financial wellbeing of senior citizens. Healthcare is data targeted by malicious parties because it often contains all individual's personally identifiable information. With the increased adoption of assistive technologies facilitating elderly autonomy and aging in place, it is critical that we understand the security-behavioral issues that make the elderly vulnerable, and that we navigate this without stereotyping and ageism. Addressing cybersecurity in this context highlights societal and ethical implications, since the protection of vulnerable groups could be seen as a societal responsibility (Von Solms and Van Niekerk 2013).

1.2 Research gap

There is a large body of research on the multitude of assistive technologies in elderly care (gerontechnologies) as well as general bioethical guidance on codes of conduct. Existing cybersecurity literature, however, has thus far failed to address the impact of retirement as a major life transition on technology use and cybersecurity vulnerability (Morrison et al. 2020). Moreover, the ethics of cybersecurity is not a well-established subject academically. As Yaghmaei et al (2017) highlight, it is an under-developed topic within the ethics of Information and Communications Technology, where most academic articles discuss issues like big data and privacy and ethics of surveillance. Similarly, a large body of earlier ethics research in gerontechnology focuses on surveillance and monitoring of elderly people through location tracking, fall detection sensors, and other activity recognition towards wellbeing assessment. Safety, privacy and autonomy are the recurring themes. Cybersecurity within this context is typically only discussed as a tool to protect privacy.

While the ethical implications of the use of gerontechnology have been well raised, the empirical research on the topic remains scarce, especially research focusing on the service/product providers. A fresh look at cybersecurity and ethical framing of elderly care technologies in use in Finland is lacking. This paper explores the ethical landscape of emerging technologies facilitating elderly autonomy and the human factor at the core of cybersecurity. A holistic approach is needed towards developing a roadmap for responsibly introducing new digital health technologies in a manner that safeguards and benefits all stakeholders, including patients, caregivers, health professionals and companies offering gerontechnology solutions. More specifically, this paper focuses on encompassing the nexus of psychological, behavioral, and ethical aspects of cybersecurity, emphasizing a holistic approach, which is largely missing from the mainstream cybersecurity discourse. This study examines different views and approaches to the ethics of cybersecurity in healthcare in Finland with the objective of contributing to the SHAPES project in supporting the wellbeing and aging of elderly at home.

With a view to the above, this paper will focus on the following research questions:

- How do respect for autonomy and informed consent reflect in gerontechnology usage?
- What age-related ethical friction and conflicts arise in the application of networked health technology products/services?
- How do privacy issues, which are both a core value cluster in cybersecurity and desiredata in ICT in healthcare, manifest in the use of networked health technology?

Consequently, this study attempts to forward our understanding of the phenomenon of cybersecurity-ethical management in Finnish organizations providing SHAPES-solutions. However, the following three limitations are recognized. First, it is not possible to discuss the multitude of existing and emerging assistive gerontechnologies within the scope of this paper. For instance, smart homes and robots in elderly care are not addressed in this research. Second, this study focuses on companies' and product developers' perspective and it is recognized that also including a large sample of end-users of gerontechnology would allow a more comprehensive comparison of findings. And, third, this paper is an explorative qualitative research, and the limitation may be its lack of generalizability to a broader organization population outside Finland.

2 Literature Review

This chapter provides the reader with an overview of the present topic by introducing the SHAPES digital ecosystem and a conceptual model for a systematic relation analysis of ethical matters related to cybersecurity in digital healthcare and well-being built upon earlier research (Christen et al 2017) and developed by Rajamäki and Hämäläinen (2021). Furthermore, selected earlier literature on privacy and autonomy concerns in assistive elderly care technologies is discussed.

2.1 Gerontechnology and the SHAPES digital ecosystem

Gerontechnology is an interdisciplinary academic field combining gerontology (eg, medical, psychological, and social sciences of aging) and technology (eg, information and communication technologies, and robotics). In other words, it comprises technological solutions designed for older people (Sundgren et al. 2019). The knowledge basis of gerontechnology is provided by combining insights into processes of ageing individuals and ageing societies on the one hand and insights into new technological options on the other (Bouma, Herman et al 2007). The combination constitutes the field of gerontechnology.

Gerontechnology can, furthermore, be categorized as a subset of health technology. Appendix 2 presents an example of categorization of companies within this market.

Figure 1 below (SHAPES 2021) presents an overview of the diversity of digital elderly care solutions. Many can be further divided into subcategories. For example, activity recognition and security include surveillance of people in their own homes, ranging from the use of sensors to check to see if a person has fallen to surveillance on door entries. Solutions in this category also include GPS bracelet tracking to monitor movements, enabling caregivers and relatives information on their elderly relative whereabouts. Use of such technology, however, clearly has ethical and cybersecurity implications. Informed consent from the elderly person is of paramount importance and, should a malicious third-party gain access to any person's location or health data, it can result in serious harm.

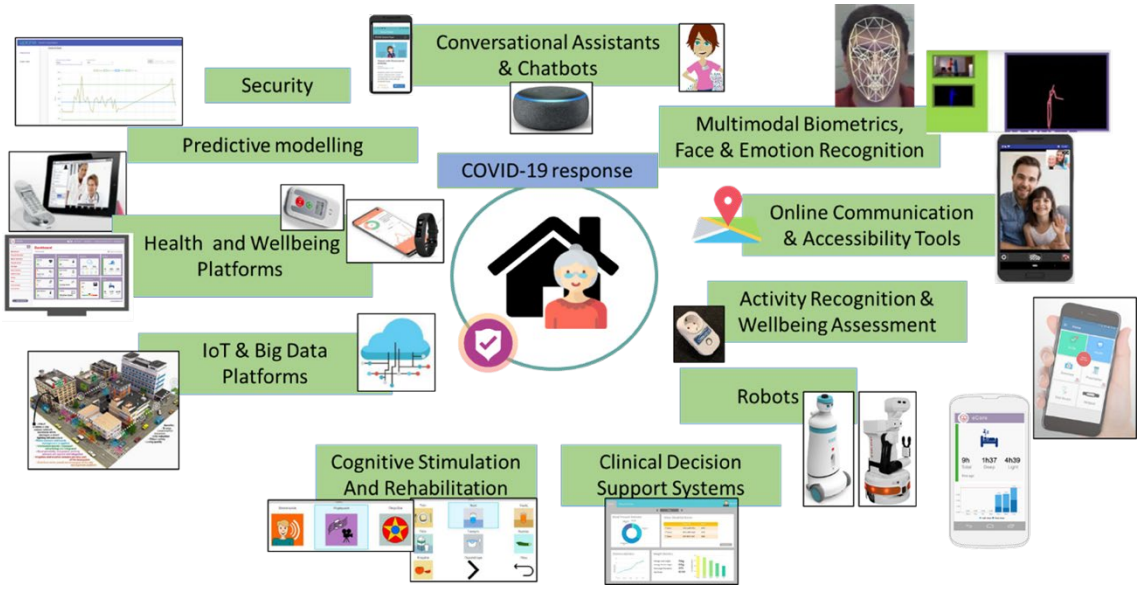

Figure 1: SHAPES Digital Solutions Overview (SHAPES 2021)

Another related area is integrated provision of technology, where many digital solutions and devices are brought together in the form of smart homes. While from technological standpoint the implementation is a reasonably simple combination of existing software and hardware solutions, the potential ethical and cybersecurity issues multiply (Coboi, Tran, Tran & Nguyen 2021). It can be argued that there is, however, a clear need for smart homes to support aging at home environment, because many homes may not be designed to accommodate the needs of aging homeowners.

Although increased collection of vitals data, such as heart rate, breathing rate, body temperature, blood sugar or heart pacifier status can be justified from remote health monitoring and diagnosis (telehealth) perspective by allowing patients to receive advice and care at a distance, it also offers a cache of data for malevolent actors in cyberspace, where

such data is stored and transmitted. Complex interconnected clinical systems require the prioritization of cybersecurity to ensure the privacy and security of health information (Hood 2021). Moreover, the key bioethical principle of respect for autonomy (Beauchamp and Childress 1979) can be violated despite any blanket consent received from the senior citizen. Kaplan (2020) has conducted a literature review of telehealth research and found that evaluations of telehealth rarely address ethical, legal, and social issues. Instead, the primary academic focus has been on the quality of care, access, consent, and privacy.

Finally, another emerging area is the use of robots which are increasingly being utilized for many different purposes both at homes and healthcare facilities. Very limited research exists regarding the processes of ethical scrutiny for their use.

In order to encourage assistive digital care technology adoption Wu et al (2015) have highlighted that designers must assure the solutions are compatible with elderly lifestyle and values, fits in their needs and is easily assimilated in their lives. It must be easy to understand and use, and it must have a clear advantage over traditional solutions.

