Information & Security

J. Rajamäki & H. Hämäläinen
vol. 50, no. 1 (2021): 103-116
https://doi.org/10.11610/isij.5002

Published since 1998

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Ethics of Cybersecurity and Biomedical Ethics: Case SHAPES

JyriRajamäki (✉), *Heikki Hämäläinen*

Laurea University of Applied Sciences, https://www.laurea.fi/en/

ABSTRACT:

The SHAPES Horizon 2020 project supports the wellbeing of the elderly at home. The object of this paper is to help to provide necessary tools and guidelines to health and wellbeing service developers in the SHAPES project for their ethical consideration of cybersecurity actions. This paper examines different views and approaches to the ethics of cybersecurity in healthcare and finds the most relevant and puzzling issues for the SHAPES project. The paper investigates the ethical issues, for example, applying the approach of principlism based on four principles of biomedical ethics (respect for autonomy, nonmaleficence, beneficence and justice) and ethics of care. The essential aims of the employment of information and communication technology in healthcare are efficiency and quality of services, the privacy of information and confidentiality of communication, the usability of services, and safety. Four significant value clusters in cybersecurity are security, privacy, fairness, and accountability. From these four different ethical aspects (biomedical ethics, ethics of care, core value clusters in cybersecurity, and technical aims), this paper proposes a new conceptual model for a system approach to analyse the ethical matters which are related to cybersecurity in digital healthcare and wellbeing. In addition, the paper provides ethical guidelines from a cybersecurity ethics and biomedical ethics perspective for the SHAPES project.

ARTICLE INFO:

RECEIVED: 07 JUNE 2021
REVISED: 22 AUG 2021
ONLINE: 08 SEP 2021

KEYWORDS:

ethics; cybersecurity; biomedical ethics; digital healthcare; SHAPES project; healthy ageing; wellbeing

✉ Corresponding Author: E-mail: jyri.rajamaki@laurea.fi

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 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 growing complexity of the digital ecosystem, in combination with increasing global risks, involves various ethical issues associated with cybersecurity. An important dilemma is that overemphasising cybersecurity may violate fundamental values such as equality and fairness, but on the other hand, neglecting cybersecurity could undermine citizens' trust and confidence in the digital infrastructure, policymakers and state authorities. One example of ethical issues concerning health and wellbeing is that if a medical implant producer protects the data transfer between the implant and receiver server utilising suitable cryptology, this significantly increases the energy consumption of the implant and frequently requires more surgeries for battery exchange.[1]

Digital transformation and ecosystem thinking steer the Smart and Healthy Ageing through People Engaging in Supportive Systems (SHAPES) Horizon 2020 project that supports the wellbeing of the elderly at home. From an ethics point of view, SHAPES is a diverse solution, and ethical requirements and their implementation are essential for the sustainability of SHAPES. The implementation of ethical requirements has an impact not only on technical solutions and services but also on the organisational arrangements of SHAPES. Alongside user requirements, ethical requirements are particularly important when developing solutions linked to fundamental rights and when the target group is older persons.[2]

This study is part of the SHAPES project. The aim of this paper 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 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.

The paper is structured as follows. After the introduction, the literature review investigates four different ethical aspects related to cybersecurity in digital healthcare and wellbeing: biomedical ethics, ethics of care, core value clusters in cybersecurity, and technical aims of Information and Communication Technology (ICT) systems in healthcare. The third section proposes a new conceptual model for a systematic analysis of relations between these different ethical aspects. The fourth section presents ethical guidelines for the SHAPES project from four viewpoints; privacy, autonomy, consent and beneficence. The last section concludes the paper and discusses future work.

Ethical Frameworks Related to Digital Healthcare and Well-Being

Core Values in Cybersecurity

According to van de Poel,[3] four important value clusters exist that should be considered when deciding on cybersecurity measures. The first one, 'security,' is a combination of more specific values, such as individual security, national resilience and information security. These values protect humans and other valuable entities from all kinds of harm and respond to morally problematic situations in which harm is done, ranging from data breaches and loss of data integrity to cybercrime and cyberwarfare.[3]

The second value cluster, 'privacy,' contains such values as privacy, moral autonomy, human dignity, identity, personhood, liberty, anonymity and confidentiality. According to van de Poel,[3] these values correspond to the following norms: "we should treat others with dignity, we should respect people's moral autonomy, we should not store or share personal data without people's informed consent, and we should not use people (or data about them) as a means to an end." Moral problems with these values include the secret collection of large amounts of personal data for cybersecurity purposes or the unauthorised transfer of personal data to a third party.[3]

