Chapter 7
Cybersecurity in Health Care

Karsten Weber and Nadine Kleine

Abstract Ethical questions have always been crucial in health care; the rapid dissemination of ICT makes some of those questions even more pressing and also raises new ones. One of these new questions is cybersecurity in relation to ethics in health care. In order to more closely examine this issue, this chapter introduces Beauchamp and Childress' four principles of biomedical ethics as well as additional ethical values and technical aims of relevance for health care. Based on this, two case studies—implantable medical devices and electronic Health Card—are presented, which illustrate potential conflicts between ethical values and technical aims as well as between ethical values themselves. It becomes apparent that these conflicts cannot be eliminated in general but must be reconsidered on a case-by-case basis. An ethical debate on cybersecurity regarding the design and implementation of new (digital) technologies in health care is essential.

Keywords Autonomy · Beneficence · Electronic health cards · Implants · Justice · Nonmalefience · Principlism

7.1 Introduction: The Value of Health

In the preface of his book *The value of life* (1985: xv) bioethicist John Harris writes, with a dash of sarcasm, that

> [n]ot very long ago medical ethics consisted of two supremely important commandments. They were: do not advertise; and avoid sexual relations with your patients. At about the same time as doctors were doing their best to obey these commandments, moral philosophers were more concerned with the meaning of words than with the meaning of life. Now,

K. Weber (✉)
OTH Regensburg, Regensburg, Germany
e-mail: Karsten.Weber@oth-regensburg.de

N. Kleine
Universität Osnabrück, Osnabrück, Germany
e-mail: Nadine.Kleine@uni-osnabrueck.de

M. Christen et al. (eds.), *The Ethics of Cybersecurity*, The International Library of Ethics, Law and Technology 21,
https://doi.org/10.1007/978-3-030-29053-5_7

> not just doctors but all health care professionals are interested in ethical questions as they relate to medical practice […].

The questions Harris addresses are of fundamental character: the value of life, the beginning and end of life, euthanasia, and the like. Most astonishingly, health is not mentioned at all in the table of contents, although the whole book is dedicated to providing arguments that protecting the life and health of their patients is the most important responsibility of physicians and other health care professionals, since health is seen as the most important prerequisite of a good life.

In Western culture, at least since the time of ancient Greece, there has been a great deal of thought given to the value of health for a good and successful life. Even after more than 2500 years, the Hippocratic Oath still has an important significance for medical action; the value of health, not only throughout Western intellectual history, is a recurring theme. It is probably no exaggeration that health, despite all the problems inherent in a precise definition of this term, enjoys high priority worldwide. Given this importance, it cannot be surprising that in order to protect health, the WHO has formulated access to it as a central human right.

If health actually is an important, if not the most important, value to human beings, then a health care system being able to provide effective and efficient help in case of medical problems also is most valuable—from an individual as well as societal point of view. That immediately raises the question of who must be obliged to provide for the necessary resources to maintain an effective health care system (e.g. Daniels 1985; Harris 1988). Although we do not discuss the benefits and burdens or moral justifications of different ways to maintain and finance an effective and efficient health care system, justice and fairness will be an important issue in what follows. The provision and maintenance of cybersecurity in health care can be very resource-intensive; this raises the question of who has to pay for these resources.

Health care systems most obviously need huge amounts of resources—according to the WHO in 2015, US $7.2 trillion worldwide was spent on health care. This amounts to 10% of the 2015 global GDP. At the same time, in many countries providing these resources is becoming more difficult because political or economic factors, as present in most countries with aging populations, make it difficult to finance their respective health care system. Therefore, as Nancy Lorenzi (2005: 2) puts it, "[a]lmost every major economy in the world experiences the effects of the high cost of health care, and many, if not most, national and regional governments are in some stage of health care reform". Although this was being said more than a decade ago it is still valid—and it is to be expected that it still will be valid in the years to come.

Attempts to reform existing health care systems most often include the development and implementation of Information and Communication Technology (ICT) in order to support the provision of effective and efficient health care services. In other words, ICT shall be employed to reduce or at least stabilise the costs of health. One of the main purposes of ICT systems in health care is the administration of information about patients and treatments that "[…] is a vital but complex component in the modern health care system. At a minimum, health care providers need to know a

patient's identity and demographic characteristics, recent and distant medical history, current medications, allergies and sensitivities, chronic conditions, contact information, and legal preferences." (McClanahan 2007: 69) However, McClanahan also stresses that "[t]he increased use of electronic medical records has created a substantial tension between two desirable values: the increased quality and utility of patient medical records and the protection of the privacy of the information they contain".

At the same time, "[i]mprovements in the health status of communities depend on effective public health and health care infrastructures. These infrastructures are increasingly electronic and tied to the Internet. Incorporating emerging technologies into the service of the community has become a required task for every public health leader". (Ross 2003: v) In other words, stakeholders (see Chap. 6 for an example of a comprehensive stakeholder identification) such as patients, health care professionals, health care providers, or insurance companies are confronted with competing or even contradictory aims such as increasing efficiency, reducing costs, improving quality, and keeping information secure and confidential (cf. Fried 1987). Employing new technologies in health care therefore creates new value conflicts (see Chap. 3) or at least makes old conflicts and problems more visible or increases their urgency.

Simultaneously, other moral values also shall be protected and supported, either as fundamental moral values in European societies and/or as moral values (see Chap. 3), which are constitutive for the relationship between patients on the one side and health care professionals on the other. Conflicting or even contradictory aims and values raise moral concerns, since it has to be decided which aim and which value should be prioritised. To illustrate this, studying the conflict between beneficence and autonomy—both are important moral values within and outside the medical sphere —can be of assistance: When ICT is deployed in the health sector, it shall be aimed at ensuring that patients themselves determine when which information is revealed to whom—password protection and encryption are common measures to achieve this aim. However, in emergencies, when patients are no longer able to make this decision, there is now a risk that important medical information will no longer be accessible.