2.2 Conceptual model for analysing ethical aspects of cybersecurity in healthcare

Rapid digitalization has resulted in the emergence of new stakeholders in health care, because human behaviour is increasingly determined by information and communications technology. Therefore, when formulating ethical guidelines, more emphasis should be on the fact that technology can expand/restrict the scope of action for stakeholders (Yaghmaei et al. 2017). Stakeholders, who design and deploy novel technological elderly care solutions must become more aware that technology, particularly when used in elderly health care brings special ethical requirements with it. Figure 2 below (Rajamäki and Hämäläinen 2021) presents a conceptual model for a systematic relation analysis of ethical matters related to cybersecurity in digital healthcare and well-being. The interlinkages of the model are discussed throughout this paper, and examples provided, when feasible.

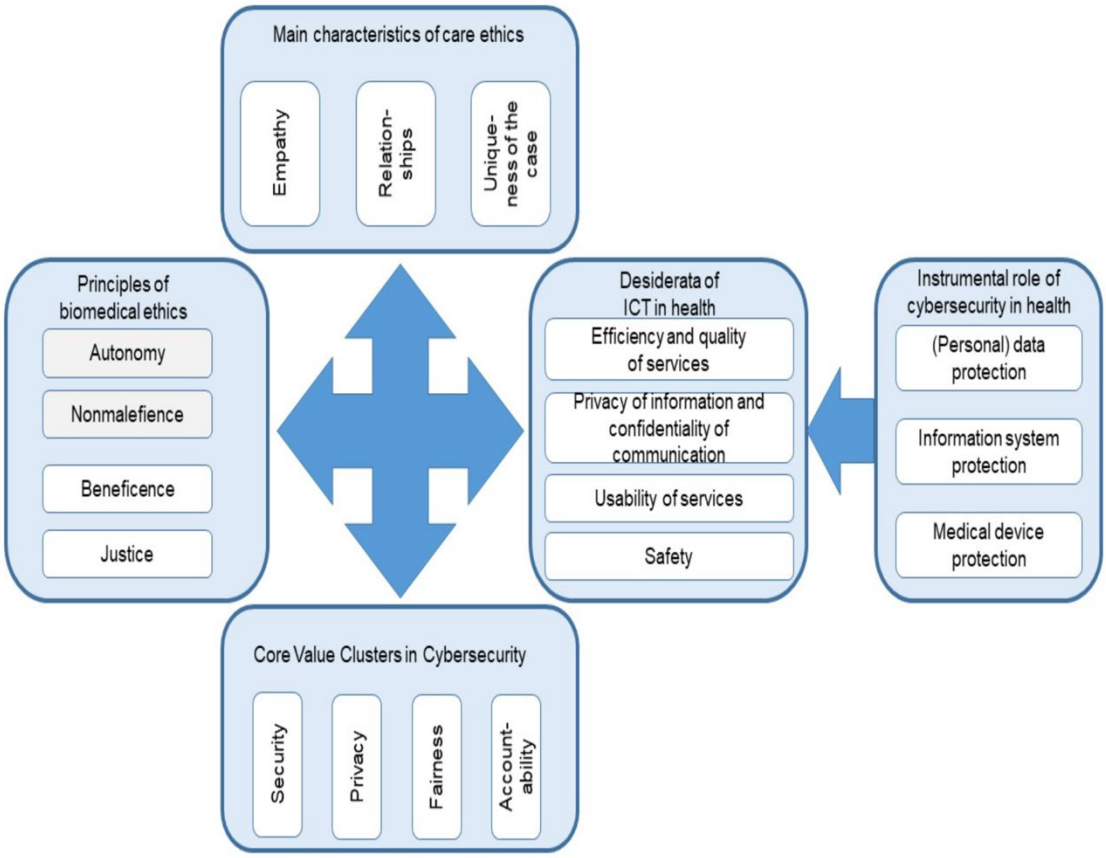

Figure 2: Conceptual model for analysing ethical aspects of cybersecurity in healthcare (Rajamäki & Hämäläinen 2021)

Principles of biomedical ethics, also referred to as Principlism, are the moral principles governing the practice of medicine. Regardless of gender, religion, age or race, medical ethics ensures guaranteed quality and principled care for all people. Medical ethics applies not only to members of medical profession but also to social care professionals, lawyers and policy makers. The principles of biomedical ethics by Beauchamp and Childress (1979) form the most widely used and generally accepted guiding medical ethics framework. Since their introduction they have been the dominant approach to the teaching and evaluation of medical ethical dilemmata in health care. The four principles are:

Respect for Autonomy: respecting the decision-making capacities of autonomous persons; enabling individuals to make reasoned informed choices. This principle is set for the practice of informed consent.

Beneficence: this considers the balancing of benefits of treatment against the risks and costs; the healthcare professional should act in a way that benefits the patient. Principle describes ethics of not causing intentional harm or injury to the patient.

Non maleficence: avoiding the causation of harm; the healthcare professional should not harm the patient. All treatment involves some harm, even if minimal, but the harm should not be disproportionate to the benefits of treatment.

Justice: distributing benefits, risks and costs fairly; the notion that patients in similar positions regardless of gender, race, age or religion should be treated in a similar manner.

Of note, bioethical challenges can also be approached and addressed with other ethical frameworks, including Utilatiarism and Human Rights. First, Utilatiarism holds that the most ethical choice is the one that will produce the greatest good for the greatest number and is, therefore, basically a cost-benefit analysis, where the expected value of each option in any decision-making scenario is calculated, i.e. likelihood of outcome multiplied by the value of the actually occurring outcome of that option (Marseille and Kahn 2019). The challenge of applying utilitarianism is that the probability is often difficult to estimate. Moreover, when possible cost of loss of human life is discussed, the standard legal approach is using statistical expectations of future salaries. In the case of elderly citizens, this approach would be ethically highly controversial. Second, Human Rights principle is developed in terms of five distinct core concerns regarding respect for persons: autonomy, dignity, integrity, privacy, and vulnerability (Brännmark 2017). While the above-described principle of human rights is also well suited to address gerontechnology cybersecurity-ethical challenges, for the purposes of this paper the Beauchamp and Childress (1979) principles are used.

Desiredata of ICT in health covers all the technologies adopted in the healthcare sector and stresses the four key tenets of efficiency, privacy, usability and safety (Rajamäki and Hämäläinen 2021). For the purposes of this study, the author has narrowed the focus into privacy in the various solutions connecting over the Internet. These include, for instance, a) smart wearable devices (monitoring heart rate, blood oxygen level, blood pressure, perspiration level, blood alcohol level), b) home-use medical devices (glucose monitor, INR-test, insulin pumps), c) implantable devices (cardioverter defibrillators, heart pacemakers) d) point-of-care kits (diagnostic tests, analysers), e) emergency response systems and f) virtual home assistants (prescription medicine reminders).

Core value clusters of cybersecurity are security, privacy, fairness and accountability (van de Poel 2020). Moreover, each cluster consists of a range of sub-values, which can be viewed as articulating specific moral reasons relevant when devising cybersecurity measures. The first value cluster, security in the context of healthcare can be understood as primarily individual security, and especially the protection of confidentiality, integrity and availability of digital data. The second value cluster is privacy, and contains values such as moral autonomy, human dignity, identity, personhood, liberty, anonymity and confidentiality. Examples include treating others with dignity, respecting people’s moral autonomy and seeking

informed consent for collecting, transferring, using and storing people's data, as well as explaining the purpose of collecting such data. The third cluster is fairness. Important moral reasons that correspond to this value cluster are that people should be treated fairly and equally, and that democratic and civil rights should be upheld (van de Poel 2020). Finally, the fourth value cluster is accountability. It comprises values such as transparency, openness and explainability. Common reasons to which accountability is related include the obligation to account for one's actions but also being blamed for unjustified behaviour or paying damages, or a fine, for the harm that arises from unjustified behaviour (van de Poel 2020). According to van de Poel (2020) cybersecurity value conflicts in healthcare are typically related to privacy and data protection against unauthorized access. Cybersecurity may often also contradict usability and accessibility.

The common denominator of the organizations in this study is that as part of their daily operations, they are involved in securing national electronic health records, patient psychotherapy data collection and storage, and real time location data of elderly people. Within this realm, the clients' health, privacy and even survival can depend upon cybersecurity success or failure. In several cases the well-being of patients' families or caregivers is being protected as well. While it may be easier to visualize a cybersecurity professional protecting a hospital's network and critical patient data, the reality is that an increasing part of healthcare and the resulting data generation, cloud storage and transfer over Bluetooth and Wi-Fi takes place through networked devices outside the hospital environment. This is also a critical feature in the provision of telemedicine. World Health Organization (2010) has defined telemedicine as: "The delivery of healthcare services, where distance is a critical factor, by all health care professionals using information and communication technologies for the exchange of valid information for diagnosis, treatment and prevention of disease and injuries, research and evaluation, and for the continuing education of health care providers, all in the interests of advancing the health of individuals and their communities."