The third cluster, 'fairness,' consists of values such as justice, fairness, equality, accessibility, freedom from bias, non-discrimination, democracy and the protection of civil liberties. These values respond to the fact that cybersecurity threats, or measures to avoid them, do not affect everyone equally, being sometimes morally unfair. Another moral problem is that cybersecurity threats, or measures to increase cybersecurity, may undermine democracy, civil rights and liberties. Moral reasons that correspond to these values are that people should be treated fairly and equally, and democratic and civil rights should be upheld.[3]

The fourth cluster, 'accountability,' includes values such as transparency, openness and explainability. If governments take cybersecurity measures that harm citizens and require the weighing of a range of conflicting substantive values such as security, privacy and fairness, then accountability, as a more procedural value, is particularly relevant.[3]

In addition to the four value clusters, some domain-specific ethical principles and values are different from domain to domain, and technical aims can be different even from application to application. They are connected to a range of instrumental or technical values related to the proper functioning of applications, such as efficiency, ease of use, understandability, data availability, reliability, compatibility and connectivity. However, technical values are morally relevant as they are instrumental for achieving moral values.[3]

Ethical Frameworks for Cybersecurity

Cybersecurity ethics is an interdisciplinary 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.[4]

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.[4]

Principlism

Commonly known ethical frameworks should also be considered when looking into cybersecurity ethics. 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 the good for 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 the difficult task of weighing these principles against each other when trade-offs occur.[5]

From a cybersecurity perspective, the respect principle should be observed in all cases in which data may relate to identifiable personal data, for example, communication between persons and ID addresses. Respect also involves all research done where consent is requested from a person in some experimental research on human factors in cybersecurity.[5]

The benefit principle (to pursue the good of others) generally applies to cybersecurity research, meaning it should maximise benefit and minimising harm. When minimising harm, one needs to consider a broad set of risks for persons, including emotional, reputational, financial and physical harm.[5]

The justice principle is aiming to distributing an equal amount of benefits for all stakeholders. Justice in research implies that research should be designed in a way that a group of people do not benefit more from the research than others.[5]

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 imply that priorities need to be given. 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.[5]

Protecting the security of 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 to human rights, for example, when collecting personal data for authentication purposes. In addition, cases where the goal is to enhance cybersecurity by monitoring traffic and possible cyberattacks might infringe directly on human rights. Cybersecurity might conflict with human rights in some cases; therefore, balance is required. 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.[5]

Utilitarianism

Utilitarianism allows for the possibility of situational ethics, meaning that in some circumstances, one might need to violate a society's or a personal moral code if the outcome is better for a greater number of people. Utilitarianism always aims for the decision with the highest pay-off or the highest utility.[4]

From a cybersecurity perspective, the utilitarian approach can be hard to define. One might encounter the debate whether individuals should be treated on the basis of different norms and morals in the cybersecurity space than in normal life. In addition, it should be defined if "good" in normal life equals the same from 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 negative impacts like death, pain or disability. Maximising the goods should also be looked at from a longer time perspective to avoid unpleasant outcomes long-term.[4]

Biomedical Ethics

Biomedical ethics is an interdisciplinary, contemporary ethical approach based on Beauchamp and Childress's [6] four main principles: justice, beneficence, nonmaleficence, and autonomy. It serves as a paradigm that assists healthcare professionals and public policymakers to identify and respond to moral dilemmas in biomedical and healthcare research and encompasses different types of moral norms: moral ideals, virtues, rules, and principles. Principles are considered general norms, and they leave considerable space for judgement in several cases. Principles do not function as 'precise action guides' that would inform us in every single circumstance on how to act the same way as detailed judgements and rules would guide. The principles are rather abstract, and they do not form a general moral theory but a framework to identify and reflect on moral problems.[2]

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 age or location, have the same access to healthcare services?" Many principles of justice in a biomedical ethics point of view are not distinct and independent of other principles, such as beneficence and nonmaleficence.[6]

Beneficence

Beneficence and nonmaleficence 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 kinds of actions, where the intention is to help others.[6]

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 bringing benefit to the individual. The 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.[6]

Nonmaleficence

Nonmaleficence is the principle, which asserts an obligation not to do harm to others. Healthcare professionals often invoke this 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 recognise nonmaleficence, and it is often combined with the beneficence principle, which is covered in the next chapter.[6]

The principle of nonmaleficence can be seen quite broad, and it supports many other more specific moral rules, such as "do not kill" and "do not cause pain or suffering." Nonmaleficence 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.[6]