Moreover, it might be very helpful to share medically relevant patient information widely among health care professionals to improve the quality and efficiency of treatment. The goal of protecting patients' privacy and autonomy, however, may be at odds with this aim. In addition, in scholarly debates it is often mentioned that to provide cybersecurity it might be necessary to compromise privacy (see also Chap. 10). This can occur, for example, when non-personal health information on the Internet is only accessible if potential users of this information have to disclose their identity. It is argued that the respective platforms are better protected against attacks because the identity of the attackers could be determined. The problem here, however, is that anonymous searching, for example for information on diseases that are socially stigmatised, would then no longer be possible.

Such conflicting aims raise particular concern because it is obvious that both the protection of patients' privacy as well as the security of information systems and patient data must be important objectives in health care. Without privacy, trust

among patients and health care professionals necessary for medical treatment is jeopardised (cf. Beauchamp and Childress 2009: 288ff.) and without the certainty that patient data will not be tampered with or stolen, treatment itself is at risk.

Approaching cybersecurity in health, in the second section we first discuss the relevant moral principles, values and technical aims relevant for the health domain. To illustrate the complexity of these issues, in the third section we present case studies from health practice. We furthermore explain in detail the conflicts that have emerged, which are examples of the broad spectrum of existing conflicts and trade-offs in health care. Finally, we outline the relationship between moral values and cybersecurity in health care. In the fourth section, we draw a brief conclusion.

7.2 Principles, Moral Values and Technical Aims

7.2.1 Principlism as a Starting Point of Ethical Analysis

Those involved in scholarly and professional debates concerning biomedical ethics will be familiar with autonomy, beneficence and justice: Together with nonmaleficence these values—or more accurately 'principles'—can be seen as core moral aims, as particularly emphasised in Beauchamp and Childress' considerations on the foundations of biomedical ethics (see also Chap. 4). Their book *Principles of Biomedical Ethics* (2009) first published in 1977 is a groundbreaking text. The core features of their approach—'principlism'—involves four moral principles, namely autonomy, nonmaleficence, beneficence and justice, which are pertinent to a particular moral situation; furthermore, they use their specification, balancing and (deductive) application to create a bridge between the moral situation and the relevant principles.

It must be stressed that principlism is far from an indisputable tenet in biomedical ethics; its weaknesses include neglect of emotional and personal factors that are inherent in specific decision situations, oversimplification of the moral issues, and excessive claims of universality (e.g. Clouser and Gert 1990; Hine 2011; McGrath 1998; Sorell 2011). Nevertheless, principlism remains highly influential for scholarly thinking about ethical issues arising (not only) in the health domain (e.g. Reijers et al. 2018). Hence, we use principlism as the starting point of our ethical analysis concerning cybersecurity in health.

As already mentioned, Beauchamp and Childress' four principles of biomedical ethics are *respect for autonomy*, *nonmaleficence*, *beneficence* and *justice,* the definitions of which can be briefly summarized as follows (cf. Loi et al. 2019):

– *Respect for autonomy* as a negative obligation means avoiding interfering in other people's freely made decisions. Understanding respect for autonomy as a positive obligation means informing people comprehensibly and thoroughly about all aspects of a decision, for example about its consequences. Respect for autonomy also may "[…] affect rights and obligations of liberty, privacy, confi-

dentiality, truthfulness, and informed consent […]" (Beauchamp and Childress 2009: 104).

- The principle of *nonmaleficence* is derived from the classic quote "above all, do no harm" which is often ascribed to the Hippocratic Oath. As Beauchamp and Childress (2009: 149) state, "[…] the Hippocratic oath clearly expresses an obligation of nonmaleficence and an obligation of beneficence". At the heart of this principle is the imperative not to harm or ill-treat anyone, especially patients.
- *Beneficence* must be distinguished from nonmaleficence. According to Beauchamp and Childress (2009: 197), "[m]orality requires not only that we treat persons autonomously and refrain from harming them, but also that we contribute to their welfare." Consequently, care must always be taken to ensure that actions that are intended to be benevolent do indeed contribute to a benefit; the advantages and disadvantages, risks and opportunities as well as the costs and benefits of those actions must therefore be weighed up.
- *Justice* as a principle is even more difficult to grasp than the other three principles, since the different existing theories of justice produce very different results. For the purposes of our considerations, justice is to be translated as a guarantee of fair opportunities and the prevention of unfair discrimination, for instance based on gender or ethnicity. Justice also means that scarce resources should not be wasted; in addition, these resources often have to be provided by others, for example by the insured (cf. McCarthy 1987), so that economic use is required.

As Beauchamp (1995: 182) emphasises, "[t]he choice of these four types of moral principle as the framework for moral decision making in health care derives in part from professional roles and traditions." Hence, it should be considered that it might have repercussions on the principles as a framework for moral decision making in health care if professional roles and traditions change in time. It is most obvious that new technologies contribute to such changes.

7.2.2 Technical Aims Mapping to Ethical Principles

Despite justified criticism, we chose to use principlism as a starting point of our ethical analysis because its four moral principles can be mapped to the important aims of the employment of ICT in health care, which are *efficiency and quality of services*, *privacy of information and confidentiality of communication*, *usability of services* and *safety* (this idea was first developed by Christen et al. 2018; see also Fig. 7.1). The definitions of these for aims can be summarised as follows:

- *Efficiency and Quality of Services:* One of the main purposes of ICT systems in health care is the administration of information in order to increase the *efficiency* of the health care system and to reduce its costs. Improvements in health care 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