Cybersecurity in this context is, hence, focused on protecting the lives, privacy and psychophysical well-being of the human beings who depend on the use of such devices. With a view to the above, ethical issues and the ethical responsibility to protect others are at the core of cybersecurity practices, especially in gerontechnology applications due to the vulnerability of elderly users.

2.3 Privacy and autonomy concerns in assistive elderly care technologies

Sundgren et al (2020) conducted a scoping review analysing 17 studies on ethical issues when using gerontechnology in the home care of elderly people and identified two main themes. These were 'balancing between the benefits of using gerontechnology and the basic rights of

older people', consisting of the sub-themes safety, privacy and autonomy. The other main theme, 'gerontechnology as a risk of insecurity for older people', included the subtheme fear of losing human contact. Studies reviewed were mainly surveillance and monitoring technologies. Landau and Werner (2012) and Ellis (2005) have studied ethical aspects of using Global Positioning System (GPS) enabled devices to track people with dementia, and highlighted the lack of ethical consensus, policies and guidelines. While electronic tagging enables elderly with early-stage wandering/dementia to continue living in their homes rather than moving into a nursing home, there is sensitivity to civil liberties and a trade-off between protection/safety and autonomy/privacy. For clarity, it may be helpful to seek informed consent for GPS tracking from those diagnosed with early stages of memory debilitating illnesses, as this so-called precedent autonomy allows the currently capable person to control decision-making at a later point in life, when he/she no longer has the ability to do so. Ellis (2005) highlights that such pre-commitment would allow the elderly to regain some authority over the use of new technologies to monitor their movements/vitals. In other words, if an elderly person becomes incompetent and failes to make advance decisions on the use of assistive gerontechnology, his/her autonomy can be respected by taking the decision that she would have taken, based on evidence of her previously competent wishes, preferences and values. A key emerging question on GPS tracking is, who does the technology serve, the elderly person wearing the tracker, or the anxieties of the caregiver. Wirelessly transmitting a person's GPS location to a central computer and sharing it live with third parties, like security companies and relatives, not only poses obvious cybersecurity concerns but can be seen as an invasion of privacy and a violation of European General Data Protection Regulation (GDPR 2013). Of note, a large body of earlier research on GPS tracking of elderly people has been completed before privacy-protecting legislation was introduced and fails to address cybersecurity issues. Most of the prior research also focuses on dementia patients rather than senior citizens, who still have full or partial decision-making capacity. In a more recent study Lodha and Sousa (2020) looked into the ethics of electronic tagging of cell phones to help relatives track the whereabouts of their elderly dementia patients and, in addition to the above liberty and autonomy concerns, noted that GPS tracking technology and personal information revealed by the linking of personal and Google accounts may be used by companies to electronically spam caregivers with information about dementia care products and also raises privacy concerns for both the caregivers and patients.

Chung et al (2016) in their integrative literature review of 16 articles on ethical considerations regarding the use of smart homes for older adults also brought up the importance of informed consent for ensuring that older people are aware of the mechanisms of their health-related information gathering and sharing. Wang et al (2019) studied older adults' perspectives on technology to support aging in place through focus group research. Their sample comprised of 31 retirement community residents. A large majority of their

participants indicated that they were concerned with data privacy in their daily usage of technology. This high level of concern with controlling their personal data suggests a hesitancy in adopting a technology or submitting personal data to a digital platform (Wang et al 2019).

In their extensive literature review of cybersecurity research and discourse Christen et al (2017) have tracked how major themes have developed with focus on ethical topics. On one hand, overemphasizing cybersecurity may violate fundamental values like equality, fairness, freedom, or privacy, and on the other hand, neglecting cybersecurity could undermine citizens' trust and confidence in the digital infrastructure as well as in policy makers and state authorities (Christen et al 2017). While most cybersecurity measures are aimed at preventing harm, they can, at the same time, cause harm and violate human rights; for instance, by limiting personal freedom in order to counter threats.

To sum up the discussion thus far, we have identified privacy and autonomy as the recurring themes in ethics discourse within gerontechnology. Cybersecurity, however, is typically only discussed as a tool to protect privacy. On the other hand, the 'ethics of cybersecurity' is not a well-established subject academically, and seldom addresses gerontechnology. There are two streams of academic research that rarely cross. The above highlights the interdisciplinary nature of this paper.

2.4 Elderly cybersecurity awareness and the digital divide

For a holistic approach into analysis of cybersecurity-ethical issues in elderly care, general cybersecurity awareness of the target demographic is of paramount importance. The word "cyber" is short for the term cyberspace, which is generally understood as the interactive domain composed of all digital networks used to store, modify and communicate information. It comprises all information systems used to support businesses, infrastructure and services (Biener et al. 2014). Typically, cybersecurity cases involve risks that are hard to model and quantify in terms of likelihood and severity (Biener et al. 2014). And even when the risks are known, assessing them from an ethical perspective can be very challenging.

Cybersecurity skills, for instance, preventing malware and personal identifiable information theft, correspond to an individual's technical knowledge, ability, and experience surrounding the hardware and software required to execute information security to mitigate cyber-attacks (Carlton and Levy 2017). Age is a significant factor influencing the digital divide, a concept that refers to the tendency for older adults to be less likely to use the Internet and latest digital technology than younger generations (Krueger et al. 2018). As online security threats to the general public continue to evolve, the elderly networked-smart device users with limited skill and knowledge are left playing catch-up in an ever-widening gap in fundamental cyber-related awareness and comprehension. Senior citizens are less likely to have access to

training courses and are often less able to seek advice online. As a result, senior citizens generally lack awareness of current security threats and remain under-educated in terms of applying appropriate controls and safeguards to their personal computers and networked smart devices. A digital divide is commonly considered a social inequality/injustice that a society must find ways to bridge (Wu et al 2015).

New digital tools and services like mobile banking, online grocery shopping, digital payments, telemedicine, wearables and assistance and peer support via social media offer elderly people an opportunity to extend stay at home as their physical and mental condition gradually declines. However, it also increasingly exposes them to cybercrime. Digital progress and the relevant cyber safety awareness and education programs should encompass this underserved and growing part of the population, sometimes referred to as silver surfers or silver economy (Butt et al. 2021) and teach them to safely use digital methods. At the same time, it remains critical to continue providing and supporting non-digital traditional methods, such as accepting cash payments, filing taxes on paper, calling a human being for assistance instead of dealing with chatbots and walking into a hospital for care without using multiple password-protected health applications to book a doctor's appointment. The elderly often wish to stay home and maintain their independence as long as possible before being institutionalized.

Discussion on elderly vulnerability to cybercrime has largely been omitted in Finland. In a major recent government study on the current state of cybersecurity in Finland (Kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi 2017), there is no mention of the most vulnerable demographic: the elderly, who represent 22 percent of the population. Very few government plans directly address the needs of seniors, and those that do are frequently vague and lack specificity. Finland was ranked 14th out of 49 countries in a recent comparison of Cyber Risk Literacy and Education (Oliver Wyman Forum 2021). The index measures the population's cybersecurity knowledge as well as the ways that geographies can enhance that knowledge through education and training. Finland ranked 40th out of 49 in government policies to improve cyber risk literacy and education.

It is clear that having a more cyber risk aware population will become increasingly important as individuals, organizations, and governments face the consequences of aging population and more digital assistive healthcare solutions are introduced, especially into the home environment. Statistically, 95 percent of cybersecurity breaches are caused by human error as a contributing factor, whether through accidentally clicking on a malicious link or weak passwords (Milkovich 2018). A better understanding of cyber related risks and human behavior should directly reduce the frequency of cybersecurity incidents. Further research is needed to

identify efficient means for the society to protect its weakest members, while assuring their right for freedom, independence and digital privacy.

3 Methodology

The previous chapters explained the background of cyber-ethical discourse in healthcare, the main concepts, the SHAPES digital ecosystem, and presented many of the existing models and principles in this field of research. This chapter will go further by explaining the empirical part of the study, how the data was gathered to answer the original research questions, the methods used in the research process, and the reasons why these particular methods were chosen.