Autonomy

Autonomy in a biomedical ethic setting refers to respecting the decision-making capacities in the healthcare of individuals. Decision-making in such a setting especially includes informed consent and refusal. Personal autonomy in biomedical ethics is at least 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.[6]

Ethics of Care

The care sector applies 'Ethics of care' based on Gilligan's ideas [7] that there are two different types of moralities: the ethic of justice and the ethic of care. Gilligan explains, "the ethic of care is centred on maintaining relationships through responding to the needs of others and avoiding hurt."[7] Care ethics see moral problems arising from ruptures or tensions in relationships. Within care reasoning, moral problems are solved by considering the unique characteristics of situations and persons, more than applying a hierarchy of rights or rules; the latter would be more typical of a justice ethics approach. The nursing field greets Gilligan's theory with enthusiasm, as it has theoretically captured the essence of caring embedded in patient-nurse relationships and explained the ethical difficulties nurses encountered in medically dominated healthcare contexts.[8] It is a promising approach to strengthen the voices of nurses in ethical discussions, in which justice-based theories traditionally dominate. Table 1 presents the main characteristics of care ethics in the SHAPES context.

Table 1. Main characteristics of care ethics.[2]

Perspectives	In the SHAPES context, especially
Empathy	Showing empathy might need new forms when acting on digital platforms: e.g., a smile, touch and eye contact might not work as in traditional face-to-face encounters – this applies to caregivers, researchers and older persons.
Relationships	Building and maintaining relationships might mean learning new methods and forms when acting on digital platforms. Building and maintaining relationships also means an understanding of, e.g., psychology, sociology and spirituality of human beings.
Uniqueness of the case	In hectic working life, it might not always be easy to provide care, as the case is unique and not just one of a dozen similar-looking ones.

Desiderata of ICT in Health and the Instrumental Role of Cybersecurity

Four main functions of ICT systems in healthcare are: improving the quality and efficiency of services, protecting confidentiality, enhancing usability, and protecting patients' safety. Weber and Kleine summarise these functions as follows:[9]

- "One of the main purposes of ICT systems in healthcare is the administration of information to increase the *efficiency* of the healthcare system and to reduce its costs. Improvements in healthcare in *qualitative* terms refer, for instance, to new services that provide treatment or processes with better health-related outcomes. Big Data, the collection and sharing of as much health-related data as possible might be used to establish new insights regarding diseases and possible treatments."
- "Using ICT to process patient data creates a moral challenge in terms of quality on the one hand and *privacy* and confidentiality on the other hand—yet both are important aims in healthcare. In particular, privacy is often seen as a prerequisite of patients' autonomy"... "Privacy and confidentiality are also foundations of trust among patients on the one hand and healthcare professionals on the other."
- Roman, et al.[10] define *usability* as the degree of effectiveness, efficiency, and satisfaction with which users of a system can realise their intended task. Concerning health, users include patients, medical staff and/or admin-

istrators, which have different degrees of ICT competences, depending on personal attitudes and socio-demographic variables.[9]

- "*Safety* can be defined as the reduction of health-threatening risks. Safety, quality, efficiency and usability are interrelated, but they do not align, because safety measures might reduce the efficiency and usability of services and therefore quality."

The instrumental role of cybersecurity in healthcare is to protect against three types of threats based on the target of the attack: threats against information, information systems and medical devices.[11]

Conceptual Model for Systematic Analysis of the Ethics of Cybersecurity in Healthcare

Figure 1 proposes a new conceptual model for a systematic relation analysis of ethical matters related to cybersecurity in digital healthcare and wellbeing. The systematic mapping of the relations between the four different ethical aspects (biomedical ethics [n=4], care ethics [n=3], core value clusters in cybersecurity [n=4] and technical aims [n=4]) generates 84 value pairs.