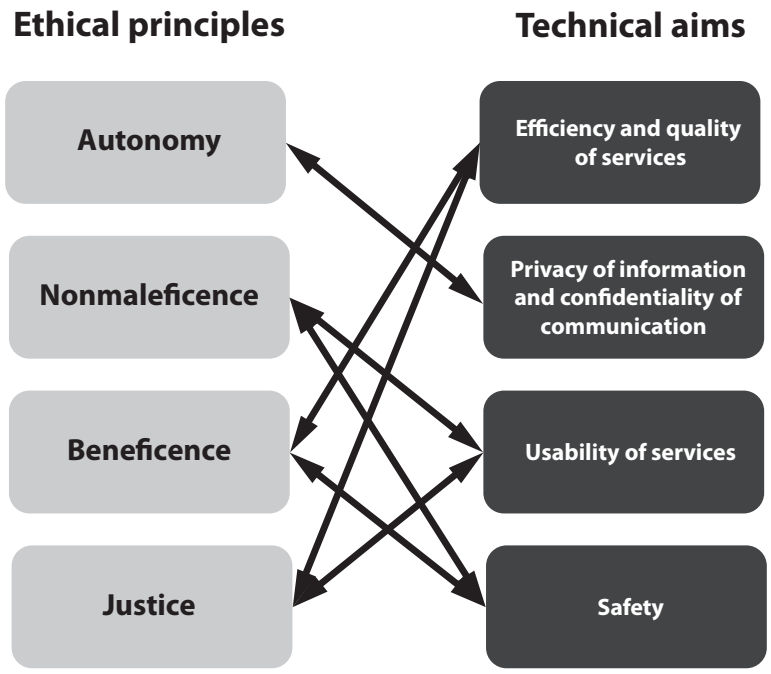

Fig. 7.1 Technical aims mapping to ethical principles

insights regarding diseases and possible treatments (e.g. Vayena et al. 2016). In this regard, *quality and efficiency of services* map to the *principle of beneficence*. *Efficiency of services* map also to the *principle of justice* insofar as services contribute to the economic use of resources, in this way diminishing the risk of unfair allocations.

– *Privacy of Information and Confidentiality of Communication:* 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 health care. In particular, privacy is often seen as a prerequisite of patients' autonomy and therefore *privacy* maps to the *principle of autonomy*. Privacy and confidentiality are also foundations of trust among patients on the one hand and health care professionals on the other.
– *Usability of Services: Usability* can be defined as "[…] the degree of effectiveness, efficiency, and satisfaction with which users of a system can realize their intended task" (Roman et al. 2017: 70). With regard to health, users can be patients, medical staff and/or administrators, which have different degrees of ICT competences, depending on personal attitudes and socio-demographic variables (Kaplan and Litewka 2008). *Usability of services* map to the *principle of nonmaleficence* since poor usability can hurt people (e.g. Magrabi et al. 2012; Viitanen et al. 2011). Thus, usability, quality and efficiency are interrelated since reduced usability may compromise quality and efficiency. *Usability of services* additionally maps to the *principle of justice* in that usability for all kinds of users increases the accessibility of services.

– *Safety: 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. *Safety* maps to the *principle of nonmaleficence* as well as to the *principle of beneficence*.

The four technical objectives mentioned above are composed of various subgoals. For instance, accessibility, availability, responsibility and transparency can be considered part of safety. Another example is universal design as "design-for-all, barrier-free design, transgenerational design, design-for-the-broader-average, or design-for-the-nonaverage" (Sandhu 2000: 80) that can be understood as part of usability. A detailed ethical analysis of case studies requires a very thorough examination of what subgoals make up the above mentioned technical aims in each case—this can be understood as a "specification" in the sense that Beauchamp and Childress understand it in relation to their ethical principles. This kind of specification is important not only for the technical requirements, but—as will become apparent—also for the identification of moral values that could be affected by technical aims.

7.2.3 Other Moral Values

The findings of an extensive structured literature search (Christen et al. 2017; Yaghmaei et al. 2017: 9–17) show that, beside the four principles, additional moral values are affected by cybersecurity in health care. These values may often have a connection to Beauchamp and Childress' principles, but, to different extents, they go beyond them. The most relevant ones with regard to cybersecurity in health care are *freedom and consent*, *privacy and trust*, *dignity and solidarity*, and *fairness and equality.*

– *Privacy and Trust:* Privacy plays a crucial role, not least because of the use of constantly growing amounts of data (Big Data). Privacy of patients shall be guaranteed, also with particular regard to the sensitive nature of health-related data. Risks such as uncontrolled access by third parties, disclosure of data and the like are to be eliminated. Patients must be able to trust new health technologies, professionals and the health care system in general. In other words, they must be certain to be protected from harm, which is connected to the *principle of nonmaleficence*.
– *Freedom and Consent:* Freedom includes both the unrestricted choice of (non-) use of new technologies as well as the unhindered choice of how and for which purposes new technologies are being used. To achieve this, patient consent must be recognised as an important factor in health care. This refers, in contrast to presumed consent, to informed consent. The idea of informed consent and the general freedom of use and freedom of choice emphasises the *principle of autonomy*.

- *Fairness and Equality:* An important value in terms of health is fairness in treatment. This includes access for all patients to all types of treatment, regardless of, for instance, their ethnicity and social background. This is closely linked to the principle of justice, but emphasises the protection against subtle unfair treatments, e.g. special consideration for people with a lack of skills, knowledge or abilities: Patients with limited health and technical literacy should be treated equally compared to those who know how to operate health technology. Everybody must be protected from unfair treatment, discrimination and stigmatisation; vulnerable groups shall not be excluded. Fairness and equality are closely linked to the *principle of justice*.
- *Dignity and Solidarity:* Human dignity is a major democratic and European value. Dignity must always be maintained, regardless of technical innovations, necessary moral compromises and limited resources. While dignity in its abstract form is difficult to grasp and primarily addresses the individual, solidarity describes a societal value in a more concrete way: the interpersonal commitment of individuals and groups who have both responsibility and benefits as a community, e. g. in a health insurance system and public welfare. Both dignity and solidarity, especially in relation to health and cybersecurity, are tied to the *principle of beneficence*.