3.1 Research design

Qualitative research method was chosen for the present study, as it is recommended when studying a phenomenon about which little is known and when studying organizations and their actions (Ghauri et al. 2020). Qualitative research is a type of research that explores and provides deeper insights into real-world problems. Furthermore, with qualitative research researchers can explore subjects that are poorly studied with quantitative methods. These include opinions, individual's actions, and social science research (Tenny, Brannan & Sharts-Hopko 2021). Within qualitative research data collection semi-structured interviews are characterized by open-ended questions and the use of an interview guide in which the broad areas of interest are defined (Busetto, Wick & Gumbinger 2020). These pre-defined topics in the interview guide can be derived from the literature, previous research or a preliminary method of data collection. Busetto et al (2020) also emphasize that across interviews the focus on the different questions may differ and some questions may be skipped altogether (e.g. if the interviewee is not able or willing to answer the questions). Compared with written surveys, semi-structured interviews have the advantage of being interactive and allowing for unexpected topics to emerge and to be taken up by the researcher (Busetto et al 2020). Reporting on qualitative research involves including details and descriptions of the setting involved and quotes from participants. This detail is called ‘thick’ or ‘rich’ description and is another strength of qualitative research (Tenny et al 2021).

With a view to the above, the empirical part of the present study was conducted as a qualitative survey. This approach is the preferred strategy when “how” and “why” questions are being posed, when the investigator has little control over events, and when the focus is on contemporary phenomenon within some real-life context (Yin 2017). Even though a company-specific case-by-case analysis is not presented within this paper due to

confidentiality and the scope of the present research, it is the purpose of the author to continue with such a detailed analysis in later works.

Finally, the research project was part of the Smart & Healthy Ageing through People Engaging in Supportive Systems (SHAPES) project, which seeks to facilitate long-term healthy and active ageing and the maintenance of a high-quality standard of life. Mediated by technology, in-home and local community environments interact with health and care (H&C) networks contributing to the reduction of H&C costs, hospitalizations and institutional care.

3.2 Process of data gathering

The data was collected by interviewing Finnish managers both at private and government sector. The case organizations were chosen so that they provide insights both from software and hardware vendors offering digital healthcare solutions. Business Finland's Smart Life Finland Project (Business Finland 2021) was contacted to gain a diverse list of suitable case organizations as a starting point.

The process of data gathering took place between September 2021 and January 2022. The data was gathered in empirical in-depth interviews, the duration of one interview generally being between 40 minutes and one hour. The interviews were semi-structured discussions and were supported by an interview guide (Appendix 1) containing several possible questions and topics for discussions. There were altogether seven managerial-level interviewees from four organizations. The four organizations, who significantly contributed to this study were the Social Insurance Institution of Finland (KELA) Kanta Services, Fujitsu, AddSecure and Solita. Below, a brief introduction of the organizations.

KELA Kanta Services produces digital services for the social welfare and healthcare sector. Finland is one of the leading countries in the electronic data management of health and wellbeing. One of the main purposes of information and communications technology (ICT) systems in healthcare is the administration of data on patients and treatments to increase the efficiency of the healthcare system and, at the same time, to reduce its costs. With the use of Electronic Health Record (EHR), ICT assists in improving the quality of medical care for all ages, hence serving as a strategy in making health care delivery increasingly patient-centered. In My Kanta pages citizens can browse their medical records and prescriptions and order repeat prescriptions in the online service. The Kanta Patient Data Repository plays a key role in sharing information between healthcare service providers (KELA 2022). Figure 3 (My Kanta Pages 2022) below shows the architecture of the Kanta-system. Citizens are able to access practically all their health information via the system.

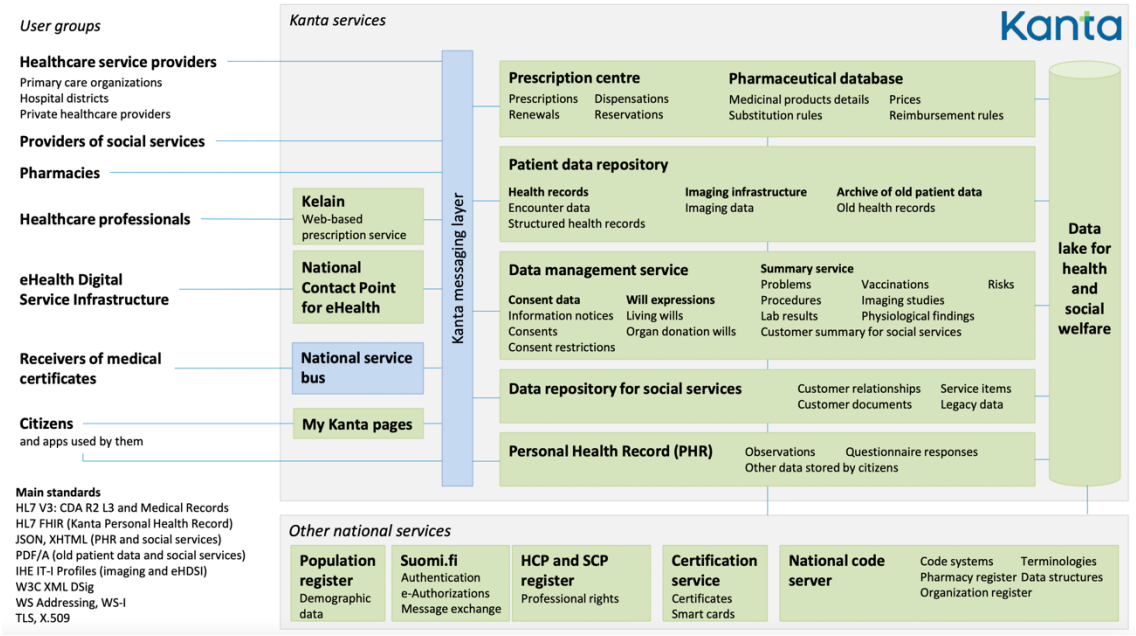

Figure 3: Kanta architecture (My Kanta Pages 2022)

Fujitsu is one of the leading global organizations providing innovative technology solutions to the healthcare industry, especially in integrated care concepts bridging various medical disciplines. Specialized in product design and manufacture, as well as application, data management, healthcare information systems and systems integration, Fujitsu is optimizing the patient experience through IT-enabled change (Fujitsu 2022).

AddSecure Smart Care provides end-to-end safety solutions for elderly living at home. The product and service offering includes the provision and installation of safety devices, alarm monitoring, and alarm management. AddSecure helps seniors live independently at home and be safe by combining human care with reliable and safe technology, helping municipalities and relatives support their elderly and dependent family members so that they can be cared for in real time. Smart Care product portfolio includes, for instance, a GPS safety watch, which is a geolocation wristwatch and a care-phone in one. The watch is equipped with a loudspeaker and a microphone for calling the Alarm Receiving Center. The watch also has telephone functions that enable the user to call relatives. The watch is primarily targeted for active elderly or for those who are suffering from dementia or Alzheimer's disease (AddSecure 2022).

Solita combines expertise from strategic consulting to service design, software development, AI & analytics, cloud and integration services, and designs and builds services with human insight and intelligent technology: helping individuals, health care professionals to create better everyday life, promoting equality, transparency and co-operation. Solita Health assists in creating new services from strategy, design and customer insight to large implementations

and continuous development. Solita Health has over 200 experts, and the division supports change management, taking new ways of working into use and utilising modern technology by using data effectively, safely and ethically in the regulated health care sector. Solita strives for decreasing health and social inequalities between different age-groups, genders, ethnic background, family status and economical status (Solita 2022).

The common denominator of the above organizations in this study is that as part of their daily operations, they are involved in securing national electronic health records, patient psychotherapy data collection and storage, and real time location data of elderly people.

3.3 Objectivity, reliability and validity

Interview, questionnaire, focus group, and participant observation-based data are, evidently, subject to biases of those who provide information and those who collect it. To avoid researcher bias in case organization selection, Business Finland's Smart Life Finland Project (Business Finland 2021) was contacted to gain a diverse list of suitable case organizations as a starting point. Semi-structured interviews can also help overcome a provider or researcher-centred bias often found in written surveys, which by nature, can only measure what is already known or expected to be of relevance to the researcher (Busetto, Wick & Gumbinger 2020). To assure objectivity of the study, full focus has been on the facts and data. The author's interpretation has been based on the factual data collected, and relevant direct quotes from interviews have been included to control and mitigate possible researcher bias. Moreover, any values presented in the study are discussed in the light of earlier body of research and do not represent the author's own values or beliefs. Furthermore, there are no financial conflicts of interest to disclose. No financial support was received for this study and the author has no ties to any of the case organizations or interviewees. In terms of reliability, a concept closely linked to consistency, the same interview guide (Appendix 1) has been meticulously used. Finally, as with any explorative study, there are limits on how far one can generalize about the findings. Although anonymity of participants was required, all interviewees were considered subject matter experts in their respective companies, and all had over a decade of experience in digital healthcare solutions. Both genders were represented in the composition to avoid gender-bias in the sample. Although some of the case organizations had operations in multiple countries, the focus was on their products and operations in Finland. It has to be recognized that this variation erodes the generalizability of the findings to some extent. However, the author believes that the results and conclusions presented in this paper can still be widely applied to digital elderly care both in Finland and other EU countries.