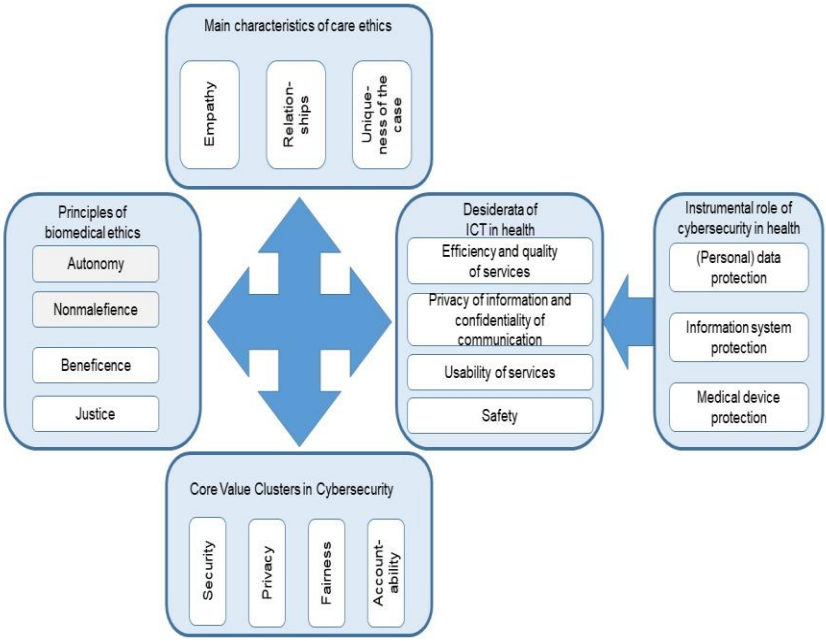

Figure 1: Conceptual model for analysing ethical aspects of cybersecurity in healthcare.

Ethical Guidelines for SHAPES Project

This section presents ethical guidelines for the SHAPES project from four viewpoints; privacy, autonomy, consent and beneficence. The guidelines are reflections and comparisons of known ethical frameworks from both a biomedical and cybersecurity ethics perspective. In the SHAPES context, different key stakeholders need to be taken into consideration when making ethical decisions, covering all aspects from software development to interaction between the platform and the end-user, as Figure 2 shows.

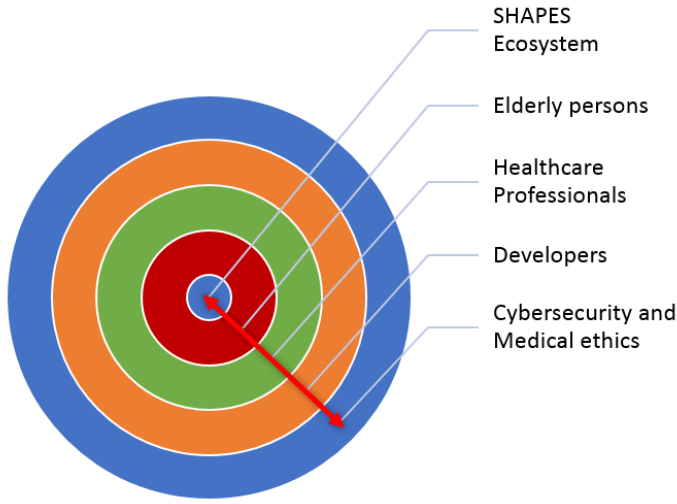

Figure 2: Stakeholder layers in Ethical decision-making in SHAPES project.

Ethical Guidelines for SHAPES Regarding Privacy

Health-related personal data is seen as one of the most sensitive forms of personal data. In the 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, no clear ethical core value would correlate to privacy, but one might face ethical dilemmas related to privacy when utilising the SHAPES ecosystem. Biomedical ethics aim closely at the wellbeing of the patient and drives action for the best result for the patient's physical health. Furthermore, in cases where healthcare professionals need to take action to prevent harm to 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 the medical procedure is carried through.

The ethical guidelines for SHAPES project regarding privacy might be summarized as follows:

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

Ethical Guidelines for SHAPES Regarding Autonomy

Autonomy is 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 relates 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, anonymity can be referred to as 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. In addition, the elderly should have the feeling of autonomy when living daily life. One example could be assistive technology such as a fall detector. When de-

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

The ethical guidelines for SHAPES project regarding autonomy are:

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

Ethical Guidelines for SHAPES 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 utilising already collected data for other purposes. In the 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. In addition, elderly people with not that much experience with technological devices might not be aware of the capabilities of data collecting and distributing, and hence consent should be requested in several different touchpoints.

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. Authorisation methods and verifying the consent given should be a part of the process.

The ethical guidelines for SHAPES project regarding consent are:

- Design and develop all functionalities so that consent is requested from the end-user on a regular basis.
- 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.

- 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.
- 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.

Ethical Guidelines for SHAPES 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 prohibit 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 maximising the good and treat each other with justice.