These ethical principles and additional values are often both interlinked and in conflict with each other. In addition, there is the different use of terms: Privacy, for example, appears as part of an ethical principle, a technical aim and a moral value. Privacy as technical aim refers to data protection whereas Beauchamp and Childress consider privacy as a specification of the principle of autonomy. This ambiguity again demonstrates the importance of a detailed analysis of moral principles and values on the one hand and technical aims on the other.

7.3 Case Studies

7.3.1 Cardiac Pacemakers and Other Implantable Medical Devices

7.3.1.1 Brief Description of the Case

Implantable medical devices (IMDs) are employed with the intention of improving the quality of a patient's life. Implants such as cardiac pacemakers, insulin pumps, biosensors and cochlear implants offer therapeutic, monitoring and even life-saving benefits: medical treatment can be made more precise, efficient, customised and flexible (Burleson and Carrara 2014, 1 f.; Ransford et al. 2014, 157/167 f.). An increasing number of IMDs are wirelessly networked and can be connected to other devices to, for example, monitor functionality, set parameters, exchange data or install software updates.

However, for some years, there have been reports about the dangers of implantable medical devices. In addition to the risk of unintentional loss of function due to defects, the connectivity of IMDs leaves them open to malicious attacks. Examples of such possible attacks are (Baranchuk et al. 2018: 1285 f.; Coventry and Branley 2018: 48 f.; Mohan 2014: 372, Ransford et al. 2014: 158/161 f.):

- Unauthorised access to sensitive data, and their manipulation or further misuse such as identity theft.
- Spread of malware and viruses to interconnected devices and system networks.
- Manipulations of the devices to, for instance, modify the automatic insulin output or the impulse rate of a cardiac pacemaker.
- Switching off devices, which can endanger the health or, in the worst case, even the life of the person carrying the device.

Although there have been no real incidents known to date, for years, hackers, security experts, and scientists have been illustrating the vulnerabilities of IMDs: Jerome Radcliffe presented a talk at the Black Hat conference in 2011 at which he explained how he was able to get access to implanted insulin pumps through reverse engineering (Radcliffe 2011); Barnaby Jack showed his successful hack in order to control pacemakers (Burns et al. 2016: 70); and Pycroft et al. (2016) discussed the actual possibilities of 'brainjacking' neurological implants. In 2017, the FDA published a safety communications issue in which it announced that almost half a million cardiac pacemakers must get a software update "[…] to reduce the risk of patient harm due to potential exploitation of cybersecurity vulnerabilities […]" (FDA 2017). In one of the most recent cases, Billy Rios and Jonathan Butts explained in the abstract of their Black Hat 2018 presentation that they "[…] provide detailed technical findings on remote exploitation of a pacemaker system [sic!], pacemaker infrastructure, and a neurostimulator system. Exploitation of these vulnerabilities allow for the disruption of therapy as well as the ability to execute shocks to a patient." (Rios and Butts 2018) Already some years ago, this issue received special public attention when the media widely reported that the wireless function of then US Vice President Dick Cheney's pacemaker was deactivated due to security risks (e.g. Vijayan 2014).

Although dangers posed by attacks on IMDs should not be underestimated, their occurrence is, due to the complexity of such attacks, not yet too realistic: First, depending on the type of data transmission, a short distance may be required, not least because of the already difficult energy provision of IMDs. Second, the motivation to potentially risk the lives of implant users need to be given; if it was a matter of financial gain through access to personal data, other cyberattacks would serve a better purpose. Experts expect a greater risk of malware and viruses affecting medical networks including connected implants (Baranchuk et al. 2018, 1287; Burleson and Carrara 2014, 2–5; Coventry and Branley 2018: 49–51).

Different factors contribute to the lack of security. In addition to the risks posed by interconnectivity, there are other technical difficulties: Digital implants are supposed to have a long lifetime circle to minimise invasive treatment. Therefore, and due to the required small size and lightweight of medical devices, battery capacity

and storage space are very limited, which often results in weak or missing encryption; outdated, weak or even no virus protection; and/or in the lack of regular software updates. The latter in particular creates the risk of endangering patients' health and/or life caused by malfunctions or breakdowns of a device due to the problem of outdated and insecure software used with IMDs (Burleson and Carrara 2014: 1/4; Fu and Blum 2013: 36; Mohan 2014, 372 f.; Ransford et al. 2014: 162/166–169). The development of effective regulations to improve the security of IMDs has proven to be difficult as well: Several administrative bodies (e.g. the FDA, see Woods 2017) have been working on such regulations and on certification systems for years without successfully covering all eventualities. Due to the complex combination of various technical factors and different actors, the definition of responsibilities and requirements regarding IMDs seems to be quite difficult and often comes with a huge time delay with regard to technical improvements (Burns et al. 2016: 70 f.; Cerminara and Uzdavines 2017: 311 f.; Coventry and Branley 2018: 48).

7.3.1.2 Conflicting Ethical Values

The following analysis of possible moral conflicts demonstrates that there are not just management problems that contributes to these conflicts but that competing moral values or different value hierarchies on the part of stakeholders increase the insecurity of IMDs. Furthermore, as already pointed out, moral values can also conflict with technical requirements.

IMDs serve the primary aim of increasing the physical safety of patients. Wireless IMDs are designed to enable the continuous monitoring of vital parameters and faster communication with health care professionals both routinely and in emergency cases. While this faster access aims to enable health care professionals to use medical data more quickly, efficiently and flexibly to perform successful treatment, lack of transparency about who and under what circumstances can access what information does not ensure patient consent and control (Mohan 2014: 372). In addition, a key problem that patients do not have direct access to information stored in IMDs, particularly in the case of so-called 'closed-loop-devices', although these data could inform them about their own body and health status (Alexander 2018; Ransford et al. 2014: 165–167).