4 Results and Analysis

Chapters two and three covered the literature review and methodology respectively. This chapter focuses on the results of the empirical research in the light of the research questions presented in chapter one. Findings are categorized under two main headings, respect for autonomy and informed consent, and cybersecurity considerations in networked healthcare technology. After this, general observations and a summary of findings per research question is provided.

4.1 Respect for autonomy and informed consent

The respect for autonomy key tenet in biomedical ethics sets the practice of informed consent. The transition to the use of Electronic Healthcare Records (EHR) has created a conflict between privacy protection and utility and quality of the patient records. Informed consent is when the patient gives permission to the treatment or procedure with full knowledge of all possible consequences. In gerontechnology such treatment/procedure also includes, for instance, monitoring of elderly person's behaviour, movements, vitals, medication and home environment. No significant age-related challenges in informed consent were found in this research. As one of the interviewees described:

> "*Understanding how informed consent in the Kanta EHR system works does not seem to depend on age. All age groups are showing a lack of understanding and awareness as to how the social and healthcare information management as a whole works in Finland. There is a large number of different semi-autonomous levels, including health/hospital districts, some with common registers and then a national level as well. And some systems are not linked to the whole like, for instance, social welfare database. It is a very complex jungle for almost anyone (to understand informed consent here), not only for the elderly.*"

Due to the multi-layered healthcare system (see Figure 3 for Kanta architecture) and legal requirements, the users of Kanta services have dozens of informed consent choices to make. There was an attempt in 2021 to simplify the user experience and change this into a model, where users would have been explained the principles of how Kanta system works, and then a single acceptance/consent by default would have enable sharing his/her healthcare records with all the healthcare providers (Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä, Finlex 2021) but such a solution was ruled unconstitutional due to the sensitive nature of private health information. In other words, a user must have an active role in each decision-making situation, where his/her digital health information is transferred between parties. This example illustrates how in the desiredata of ICT in health (Figure 2) the privacy of information and the usability of a service can contradict. Government intervention

in the above example can also be interpreted as duty of care, discussed earlier in this paper, in the protection of vulnerable groups also in cyberspace. There is a trade-off between duty of care, privacy and usability. To sum up the discussion thus far, in the case of electronic health records, interviewees highlighted that legislation protecting privacy has deteriorated the usability of the system.

In the discussions on EHR, it was also highlighted that senior citizens can physically visit healthcare centers and give their consent for sharing their patient information with other health centers and healthcare providers. This has been implemented in order to assure the justice principle of biomedical ethics. In other words, assuring best medical care is equally guaranteed for all regardless of the persons technological skills. Finally, caregivers and third party informed consent was raised by some of the interviewees, which is increasingly relevant in late stages of life. Accessing Kanta services with the power of attorney (POA) was implemented and enabled in March 2021, and in September there were 5000 unique logins into the services using this method. However, the POA access currently only works if the elderly person him/herself has the means for electronical identification, which is then used by a third party with POA. Inability to verify their identity online drops some of the elderly as well as their caretakers outside the Kanta services, highlighting how people without access or the skillset required to adopt information and communication technologies are put at a socio-economic disadvantage, as they are unable or less able to obtain digital information via a system like Kanta. Previous research (Wass et al 2019) has also found that access to electronic health records positively contributes to the quality of care through shared care management. In other words, patients are using their electronic records to improve interactions with both private and public healthcare providers, actively participating decision-making regarding their health.

Ethical concerns were raised by the interviewees also in securing informed consent from elderly with mild cognitive impairment, whether for online health care or the use of assistive technologies such as a GPS safety watch/tracker/help phone.

> "*When we think about the cognitive state of the client.. a person with memory issues and forgetfulness... he/she may still officially be compos mentis, but there might be, often lengthy, guardianship application process ongoing.. these are complicated situations. When signing a contract on the use of assistive technology such as a watch with location tracker and help phone button, there are often family members present. Should, for instance, spouse have access to their partners GPS location 24/7 ? This a question of privacy, and privacy is as important a basic human right even when you are 80 years old. Now, if the person is already under guardianship, then the permission for sharing the location can be given by the guardian. But before that everyone*

> *has to assess which is the bigger risk, the fact that someone has their live location or that they will stumble and perish into a snow bank in winter."*

In Finland, a guardian is appointed by the Digital and Population Data Service Agency or a district court. If a person himself or herself notices that he or she is, due to a degraded capacity, in need of support and assistance of a guardian, he or she may file a written petition with the Digital and Population Data Service Agency. A petition for the appointment of a guardian may also be filed with a district court. A close relative or a social welfare authority, for example, may also notify the Digital and Population Data Service Agency of a person who might need a guardian. (Applying for a guardian, Oikeus.fi 2022)

The nature of EHR and, more specifically, the highly private health data, was found to result in significant challenges in providing customer service. The interviewees described the dilemma as follows:

> "*Providing real time digital support services for the elderly users is extremely difficult due to the fact that only the elderly person him/herself is allowed to access and view any of their private health data, such as prescriptions, in the system. In practice, customer support cannot see who is trying to access what. A user calling to ask, for instance, laboratory results can therefore only be instructed in general terms... first click second box from left and then click..we have no access whatsoever to customer records."*

Of note, to implement law-mandated duty of care and assure equal access to the Electronic Health Records and Kanta services KELA is regularly organizing Kanta service training sessions for instance in libraries as well as online. This is a good example of government efforts to narrow the digital divide.

4.2 Cybersecurity considerations in networked healthcare technology

This research found that privacy, which is both a core value of cybersecurity and desiredata of ICT in health was a key consideration for all the case organizations. More specifically, detaching personal identification information from health data was an integral part of the new product/service concept development. Several of the interviewees highlighted that voice is biometric data and, therefore, entails significant privacy considerations. One of the interviewees described that voiceprint analysis can, however, be implemented without compromising cybersecurity:

> "*..we developed an anonymous voice pattern recognition to detect the level of stress, which can be used to monitor elderly people living alone. A networked device with microphone at home can, without collecting a voiceprint, identify*

> *stress and automatically alert help, in which case the elderly person can be contacted to assure he/she is alright."*

According to the EU General Data Protection Regulation (GDPR, 2013) biometric data is: "personal data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person". Digital technology enables identifying a person based on their facial geometry, fingerprint, DNA, palm print, iris and, for instance, walking style. Voiceprint is another unique authentication method and, therefore, sensitive personal information, the use of which requires informed consent, as stipulated in the GDPR.

The results indicate there is a certain degree of change resistance in adopting such new elderly care technology due to perceived privacy concerns. Especially less technologically inclined users were described as cautious towards having, for instance, a safety microphone installed at their house, despite assurances that the device would only detect stress level guaranteeing anonymity. Interviewees highlighted that many daily consumer products such as televisions feature voice recording and voice pattern recognition capabilities and are often much more vulnerable to cyberattacks than certified medical devices. End users, however, seem more willing to accept the trade-off between privacy and usability in consumer electronics. With a view to the above findings, the caveat is that the empirical research focused on gerontechnology solution providers, and not the end users.

A possible solution to gerontechnology adoption resistance offered by another organization was to start introducing smart home technology and wearables earlier in life in order to avoid stigmatizing it as elderly-tech. Aging is a process, and debilitating conditions, such as loss of memory, do not just emerge overnight.

> "*Especially in the case of elderly care technologies that require the client to actively do something, for instance, charging their location-tracking safety watch after each day, the adoption of such technology should take place as early as possible before the debilitating conditions emerge. Once you already have, for example, Alzheimer's disease, dementia or severe arthritis the adoption of any such new assistive technology is considerably more difficult."*

Security issues often arise when there is a disconnect between what users see as their cybersecurity role, and what is expected of them by others, including product/service developers. As more networked devices are introduced in the home environment the cybersecurity risks multiply.

Privacy was also found to be a key cybersecurity concern also in the use of electronic location-enabled safety watches. As the elderly are legally, from the point of information

security, categorized as vulnerable individuals there are special provisions for the processing of personal data for such individuals. More specifically, impact assessments are designed to identify, evaluate and control risks involved in the processing of personal data. The procedure covers describing the envisaged processing of personal data and assessing the necessity and proportionality of the processing operations in relation to the purposes and the resulting risks as well as the measures envisaged to address the risks. The aim is to establish whether the remaining risk is justified and acceptable in the circumstances in question. Impact assessments help controllers to ensure, document and demonstrate their compliance with data protection regulations (Tietosuojavaltuutetun toimisto 2022). As one of the interviewees described:

> "*We have reached the conclusion that although not all information in our databases and registries fall under the category of vulnerable individuals, it is much simpler (for compliance) for us to conduct a data protection impact assessment on absolutely everything rather than try and isolate the data by category.*"

The example highlights how a company operating in an area of elderly care technology must not only assess ethical aspects but also cybersecurity-legal compliance of all areas of the business concept. This was an emerging theme in practically all the interviews.

