doi: 10.34190/EWS.21.009

Ethics of Cybersecurity in Digital Healthcare and Well-Being of Elderly at Home

Jyri Rajamäki
Laurea University of Applied Sciences, Espoo, Finland
jyri.rajamaki@laurea.fi
DOI: 10.34190/EWS.21.009

Abstract: The SHAPES Horizon 2020 project supports the well-being of the elderly at home. 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 well-being is that if a medical implant producer protects the data transfer between implant and receiver server utilising suitable cryptology, this significantly increases the energy consumption of the implant and frequently requires more surgeries for battery exchange. The object of this work in progress paper is to help to provide necessary tools and guidelines to health and well-being 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 important 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 important 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 well-being.

Keywords: ethics, cybersecurity, digital healthcare, SHAPES project, healthy ageing, well-being

1. Introduction

Digital transformation and ecosystem thinking steer the Smart and Healthy Ageing through People Engaging in Supportive Systems (SHAPES) Horizon 2020 project that supports the well-being 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 (Sarlio-Siintola, 2020).

The paper is structured as follows. After the introduction, the literature review investigates four different ethical aspects related to cybersecurity in digital healthcare and well-being: 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 last section discusses future work.

2. Ethical frameworks related to digital healthcare and well-being

2.1 Core values in cybersecurity

According to van de Poel (2020), 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 (van de Poel, 2020).

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 (2020), 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 (van de Poel, 2020).

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 (van de Poel, 2020).

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 (van de Poel, 2020).

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 (van de Poel, 2020).

2.2 Biomedical ethics

Biomedical ethics is an interdisciplinary, contemporary ethical approach based on Beauchamp and Childress's (2009) four main principles: justice, beneficence, non-maleficence, 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 (Sarlio-Siintola, 2020).

2.3 Ethics of care

The care sector applies 'Ethics of care' based on Gilligan's (1982) ideas that there are two different types of moralities: the ethic of justice and the ethic of care. Gilligan (1982) explains, "the ethic of care is centred on maintaining relationships through responding to needs of others and avoiding hurt". 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" (Juujärvi, et al., 2019). 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 (Sarlio-Siintola, 2020)

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.

Perspectives	*In the SHAPES context, especially*
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.

2.4 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 (2020, 143-145) summarizes these functions as follows:

- 1. "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."
- 2. "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."
- 3. Roman, et al. (2017) define *usability* as the degree of effectiveness, efficiency, and satisfaction with which users of a system can realize their intended task. Concerning health, users include patients, medical staff and/or administrators, which have different degrees of ICT competences, depending on personal attitudes and socio-demographic variables (Weber & Kleine, 2020).
- 4. "*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 (Loi, et al., 2019).

3. 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 well-being. 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.

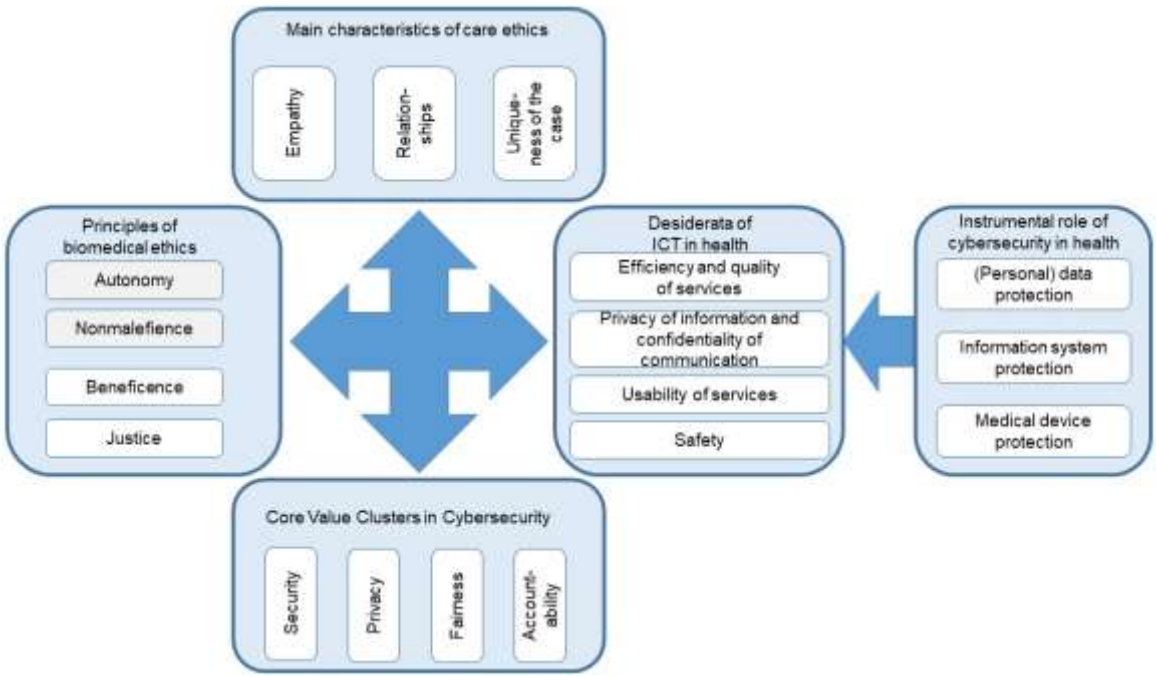

Figure 1: Conceptual model for analysing ethical aspects of cybersecurity in healthcare

4. Discussion

Ethics is crucial in healthcare and new eHealth services make ethical questions even more pressing and raises new ones, such as ethics of cybersecurity in healthcare (Weber & Kleine, 2020). Loi et al. (2019) have investigated the relation 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.

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

Beauchamp, T. & Childress, J. 2009. *Principles of biomedical ethics.* New York: Oxford University.

Gilligan, C. 1982. *In a Different Voice: Psychological Theory and Women's Development.* Cambridge: Harvard University Press.

Juujärvi, S., Ronkainen, K. & Silvennoinen, P. 2019. The ethics of care and justice in primary nursing of older patients. *Clinical Ethics, 14*(4), 187–194.

Loi, M., Christen, M., Kleine, N. & Webe, K. 2019. Cybersecurity in health–disentangling value tensions. *Journal of Information, Communication and Ethics in Society, 17*(2), 229-245.

Roman, L., Ancker, J., Johnson, S. & Senathirajah, Y., 2017. Navigation in the electronic health record: A review of the safety and usability literature. *Journal of Biomedical Informatics,* Volume 67, pp. 69-79.

Sarlio-Siintola, Sari (ed.). 2020. *SHAPES Ethical Framework D8.4.* [online] Available at: https://shapes2020.eu/wp-content/uploads/2020/11/D8.4-SHAPES-Ethical-Framework.pdf

van de Poel, I. 2020. Core Values and Value Conflicts. In: *M. Christen et al. (eds.), The Ethics of Cybersecurity.* Cham: Springer, pp. 45-72.

Weber, K., & Kleine, N. 2020. Cybersecurity in Health Care. In: *M. Christen et al. (eds.), The Ethics of Cybersecurity*. Cham: Springer, pp. 139-156.