If patients think that they might have little or no control over their own health-related data, that could, in the long run, contribute to a loss of confidence in health technology as well as in health care professionals. Because IMDs can be attacked and personal data stolen, patients may perceive danger for themselves and their data and thus for privacy and trust. Furthermore, there is the risk that implant users will be discriminated against as a consequence of unauthorised access to sensitive data, their uncontrollable use and disclosure to third parties. (Burleson and Carrara 2014: 1f; Coventry and Branley 2018: 48, Ransford et al. 2014: 158).

Another possible negative effect on patients' trust is the lack of a clear attribution of (moral) responsibility to the various stakeholders involved (e.g. manufacturers and designers, health care professionals and insurance companies, legislators and regula-

tors), who pursue different interests and are not always primarily focused on patients' well-being (Alexander 2018; Baranchuk et al. 2018: 1285 f.; Burns et al. 2016: 72).

If patients were to decide who exactly has access to their IMD or if the access would be at least (through technical or regulatory measures) more protected, however, other problems (in addition to the ones mentioned above) would arise:

> Requiring users to authenticate to a device before altering its functionality is a boon for security, but it introduces risks in case of an emergency. A medical professional may need to reprogram or disable a device to effectively treat a patient. […] [E]ncryption or other strong authentication mechanisms could make such emergency measures impossible if the patient is unconscious or the facility does not possess a programming device with a required shared secret. (Ransford et al. 2014: 170).

In this case, the effective use and safety of the IMD would be in jeopardy. The conflict between usability and security does not only occur with the use by health care professionals. In the case of an open-loop system in which patients have access to the information stored in the device, their literacy level must be considered to ensure that patients with little technical knowledge and understanding for security do not suffer disadvantages. The degree of dependency and the level of risk must also be considered (Alexander 2018; Ransford et al. 2014: 164 f.).

7.3.2 Electronic Health Card (eHC) in Germany and Elsewhere

7.3.2.1 Brief Description of the Case

Conflicts with regard to cybersecurity are often related to privacy and data protection (e.g. Fernández-Alemán et al. 2013; see also Chap. 10). However, there are other types of conflicts. For instance, reaching a high level of cybersecurity might be very expensive. In a health care system financed on a solidarity basis, as it exists, for instance, in many European states, such costs would be passed on to all insured persons and thus potentially make the health care system more expensive for all. In health care systems where every person insures her own risk, as in the United States for example, it could be the case that only those who are willing and able to pay for expensive security would be able to enjoy the benefits of appropriately secured technology. This might raise concerns regarding social justice. As mentioned above, cybersecurity can also conflict with usability and accessibility. Despite these potential difficulties, there are high hopes for the use of IT in health care, in particular regarding electronic health records and electronic health cards. This is demonstrated with reference to the German eHealth Card (eHC):

> As part of the German health-care reform, the current health insurance card is being upgraded to an electronic health card. On it, data on patient investigations, drug regulations, vaccinations and emergency data are stored. The aim is among other things to improve medical care and the prevention of drug incompatibilities and duplication of investigations. (Jürjens and Rumm 2008)

The development of an eHC in Germany was already discussed for the first time in 2004. Technical development then began in 2006, but in 2009 the project was halted (Tuffs 2010) because it was feared that the costs and benefits were no longer in reasonable proportion to each other. There was also a great deal of resistance, particularly on the side of physicians. Now, in 2019, the nationwide introduction of the German eHC has yet to begin (cf. Stafford 2015).

In particular, German physicians are quite sceptical with regard to the eHC, since it is feared that its deployment will result in huge costs and increase the workload of physicians and health care personnel: "The cost-benefit factor plays an important role in the implementation process, because—in the opinion of many physicians—the financial effort for acquiring and maintaining the system does not sufficiently outweigh the resulting benefit" (Wirtz et al. 2012: 659). As Ernstmann et al. (2009: 185) write, "[…] the ratings of perceived usefulness are rather low, i.e. physicians are not aware of useful aspects of the new technology or do not judge the established aspects as useful in their practice."

It is difficult to make accurate statements about whether this dissatisfaction has improved, as there is little practical experience with the eHC to date. A large-scale study (Schöffski et al. 2018) shows that many practitioners are still sceptical about the benefits. Although it is emphasised that the validity of the insurance status can be determined more reliably by the eHC—which is an important (cyber)security aspect—the administrative effort has not decreased. Since the functional capabilities of the eHC have also been very limited to date, it is still not possible to prove any medical benefit. Some scholars (Deutsch et al. 2010; Klöcker 2014) assume that these attitudes result from the perception of different aims on the part of the stakeholders; this would strengthen the assumption that technical, medical and ethical values or principles often compete or conflict with each other, especially in the health care sector. Although not discussed in detail here, it should be added that economic considerations play a dominant role in this particular case, which may also compete with other goals and values.

This rather sceptical attitude changes if it is assumed that the functional scope of the eHC is supplemented by the storage of a so-called emergency dataset, which, for example, would make it considerably easier for emergency physicians to provide first aid more accurately (Born et al. 2017). Since the medical benefit for physicians and, of course, for patients is most obvious, other considerations such as privacy, data protection and the like seem to be pushed into the background.

At the same time, at least to some stakeholders, benefits such as increased security are less obvious: "The efficiency of the system is considered as critical by the physicians, particularly in terms of data security and potential misuse of data. The primary concern of the physicians is the unauthorised access of a third party to stored data." In addition, "[r]egarding the introduction of the eHC to date, most physicians have criticized the very opaque communication and poor instruction on the subject" (Wirtz et al. 2012: 651). Or, to put it in other words (Ernstmann et al. 2009: 181): "Primary care physicians rate their involvement in the process of the development of the technology and their own IT expertise concerning the technological innovation as rather low."