In the use of assistive software solutions, Solita Health Sidekick is a tool providing support in trauma psychotherapy, especially between live sessions with therapists. Privacy and cybersecurity were the key considerations in developing the solution. Due to the highly sensitive and private nature of the data, the developers decided to implement the tool as a stand-alone software. In other words, all user data is stored in the user's own mobile device. No private data is sent from the user either to his/her therapist, or the software vendor. Only population level mass-data is collected for product development, such as how many users use a certain feature of the therapy support tool. The user interface and visual appearance of the software was developed so that it does not look like a psychotherapy tool, so as not to stigmatize a person as someone requiring mental wellbeing services, should he/she use it in a public place. When the user has a live session with his/her therapist the user can review personal notes from the software and choose what he/she wishes to share with the therapist. As one of the interviewees described:

> "*In concept development of this software tool we discussed what would be the worst case scenarios of person's psychotherapy information being hacked.. and it could even lead to a suicide. This is why we decided all data should only stay in the client's mobile device. This eliminates cybersecurity concern in*

data transmission and assures privacy, leaving client with full control what information he/she wishes to share with his/her therapist.

4.3 Synthesis of key findings

This chapter has presented the findings of the study, general observations, and provided practical narratives to highlight the key results, while avoiding over-interpretation. The aim of this research has been to seek answers for the three research questions presented in Chapter one. One of the key observations was that, despite the companies in this empirical research providing very different assistive technology solutions, all the interviewees brought out similar experiences, when cybersecurity and ethics were discussed. No company had a designated ethical advisor, but all the organizations mentioned ethics being a key concern, especially because their client base included elderly citizens. The three research questions were found to be highly interrelated and interlinked, which gives strong support to the usability of the conceptual model for analysing ethical aspects of cybersecurity in healthcare (Figure 2) by Rajamäki & Hämäläinen (2021). Below table (Table 1) presents a summary of key findings per research questions.

Question 1: How do respect for autonomy and informed consent reflect in gerontechnology usage?	• Finnish gerontechnology solution providers are highly sensitive to respecting the elderly decision-making capacities. • Using gerontechnology can put the basic rights of elderly people at risk, and legislative frameworks typically mandate companies to seek informed consent from the end users because of the sensitive nature of the health data collected, transmitted and stored.
Question 2: What age-related ethical friction and conflicts arise in the application of networked health technology products/services?	• Securing informed consent from elderly with mild cognitive impairment requires ethical sensitivity. • Debilitating conditions emerge gradually, and some of them affect cognitive functions, requiring involving caregivers and other stakeholders into the decision making on assistive technology use. • Solution providers are sensitive to avoid stigmatizing their users as elderly. Efforts are made to narrow any perceived digital divide.
Question 3: How do privacy issues, which are both a core value cluster in cybersecurity and desiredata in ICT in healthcare, manifest in the use of networked health technology?	• Transition to the use of networked health technology has created conflicts between privacy protection and usability, forcing a trade-off between desiredata of ICT in health and core value of cybersecurity. • Privacy issues were in some cases critical guiding principles already in health technology solutions' concept development phase. • Privacy was found to be strongly interlinked with autonomy and informed consent (question 1).

Table 1: Summary of key findings

5 Summary, Discussion and Conclusion

This research found that respect for autonomy and informed consent are fundamental values in gerontechnology use in Finland, and product/service providers are very sensitive to respecting these values. Age-related ethical concerns were, however, raised by the interviewees especially in securing informed consent for gerontechnology use from elderly with mild cognitive impairment. Organizations in the empirical study were found to be very tuned to both the debilitating conditions their customer base has as well as to their level of technology literacy. Privacy was found to be a key cybersecurity concern in all the gerontechnology use due to high perceived value of private healthcare data and legal requirements.

Both the adoption of and product/concept development in assistive technologies was found to be strongly influenced by cybersecurity, ethical and legislative (compliance) considerations. In this respect, the conclusions can be summarized in Figure 4 below, where gerontechnologies must meet all the three dimensions.

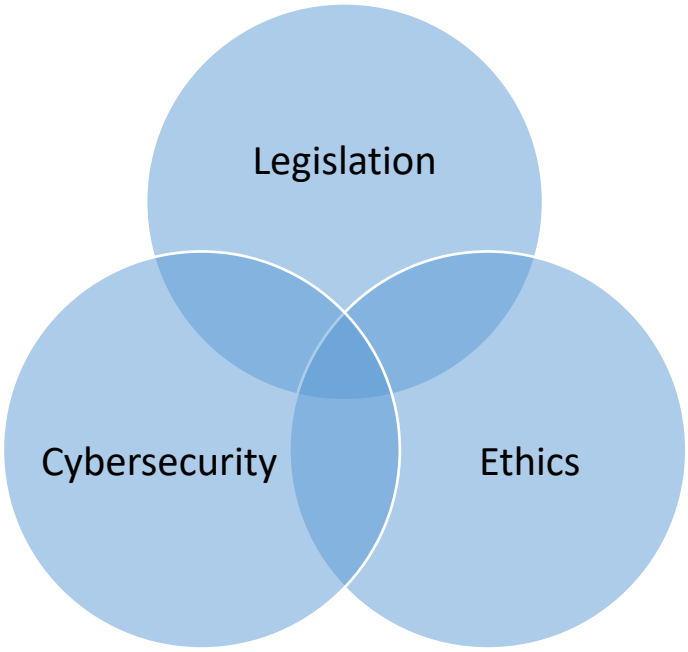

Figure 4: Key overlapping dimensions manifesting in assistive elderly care technologies

Assistive technologies, especially certified medical devices, were also found to be under significantly more scrutiny in these dimensions when compared with daily consumer electronics with similar functionalities. For instance, parents using smartphones often enable location services to track their children or share location data with friends for safety purposes when using Uber rides overseas. Not much though is given to sharing private data, or the cybersecurity aspect therein.

More research utilizing a cross-disciplinary approach in analyzing digital solutions facilitating elderly autonomy is needed in order to develop supportive frameworks and tools for product developers in this realm, especially as developers are facing significant trade-offs between security and usability/accessibility, as well as convenience and privacy. Of note, legal sensitivity to privacy concerns is varied, with the European General Data Protection Regulation imposing strong restrictions and punitive measures to any party engaging with data pertaining to European citizens, while the data of individuals in the Americas and Asia is less subject to regulation. With a view to the above, the results of this paper support earlier research (Rajamäki 2022, Loi et al 2019) highlighting how broad scale sharing of medical records and health information enables better services but can compromise privacy. The results of this paper also support findings by Christen et al (2017) that, especially in the case of electronic health records, there are cybersecurity value conflicts regarding usability and accessibility, social justice and equality. For instance, cybersecurity requirements can be so stringent that only technologically literate users are able to fully harness the benefits of the networked health care service, which broadens the digital gap and leads to social injustice. And, finally, access to the electronic health information can be so well protected from the cybersecurity reason that it doesn't enable the patient/client to manage their own information, or affect the decision-making based on that information, which in turn has a negative impact on patient/client autonomy.

Digital ageism refers to the prejudices faced by the elderly in the digital world (Rosales and Fernandez-Ardevol 2020). The results of this paper do not give support to the notion that a noticeable age-based digital divide in elderly care exists in Finland. Moreover, this paper leans support on the notion that researchers should aim to avoid digital ageism, especially the presupposition that age related digital divide applies universally across digital technology awareness and adoption. Results on wearable GPS trackers, however, indicated that gerontechnologies can contain stigmatizing symbolism, which may initially prevent some elderly users from adopting them. The results support similar findings by Landau and Werner (2012). On the notion of elderly cybersecurity awareness and how elderly online security behaviour reflects on the use assistive technologies the results were inconclusive. A behavioural focus-group study design will likely answer such questions better.

When technologies facilitating elderly autonomy are used appropriately, they have the potential to improve safety, independence and psychophysical wellbeing of the elderly, ultimately supporting the desire of senior citizens for aging at home. For organizations providing gerontechnology solutions and applications, their ability to respond to ethical concerns and navigate the legal and cybersecurity requirements will be a critical success factor in this multibillion-euro industry.