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

The ethical guidelines for SHAPES project regarding beneficence are:

- Every action and procedure made through or on the basis of information from the SHAPES ecosystem should aim at preventing harm and promoting good for the end-user.
- Collect feedback from the users to ensure that justified decisions to promote good have been made.
- When designing and developing SHAPES software, aim in all development to maximise good and minimise harm.
- Ensure that software is developed in a way that maximisation of good is achieved even without a human touch.
- Collect information of possible mistakes in the SHAPES ecosystem or decisions and revert this information transparently back to the development process.

Conclusions

Ethics is crucial in healthcare, and new eHealth services make ethical questions even more pressing and raise new ones, such as ethics of cybersecurity in healthcare.[9] Loi et al.[11] have investigated the relationship between ICT desiderata and the four principles of medical ethics and mapped trade-offs between the goals of cybersecurity into conflicts between the four principles of medical

ethics. A similar analysis is needed from the relations between (1) biomedical ethics vs ethics of care, (2) biomedical ethics vs core values in cybersecurity, (3) ethics of care vs technical aims, (4) ethics of care vs core values in cybersecurity, and (5) technical aims vs core values in cybersecurity. This paper proposes a conceptual model for a system approach to analyse ethical matters and provides ethical guidelines for SHAPES. However, the scoping is limited to provide ethical guidelines regarding biomedical and cybersecurity ethics to different stakeholders in interaction with the SHAPES ecosystem. Several opportunities remain for further research regarding the topic of ethical viewpoints in SHAPES context. Further research could be conducted in the form of analysis between processes carried over by a human versus processes carried over by a machine or artificial intelligence. SHAPES provide elderly people with the ability to stay home for a longer time and receive efficient treatment with respect for human life with the help of technological innovation and collaboration.

Acknowledgements

This work was supported by the SHAPES project, which has received funding from the European Union's Horizon 2020 research and innovation programme under the grant agreement no. 857159.

References

[1] Markus Christen, Bert Gordijn, and Michele Loi, "Introduction," in *The Ethics of Cybersecurity*, M. Christen et al. (Cham, Switzerland: Springer Nature, 2020), 1–8.

[2] Sari Sarlio-Siintola, ed., *SHAPES Ethical Framework D8.4,* Project "Smart and Healthy Ageing through People Engaging in Supportive Systems," 2020, https://shapes2020.eu/wp-content/uploads/2020/11/D8.4-SHAPES-Ethical-Framework.pdf.

[3] Ibo van de Poel, "Core Values and Value Conflicts," in *The Ethics of Cybersecurity,* edited by M. Christen et al. (Cham, Switzerland: Springer Nature, 2020), 45-72.

[4] Mary Manjikian, *Cybersecurity Ethics – An Introduction* (New York: Routledge, 2018).

[5] Markus Christen and Michele Loi, "Ethical Frameworks for Cybersecurity," in *The Ethics of Cybersecurity*, edited by M. Christen et al. (Cham, Switzerland: Springer Nature, 2020), 73–93.

[6] Tom Beauchamp and James Childress, *Principles of biomedical ethics* (New York: Oxford University, 2009).

[7] Carol Gilligan, *In a Different Voice: Psychological Theory and Women's Development* (Cambridge: Harvard University Press, 1982).

[8] Soile Juujärvi, Kirsi Ronkainen, and Piia Silvennoinen, "The Ethics of Care and Justice in Primary Nursing of Older Patients," *Clinical Ethics* 14, no. 4 (2019): 187–194, https://doi.org/10.1177/1477750919876250.

[9] Karsten Weber and Nadine Kleine, "Cybersecurity in Health Care," in *The Ethics of Cybersecurity*, edited by M. Christen et al. (Cham, Switzerland: Springer Nature, 2020), 139-156. Quotes on pp. 143-145.

[10] Lisette Roman, Jessica Ancker, Stephen Johnson, and Yalini Senathirajah, "Navigation in the Electronic Health Record: A Review of the Safety and Usability Literature," *Journal of Biomedical Informatics* 67 (2017): 69–79.

[11] Michele Loi, Markus Christen, Nadine Kleine, and Karsten Weber, "Cybersecurity in Health–disentangling Value Tensions," *Journal of Information, Communication and Ethics in Society* 17, no. 2 (2019): 229-245.

About the Authors

Jyri **Rajamäki** is Principal Lecturer in Information Technology at Laurea University of Applied Sciences and Adjunct Professor of Critical Infrastructure Protection and Cyber Security at the University of Jyväskylä, Finland. He holds D.Sc. degrees in electrical and communications engineering from Helsinki University of Technology and a PhD in mathematical information technology from University of Jyväskylä.

Heikki **Hämäläinen** is a graduate student at Laurea University of Applied Sciences, Finland.