The German eHC is based on a decentralised ICT infrastructure; its security features are strongly dependent on online network connections between end-user terminals and servers. Only if such connections are available can all security features can be fully used—two-factor authentication with PIN and eHC, for example, only works if there is an online connection between the terminal and the server. Without being online, end-user terminals can still be used, but with reduced security. In such cases, the application of the eHC comes with a potential conflict of (cyber-)security on the one hand and usability on the other (Jürjens and Rumm 2008). Since the provision of mobile Internet has improved since 2008, this problem may have been mitigated. The example shows, however, that cybersecurity builds on infrastructures that are not always and universally available—this might raise questions of social justice.

7.3.2.2 Conflicting Ethical Values

In addition to the obvious conflicts of moral values that could arise from the high infrastructural costs for the introduction of the eHC, this brief description already illustrates that there are other areas of conflict that should be examined in more detail.

Beyond the issue of unfair distributed economic burdens, which raise moral concern with regard to social justice, the deployment of the German eHC as well as similar ICT infrastructures in other countries might be accompanied with another issue concerning discrimination. Due to security considerations, e.g. to protect medical data against misuse and unauthorised access, most of these infrastructures employ encryption and password protection of sensitive data. Laur (2014) mentions that "[w]hile some people have already difficulty remembering a PIN (especially elderly and disabled people), having many more passwords that are intended to protect them could put them at risk of disclosure, loss or stealing."

Although Laur refers to electronic health records in general, the problem also applies to the German eHC in particular: The eHC not only consists of a database, but its core components are a PIN and a credit card-sized chip card for two-factor authentication. Patient data (apart from the emergency dataset) can only be accessed if the chip card and PIN are used simultaneously. For elderly and/or handicapped people, for instance the visually impaired, using the eHC could be difficult. It is very likely that the persons concerned will create their own work-arounds, for example by writing PINs on the eHC or by disclosing them to health care personnel, which will certainly reduce the level of data protection, privacy and security of those persons. In such cases, a personal relationship of trust, which was originally intended to be replaced by technology, regains importance. From an ethical perspective, this does not necessarily have to be evaluated negatively, but it demonstrates that security measures can have ambivalent consequences and might raise concerns with regard to equality. Furthermore, it must be considered that in the large study of Schöffski et al. (2018), usability was not really examined. This raises questions regarding the consideration of stakeholder groups such as handicapped or elderly people and their needs.

7.3.3 Cybersecurity and Ethics in Health: A Tentative Summing-Up

It must be stressed that there is a long history behind the collection, storage and use of patient data. During that time, moral rules or moral orders developed to manage this data conscientiously and according to the interests of all stakeholders, but these rules related to data storage in paper files. The introduction of new technologies for storing and processing patient data, such as the electronic patient record or the eHC, will undoubtedly affect traditional moral and legal rules "governing health records, for example, consent and access rules, responsibility for data quality, liability for negligence, mistakes and accidents" (Garrety et al. 2014: 72); they will certainly be called into question by the new possibilities. In the future, we will have to prove whether these changes should be called "disruption of moral orders" (Garrety et al. 2014). Nevertheless, (digital) technologies and their possibilities force us to pay more attention to how moral rights and obligations change with the use of technology.

The case studies described above should already demonstrate that in terms of cybersecurity, the design and application of new technologies in health care affect numerous principles, goals and moral values that are in competitive, conflicting or exclusive relationships. Without striving for completeness, the conflicts among technical aims and moral values and/or among different moral values should be briefly mentioned again: security vs. usability, safety and usability vs. privacy and trust, efficiency and quality of service vs. freedom and consent, and security vs. beneficence. It is likely that in many cases, conflicts can be mitigated or even completely resolved by skilful technical design or by adapting organisational processes. However, it is equally likely that in some cases no such simple solutions are available. Beauchamp and Childress have often been criticised for not providing a clear hierarchy of principles; this, as often denounced, leaves the prioritisation of principles to the discretion of the decision-makers. However, it could well be that in many conflicts this is all that can be achieved. It is therefore one of the most important tasks of the value-based design of technology to make considerations transparent that lead to a decision. This makes it possible for decisions to be reconstructed, questioned and, if necessary, revised later on. In addition, there is often a demand that as many stakeholders as possible be involved in the value-based design of technology so that their expectations, demands and fears could be considered (Hennen 2012). However, it should be kept in mind that the participatory design of technology itself raises moral concerns that cannot always be answered adequately (Saretzki 2012).

7.4 Conclusion

Verbeek (2006: 362) writes that "[l]ike a theater play or a movie […] technologies possess a "script" in the sense that they prescribe the actions of the actors involved. Technologies are able to evoke certain kinds of behaviour […] Technological

artefacts can influence human behaviour, and this influence can be understood in terms of scripts." Verbeek (2006: 361) thus stresses that it is necessary to explore technology's normative aspects because "[w]hen technologies coshape human actions, they give material answers to the ethical question of how to act. This implies that engineers are doing 'ethics by other means': they materialize morality." As a consequence, we must learn that "[…] information systems are intentionally or unintentionally informed by moral values of their makers. Since information technology has become a constitutive technology which shapes human life it is important to be aware of the value ladenness of IT design." (van den Hoven 2007: 67).

The statements above aim to provide an initial insight into how moral values can conflict with each other in the design and use of medical technology, as well as how technical design decisions can come into competition with moral values. It is to be expected that an investigation of further case studies would reveal other and more conflicts not considered here. Following the concepts of 'value sensitive design' (VSD, e.g. Friedman 1996; Friedman et al. 2013) and 'responsible research and innovation' (RRI, i.e. Burget et al. 2017; Stahl et al. 2014), every research and development project must therefore ensure that a comparable detailed analysis takes place in order to detect and then avoid such conflicts.

Acknowledgments The chapter was created with funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 700540.