5.1 Suggestions for further research

With the increasing adoption of assistive technologies to support the rapidly aging population, more understanding of the ethical and cybersecurity landscape of gerontechnology is needed. Future research in this area could focus on in-depth case studies on individual companies providing technological solutions for elderly care in Finland. Another area, where there is a clear research gap is benchmarking which elderly care digital solutions developed, for instance, in Japan could be applied in Finland. Both countries are highly technologically developed and exhibit similar population demographics. A macro-approach would also, possibly, be applying the conceptual model for analysing ethical aspects of cybersecurity in healthcare (Figure 2) into the new features of Kanta services. More specifically, Omatietovaranto option in the Kanta services enables the user to upload and share health data that he/she has personally collected with, for instance, commercially available wearable device with healthcare providers. This is a pioneering development essentially making end users health data collectors (custodians of their own health) and warrants further cybersecurity-ethical research. Finally, quantitative research methods can be applied to a broad sample of end users in order to further explore validity of the findings of the present study. However, in all studies of the end user population, special emphasis should be on research ethics. More specifically, it is of paramount importance to obtain informed consent of the elderly, who may in some way be dependent on caregivers or have a diminished cognitive capacity.

5.2 Limitations

Although the present research provides important findings towards benefiting the field of medical ethics, gerontechnology, and healthy aging at home, it is not without limitations. This is a study carried out with a small number of subject matter experts from four different companies with varying healthcare product and service offerings. Semi-structured interviews were employed for data collection. In comparison to written surveys, qualitative interviews have the advantage of being interactive and allowing for unexpected topics to emerge and to be taken up by the researcher (Busetto, Wick & Gumbinger 2020). It cannot, however, be excluded that the study participants discussed ethical and cybersecurity issues that they felt the interviewer was interested in capturing. Thus, other cybersecurity-ethical issues critical for this field may have remained undiscussed. Also of note, this study did not interview end-users or their caregivers. Therefore, the findings are based only on one stakeholder group, gerontechnology product/service providers, and not comprehensive of all possible stakeholders engaged in this topic. Finally, Shenton (2004) has argued that it is easy for researchers to develop a preoccupation with validity and transferability, but the results of a qualitative study must, ultimately be understood within the context of the particular

characteristics of the organisation or organisations and, perhaps, geographical area in which the empirical study was carried out.

References

Printed

Beauchamp, T.L. and Childress, J.F. 1979. Principles of Biomedical Ethics. New York: Oxford University Press.

Ghauri, P., Grønhaug, K. & Strange, R. 2020. Research Methods in Business Studies. 5th ed. Cambridge: Cambridge University Press.

Yin, R.K. 2017. Case Study Research and Applications: Design and Methods. 6th edition. Thousand Oaks. California: Sage Publications.

Electronic

AARP. 2016. Home Matters: Aging in Place Housing Survey. Accessed 28.4.2022. https://states.aarp.org/virginia/home-matters-survey

AddSecure. 2022. Safe on the go. Accessed 28.4.2022. https://www.addsecure.com/smart-care-mo-start-page/safe-on-the-go/

Biener, C., Eling, M. & Wirfs, J.H. 2014. Insurability of Cyber Risk: An Empirical Analysis. The Geneva Papers on Risk and Insurance - Issues and Practice, 40, pp.131–158. Accessed 28.4.2022. https://www.researchgate.net/profile/Christian-Biener/publication/265727415_Insurability_of_Cyber_Risk_An_Empirical_Analysis/links/5419c6170cf25ebee9888001/Insurability-of-Cyber-Risk-An-Empirical-Analysis.pdf

Bouma, H., Fozard, J.L., Bouwhuis, D. & Taipale, V. 2007. Gerontechnology in perspective. Gerontechnology, 6, 190-216. Accessed 28.4.2022. https://doi.org/10.4017/GT.2007.06.04.003.00

Busetto, L., Wick, W. & Gumbinger, C. 2020. How to use and assess qualitative research methods. Neurological Research and Practice. 2, 14. Accessed 28.4.2022. https://doi.org/10.1186/s42466-020-00059-z

Business Finland 2021. Smart Life Finland Project. Accessed 28.4.2021. https://www.businessfinland.fi/en/for-finnish-customers/services/programs/smart-life-finland

Butt, S.A., Elhadjamor, E.A., Pappel, I., Õunapuu, E. & Draheim, D. 2021. A Knowledge Map for ICT Integration in the Silver Economy. Procedia Computer Science, 181, pp.693–701. Accessed 28.4.2022. https://www.sciencedirect.com/science/article/pii/S1877050921002635

Britannica 2022. Definition of stereotype. Accessed 28.4.2022. https://www.britannica.com/dictionary/stereotype

Carlton, M. & Levy, Y. 2017. Cybersecurity skills: the cornerstone of advanced persistent threats (APTs) mitigation. Online Journal of Applied Knowledge Management, Vol. 5 No. 2, pp. 16-28. Accessed 28.4.2022. https://www.iiakm.org/ojakm/articles/2017/volume5_2/OJAKM_Volume5_2pp16-28.pdf

Christen M., Gordijn B., Weber K., Van de Boel, I. & Yaghmaei E. 2017. A review of value-conflicts in cybersecurity. ORBIT J 1. Accessed 28.4.2022. https://doi.org/10.29297/orbit.v1i1.28

Chung J., Demiris G. & Thompson HJ. Ethical considerations regarding the use of smart home technologies for older adults: an integrative review. Annual Review of Nursing Research 2016; 34: 155–181. Accessed 28.4.2022. https://doi.org/10.1891/0739-6686.34.155

Coboi, A., Tran, T., Tran, S. & Nguyen, M. 2021. Security Problems in Smart Homes. ICSES Transactions on Computer Networks and Communications, Vol. X, No. Y, September, 2021. Accessed 28.4.2022.
https://www.researchgate.net/publication/354859434_Security_Problems_in_Smart_Homes

Ellis, K. 2005. Society's Most Vulnerable Under Surveillance: The Ethics of Tagging and Tracking Dementia Patients With GPS Technology: A Comparative View. Accessed 28.4.2022.
https://ouclf.law.ox.ac.uk/societys-most-vulnerable-under-surveillance-the-ethics-of-tagging-and-tracking-dementia-patients-with-gps-technology-a-comparative-view/

Gerontechnologist 2022. 2021 Age Tech Market Map. Accessed 28.4.2022.
https://www.thegerontechnologist.com/wp-content/uploads/2021/03/2021-AgeTech-Market-Map-3.pdf

Federal Bureau of Investigation. 2021. FBI Releases 2020 Internet Crime Report. Accessed 28.4.2022. https://www.fbi.gov/contact-us/field-offices/anchorage/news/press-releases/fbi-releases-2020-internet-crime-report

Federal Bureau of Investigation. 2020. Elder Fraud. Accessed 28.4.2022
https://www.fbi.gov/scams-and-safety/common-scams-and-crimes/elder-fraud

Fujitsu. 2022. Healthcare division introduction. Accessed 28.4.2022.
https://www.fujitsu.com/au/solutions/industry/healthcare/

General Data Protection Regulation (GDPR). 2013. General Data Protection Regulation (GDPR). Accessed 28.4.2022. https://gdpr-info.eu

Halminen, O. 2016. Kuolevien kustannukset Suomessa – ikääntyvän väestön sosiaali- ja terveydenhuoltokustannukset kuoleman lähestyessä. Accessed 28.4.2022.
http://urn.fi/URN:NBN:fi:aalto-201611025483

Halminen, O., Linna, M. Silander, K., Mikkola, T. Tyni, T., Koivuranta, P. & Hörhammer, I. 2019. Iäkkäiden ympärivuorokautiseen hoitoon siirtymisen riskitekijät. Accessed 28.4.2022.
http://shop.kuntaliitto.fi/product_details.php?p=3565

Hood, C. 2021. Telehealth Cybersecurity. Oxford University Press. Accessed 28.4.2022.
https://doi.org/10.1093/med/9780190066475.003.0007

Kaplan, B. 2020. Revisiting Health Information Technology Ethical, Legal and Social Issues. Evaluation: Telehealth/Telemedicine and Covid-19. International Journal of Medical Informatics, Volume 143, 2020, 104239, ISSN 1386-5056. Accessed 28.4.2022.
https://doi.org/10.1016/j.ijmedinf.2020.104239

KELA. 2022. Information Services - Kanta Services. Accessed 28.4.2022.
https://www.kela.fi/web/en/information-services-kanta

Krueger, D., Lukaszewski, K. & Stone, D. 2018. Age and the Digital Divide. Accessed 12.1.2022.
https://www.researchgate.net/publication/325437066_Age_and_the_Digital_Divide

Kyberturvallisuuden nykytila, tavoitetila ja tarvittavat toimenpiteet tavoitetilan saavuttamiseksi. 2017. Valtioneuvoston kanslia. Valtioneuvoston selvitys- ja tutkimustoiminnan julkaisu 30/2017. Accessed 28.4.2021.
https://tietokayttoon.fi/julkaisu?pubid=17805

Laki sosiaali- ja terveydenhuollon asiakastietojen sähköisestä käsittelystä. 2021. Finlex. Accessed 28.4.2022. https://www.finlex.fi/fi/laki/alkup/2021/20210784

Landau, R. & Werner, S. 2012. Ethical aspects of using GPS for tracking people with dementia: recommendations for practice. International Psychogeriatrics. 2012 Mar;24/3:358-66. Accessed 28.4.2022. http://dx.doi.org/10.1017/S1041610211001888

Lodha, P. & De Sousa, A. 2020. Ethics of electronic tagging of dementia patients. Indian Journal of Medical Ethics, V1, 83-84. Accessed 28.4.2022. https://ijme.in/articles/ethics-of-electronic-tagging-of-dementia-patients/

Loi M, Christen M, Kleine N. & Weber K. 2019. Cybersecurity in health - disentangling value tensions. Journal of Information, Communication and Ethics in Society. 2019.17: 229-245. Accessed 28.4.2022. https://doi.org/10.1108/JICES-12-2018-0095

Marseille, E. & Kahn, J.G. Utilitarianism and the ethical foundations of cost-effectiveness analysis in resource allocation for global health. Philosophy, Ethics and Humanities in Medicine 14, 5, 2019. Accessed 28.4.2022. https://doi.org/10.1186/s13010-019-0074-7

Milkovich, D. 2018. 13 Alarming Cyber Security Facts and Stats | Cybint. Accessed 28.4.2022. Cybint Solutions - A BARBRI Company. https://www.cybintsolutions.com/cyber-security-facts-stats/

Morrison BA., Coventry L. & Briggs P. 2020. Technological Change in the Retirement Transition and the Implications for Cybersecurity Vulnerability in Older Adults. Frontiers of Psychology. 11:623. Accessed 28.4.2021. https://doi.org/10.3389/fpsyg.2020.00623

My Kanta. 2022. My Kanta Architecture. Accessed 28.4.2022. https://www.kanta.fi/documents/20143/106828/Kanta-arkkitehtuuri+ja+terveydenhuollon+yhteentoimivuuden+ja+IT-standardoinnin+aikajana+EN.pdf/6d93272e-b29b-1f86-423d-796ab8ee5e45

Oikeus.fi. 2022. Applying for a guardian. Accessed 28.4.2022. https://oikeus.fi/edunvalvonta/en/index/applyingforaguardian.html

Oliver Wyman Forum. 2021. Cyber Risk Literacy and Education Index. Oliver Wyman Forum. Accessed 28.4.2022. https://www.oliverwymanforum.com/cyber-risk/cyber-risk-literacy-education-index.html#

Oracle 2022. What is IoT. Accessed 28.4.2022. https://www.oracle.com/se/internet-of-things/what-is-iot/

Rajamäki, J. 2022. Cybersecurity value conflicts in coping at home health technology: Design science research towards ethical decision-making. Finnish Journal of eHealth and eWelfare, 14, pp. 43–60. Accessed 28.4.2022. https://doi.org/10.23996/fjhw.111774

Rajamäki, J. & Hämäläinen, H. 2021. Ethics of Cybersecurity and Biomedical Ethics: Case SHAPES." Information & Security: An International Journal 50, no. 1. 2021. pp 103-116. Accessed 28.4.2022. https://doi.org/10.11610/isij.5002

Rosales, A. & Fernández-Ardèvol, M. 2020. Ageism in the era of digital platforms. Convergence: The International Journal of Research into New Media Technologies, 26, pp.1074-1087. Accessed 28.4.2022. https://doi.org/10.1177/1354856520930905

Science Daily 2022. Definition of bioethics. Accessed 28.4.2022. https://www.sciencedaily.com/terms/bioethics.htm

SHAPES. 2021. Digital Solutions Overview. Accessed 28.4.2022. https://shapes2020.eu/about-shapes/

Shenton, A. 2004. Strategies for Ensuring Trustworthiness in Qualitative Research Projects. Education for Information. 22. 63-75. Accessed 28.4.2022. https://www.researchgate.net/profile/Andrew-Shenton/publication/228708239_Strategies_for_Ensuring_Trustworthiness_in_Qualitative_Research_Projects/links/56cd506808ae85c8233bc986/Strategies-for-Ensuring-Trustworthiness-in-Qualitative-Research-Projects.pdf?origin=publication_detail

Solita. 2022. Solita Health. Accessed 28.4.2022. https://www.solita.fi/en/solita-health/

Statista. 2021. Countries with the oldest population 2020. Accessed 28.4.2022. https://www.statista.com/statistics/264729/countries-with-the-largest-percentage-of-total-population-over-65-years/

Sundgren, S., Stolt, M. & Suhonen, R. 2019. Ethical issues related to the use of gerontechnology in older people care: A scoping review. Nursing Ethics. Accessed 28.4.2022. https://journals.sagepub.com/doi/full/10.1177/0969733019845132

Tenny, S., Brannan, G. D., Brannan, J. M., & Sharts-Hopko, N. C. 2021. Qualitative Study. In StatPearls. StatPearls Publishing. Accessed 28.4.2022. https://www.ncbi.nlm.nih.gov/books/NBK470395/

Tietosuojavaltuutetun toimisto. 2022. Impact assessments | Data Protection Ombudsman's Office. Accessed 28.4.2022. https://tietosuoja.fi/en/impact-assessments

Tilastokeskus. 2021. Väestö. Accessed 28.4.2022. https://www.tilastokeskus.fi/tup/suoluk/suoluk_vaesto.html#V%C3%A4kiluvun%20kehitys

van de Poel, I. 2020. Core Values and Value Conflicts in Cybersecurity: Beyond Privacy Versus Security. In: Christen, M., Gordijn, B. & Loi, M. The Ethics of Cybersecurity. The International Library of Ethics, Law and Technology, vol 21. Springer, Cham. Accessed 28.4.2022. https://doi.org/10.1007/978-3-030-29053-5_3

Von Solms, R. and van Niekerk, J. 2013. From information security to cyber security. Computers & Security, 38, pp.97–102. Accessed 28.4.2022. https://profsandhu.com/cs6393_s16/solms-2013.pdf

Wang S., Bolling K., Mao W., Reichstadt J., Jeste D., Kim HC. & Nebeker C. 2019. Technology to Support Aging in Place: Older Adults' Perspectives. Healthcare. 2019 Apr 10;7. Accessed 28.4.2022. https://doi.org/10.3390/healthcare7020060

Wangmo, T., Lipps, M., Kressig, R.W. & Ienca, M. 2019. Ethical concerns with the use of intelligent assistive technology: findings from a qualitative study with professional stakeholders. BMC Med Ethics 20, 98. Accessed 28.4.2022. https://doi.org/10.1186/s12910-019-0437-z

Wass S., Vimarlund V. & Ros A. 2019. Exploring patients' perceptions of accessing electronic health records: innovation in healthcare. Health Informatics J 2019 March; 25. pp. 203-215. Accessed 28.4.2022. https://doi.org/10.1177/1460458217704258

World Health Organization. 2010. Opportunities and developments: Telemedicine in Member States Report on the second global survey on eHealth Global Observatory for eHealth series - Volume 2 2010. Accessed 28.4.2022. https://www.who.int/goe/publications/goe_telemedicine_2010.pdf

Wu Y., Damnée S., Kerhervé H., Ware C. & Rigaud A. 2015. Bridging the digital divide in older adults: a study from an initiative to inform older adults about new technologies. Clinical Interventions in Aging. 2015;10:193-201. Accessed 28.4.2022. https://doi.org/10.2147/CIA.S72399

Yaghmaei E., Van de Poel I., Christen M., Gordijn B., Kleine N., Loi M., Morgan G. & Weber K. Canvas White Paper 1 – Cybersecurity and Ethics. 2017. Accessed 28.4.2022. http://dx.doi.org/10.2139/ssrn.3091909

Figures

Appendices

Appendix 1: Interview Guide

Interview topics

1. The interviewee´s background data (confidential).
2. Company/organization product/service offering.
3. How do you take into account that the elderly (over 65-year-old) have equal opportunity to use your product/service?
4. Do respect for autonomy and informed consent reflect in your product/service adoption? If so, how?
5. Have you identified any age-related ethical friction or conflicts in the application of your networked health technology products/services? Examples?
6. How do cybersecurity considerations manifest in the use of your networked health technology?
7. How does the fact that end users are (vulnerable, possibly not tech literate) elderly affect your cybersecurity considerations regarding your product/service?
8. Have you met ethical concerns? If so, what kind? Examples?
9. How are gerontechnology end users taken into account in the product/service design process? Do you, for instance, employ ethical advisors?

Appendix 2: Example of categorizing companies in the gerontechnology market.

Figure 5: Categorization of companies in the gerontechnology market (Gerontechnologist 2021).