References

Alexander N (2018) My Pacemaker is tracking me from inside my body. The Atlantic. https://www.theatlantic.com/technology/archive/2018/01/my-pacemaker-is-tracking-me-from-inside-my-body/551681/. Last access 7 July 2019

Baranchuk A, Refaat MM, Patton KK (2018) Cybersecurity for cardiac implantable electronic devices: What should you know? J Am Coll Cardiol 71(11):1284–1288. https://doi.org/10.1016/j.jacc.2018.01.023

Beauchamp TL (1995) Principlism and its alleged competitors. Kennedy Inst Ethics J 5(3):181–198. https://doi.org/10.1353/ken.0.0111

Beauchamp TL, Childress JF (2009) Principles of biomedical ethics, 6th edn. Oxford University Press, New York

Born J, Albert J, Bohn A et al (2017) Der Notfalldatensatz für die elektronische Gesundheitskarte: Die Sicht von Notfallmedizinern und Rettungsdienstpersonal. Notfall + Rettungsmedizin 20(1):32–37. https://doi.org/10.1007/s10049-016-0197-y

Burget M, Bardone E, Pedaste M (2017) Definitions and conceptual dimensions of responsible research and innovation: a literature review. Sci Eng Ethics 23(1):1–19. https://doi.org/10.1007/s11948-016-9782-1

Burleson WP, Carrara S (2014) Introduction. In: Burleson WP, Carrara S (eds) Security and privacy for implantable devices. Springer, New York, pp 1–11

Burns AJ, Johnson ME, Honeyman P (2016) A brief chronology of medical device security. Commun ACM 59(10):66–72. https://doi.org/10.1145/2890488

Cerminara KL, Uzdavines M (2017) Introduction to regulating innovation in healthcare: protecting the public or stifling progress? Nova Law Rev 31(3):305–312

Christen M, Gordijn B, Weber K et al (2017) A review of value-conflicts in cybersecurity. ORBIT J 1(1). https://doi.org/10.29297/orbit.v1i1.28

Christen M, Loi M, Kleine N et al (2018) Cybersecurity in health – disentangling value tensions. Paper presented at the Ethicomp 2018, SWPS University of Social Sciences and Humanities, Sopot/Poland, September 24–26, 2018

Clouser KD, Gert B (1990) A critique of principlism. J Med Philos 15(2):219–236. https://doi.org/10.1093/jmp/15.2.219

Coventry L, Branley D (2018) Cybersecurity in healthcare: a narrative review of trends, threats and ways forward. Maturitas 113:48–52. https://doi.org/10.1016/j.maturitas.2018.04.008

Daniels N (1985) Just health care. Cambridge University Press, Cambridge

Deutsch E, Duftschmid G, Dorda W (2010) Critical areas of national electronic health record programs—is our focus correct? Int J Med Inform 79(3):211–222. https://doi.org/10.1016/j.ijmedinf.2009.12.002

FDA (2017) Firmware update to address cybersecurity vulnerabilities identified in Abbott's (formerly St. Jude Medical's) implantable cardiac pacemakers: FDA safety communication. https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm. Last access 7 July 2019

Fernández-Alemán JL, Señor IC, Lozoya PÁO et al (2013) Security and privacy in electronic health records: a systematic literature review. J Biomed Inform 46(3):541–562. https://doi.org/10.1016/j.jbi.2012.12.003

Fried C (1987) The primacy of the physician as trusted personal advisor and not as social agent. In: Brody BA, Engelhardt HT Jr (eds) Bioethics: readings & cases. Prentice-Hall, Englewood Cliffs, pp 221–225

Friedman B (1996) Value-sensitive design. Interactions 3(6):16–23. https://doi.org/10.1145/242485.242493

Friedman B, Kahn PH, Borning A et al (2013) Value sensitive design and information systems. In: Doorn N, Schuurbiers D, van de Poel I (eds) Early engagement and new technologies: opening up the laboratory, vol 16. Springer, Dordrecht, pp 55–95. https://doi.org/10.1007/978-94-007-7844-3_4

Fu K, Blum J (2013) Controlling for cybersecurity risks of medical device software. Commun ACM 56(10):35–37. https://doi.org/10.1145/2508701

Garrety K, McLoughlin I, Wilson R et al (2014) National electronic health records and the digital disruption of moral orders. Soc Sci Med 101:70–77. https://doi.org/10.1016/j.socscimed.2013.11.029

Harris J (1985) The value of life. Routledge, London/New York

Harris J (1988) More and better justice. In: Bell JM, Mendus S (eds) Philos med welfare. Cambridge University Press, Cambridge, pp 75–96

Hennen L (2012) Why do we still need participatory technology assessment? Poiesis Prax 9(1–2):27–41. https://doi.org/10.1007/s10202-012-0122-5

Hine K (2011) What is the outcome of applying principlism? Theor Med Bioeth 32(6):375–388. https://doi.org/10.1007/s11017-011-9185-x

Jürjens J, Rumm R (2008) Model-based security analysis of the German health card architecture. Methods Inf Med 47(5):409–421. https://doi.org/10.3414/ME9122

Kaplan B, Litewka S (2008) Ethical challenges of telemedicine and telehealth. Camb Q Healthc Ethics 17(04):401–416. https://doi.org/10.1017/S0963180108080535

Klöcker P (2014) Understanding stakeholder behavior in Nationwide electronic health infrastructure implementation. In: 2014 47th Hawaii international conference on system sciences. IEEE, Waikoloa, HI, pp 2857–2866. https://doi.org/10.1109/HICSS.2014.357

Laur A (2014) Fear of e-health records implementation? Med Leg J 83(1):34–39. https://doi.org/10.1177/0025817214540396

Loi M, Christen M, Kleine N et al (2019) Cybersecurity in health – disentangling value tensions. J Inform Commun Ethics Soc. https://doi.org/10.1108/JICES-12-2018-0095

Lorenzi NM (2005) Introduction. In: Lorenzi NM, Ash JS, Einbinder J et al (eds) Transforming health care through information, 2nd edn. Springer, New York, pp 2–6

Magrabi F, Ong M-S, Runciman W (2012) Using FDA reports to inform a classification for health information technology safety problems. J Am Med Inform Assoc 19(1):45–53. https://doi.org/10.1136/amiajnl-2011-000369

McCarthy C (1987) The money we spend and its sources. In: Brody BA, Engelhardt HT Jr (eds) Bioethics: readings & cases. Prentice-Hall, Englewood Cliffs, pp 206–213

McClanahan K (2007) Balancing good intentions: protecting the privacy of electronic health information. Bull Sci Technol Soc 28(1):69–79. https://doi.org/10.1177/0270467607311485

McGrath P (1998) Autonomy, discourse, and power: a postmodern reflection on principlism and bioethics. J Med Philos 23(5):516–532. https://doi.org/10.1076/jmep.23.5.516.2568

Mohan A (2014) Cyber decurity for personal medical devices internet of things. In: 2014 IEEE international conference on distributed computing in sensor systems. IEEE, Marina Del Rey, CA, USA, pp 372–374. https://doi.org/10.1109/DCOSS.2014.49

Pycroft L, Boccard SG, Owen SLF et al (2016) Brainjacking: implant security issues in invasive neuromodulation. World Neurosurg 92:454–462. https://doi.org/10.1016/j.wneu.2016.05.010

Radcliffe J (2011) Hacking medical devices for fun and insulin: breaking the human SCADA system. White paper. Black Hat Conference 2011, USA, https://media.blackhat.com/bh-us-11/Radcliffe/BH_US_11_Radcliffe_Hacking_Medical_Devices_WP.pdf. Last access 7 July 2019

Ransford B, Clark SS, Kune DF et al (2014) Design challenges for secure implantable medical devices. In: Burleson WP, Carrara S (eds) Security and privacy for implantable devices. Springer, New York, pp 157–173

Reijers W, Wright D, Brey P et al (2018) Methods for practising ethics in research & innovation: a literature review, critical analysis and recommendations. Sci Eng Ethics 24(5):1437–1481. https://doi.org/10.1007/s11948-017-9961-8

Rios B, Butts J (2018) Understanding and exploiting implanted medical devices. https://www.blackhat.com/us-18/briefings.html#understanding-and-exploiting-implanted-medical-devices. Last access 7 July 2019

Roman LC, Ancker JS, Johnson SB et al (2017) Navigation in the electronic health record: a review of the safety and usability literature. J Biomed Inform 67:69–79. https://doi.org/10.1016/j.jbi.2017.01.005

Ross DA (2003) Foreword. In: O'Carroll PW, Yasnoff WA, Ward ME (eds) Public health informatics and information systems. Springer, New York, p vvi

Sandhu JS (2000) Citizenship and universal design. Ageing Int 25(4):80–89. https://doi.org/10.1007/s12126-000-1013-y

Saretzki T (2012) Legitimation problems of participatory processes in technology assessment and technology policy. Poiesis Prax 9(1–2):7–26. https://doi.org/10.1007/s10202-012-0123-4

Schöffski O, Adelhardt T, Brunner, S et al (2018) VSDM Ergebnisphase: LG 15: Evaluationsgutachten (inklusive LG 14: Statistische Auswertungen). https://www.evaluation-egk.de/wordpress/wp-content/uploads/2018/03/ORS1-WEV-VSDM_LG15_Evaluationsgutachten_inkl.-LG14_v1.0_final.pdf. Last access 7 July 2019

Sorell T (2011) The limits of principlism and recourse to zheory: the example of telecare. Ethical Theory Moral 14(4):369–382. https://doi.org/10.1007/s10677-011-9292-9

Stafford N (2015) Germany is set to introduce e-health cards by 2018. BMJ 350(jun01 1):h2991–h2991. https://doi.org/10.1136/bmj.h2991

Stahl BC, Eden G, Jirotka M (2014) From computer ethics to responsible research and innovation in ICT: the transition of reference discourses informing ethics-related research in information systems. Inf Manag 51(6):810–818. https://doi.org/10.1016/j.im.2014.01.001

Tuffs A (2010) Germany puts universal health e-card on hold. BMJ 340(Jan 12 2):c171. https://doi.org/10.1136/bmj.c171

van den Hoven J (2007) ICT and value sensitive design. In: Goujon P, Lavelle S, Duquenoy P et al (eds) The information society: innovation, legitimacy, ethics and democracy. In honor of Professor Jacques Berleur S.J, vol 233. Springer, Berlin, pp 67–72. https://doi.org/10.1007/978-0-387-72381-5_8

Vayena E, Gasser U, Wood A, O'Brien D, Altman M (2016) Elements of a new ethical framework for big data research. Wash Lee Law Rev 72(3):420–441

Verbeek P-P (2006) Materializing morality: design ethics and technological mediation. Sci Technol Hum Values 31(3):361–380. https://doi.org/10.1177/0162243905285847

Viitanen J, Hyppönen H, Lääveri T, Vänskä J, Reponen J, Winblad I (2011) National questionnaire study on clinical ICT systems proofs: physicians suffer from poor usability. Int J Med Inform 80(10):708–725. https://doi.org/10.1016/j.ijmedinf.2011.06.010

Vijayan J (2014) DHS investigates dozens of medical device cybersecurity flaws. Informationweek. http://www.informationweek.com/healthcare/security-and-privacy/dhs-investigates-dozens-ofmedical-device-cybersecurity-flaws-/d/d-id/1316882. Last access 7 July 2019

Wirtz BW, Mory L, Ullrich S (2012) eHealth in the public sector: an empirical analysis of the acceptance of Germany's electronic health card. Public Adm 90(3):642–663. https://doi.org/10.1111/j.1467-9299.2011.02004.x

Woods M (2017) Cardiac defibrillators need to have a bulletproof vest: the national security risk posed by the lack of cybersecurity in implantable medical devices. Nova Law Rev 41(3):419–447

Yaghmaei E, van de Poel I, Christen M, et al (2017, October 4) Canvas white paper 1 – cybersecurity and ethics. https://doi.org/10.2139/ssrn.3091909. Last access 7 July 2019