Chapter 3
Laws and Regulations for Digital Health

Nadezhda Purtova, Eleni Kosta, and Bert-Jaap Koops

Abstract Traditional health care is being transformed into digital health care through eHealth applications, mobile health delivery, personalized medicine, and social media. The area of health care is heavily regulated. Hence, the design and implementation of the innovative eHealth solutions must account for conventional health law. Translating legal norms into features of design and implementation may prove difficult. The aim of this chapter is to facilitate this process and make first steps towards a methodology for interpretation of legal and regulatory rules into engineering requirements. This chapter has presented an integrated approach to legal requirements engineering in the context of eHealth, bringing together a methodology for mapping existing legal and regulatory landscape and the strategies to interface the identified rules into design of the eHealth technology and processes. Drawing on earlier work of Koops (Law and technology: The challenge of regulating technological, Pisa: Pisa University Press, 37–57), we provide the eHealth stakeholders with a toolkit to map, analyze and apply the laws and regulations in order to achieve compliance. The chapter outlines a taxonomy for descriptive research in law and technology as a tool to map the regulatory field in their specific domain. It then proceeds to illustrate how the tool is to be applied and provides a non-exhaustive overview and analysis of the legal rules relevant for eHealth in Europe, with a focus on the safety and performance requirements to eHealth applications and platforms, and on data protection rights of the eHealth users. Further, we elucidate the role that the compliance-by-design strategies have in engineering legal requirements into the eHealth technology design and processes. It is suggested that the eHealth developers, sellers, and service providers engage in compliance by design in order to ensure and demonstrate compliance with the regulatory landscape.

N. Purtova (✉) • E. Kosta • B.-J. Koops
TILT – Tilburg Institute for Law, Technology, and Society,
Tilburg University, Tilburg, The Netherlands
e-mail: n.n.purtova@uvt.nl

S.A. Fricker et al. (eds.), *Requirements Engineering for Digital Health*,
DOI 10.1007/978-3-319-09798-5_3

3.1 Introduction

Traditional health care is being transformed though mobile health delivery, personalized medicine, and social media health applications. These trends create a new landscape of information and communication technologies aimed to improve health care, the so-called "eHealth." This new landscape takes shape against the backdrop of existing laws and regulations that may effect how the technology can be built or applied. Therefore, it is imperative that the eHealth developers, sellers, and service providers—stakeholders in the area of eHealth—are aware of the restraints and requirements that the regulation imposes. Yet the language of the regulator is not always easily translated into design features and application of technology. The aim of this Chapter is to facilitate this process and make first steps towards a methodology or, using the term adopted in the earlier chapters—the "cookbook," for interpretation of legal and regulatory rules into engineering requirements. The structure of this Chapter corresponds to the three goals identified for the eHealth stakeholders: (a) map laws and regulations relevant for the field, (b) design and use technology in a way compliant with these laws and regulations, and (c) demonstrate compliance.

Section 3.2 presents eHealth stakeholders with a taxonomy for descriptive research in law and technology as a tool to map the regulatory field in their specific domain (goal (a)). Section 3.3 is an exercise to apply the taxonomy. Importantly, the mapping of applicable legislation following the taxonomy is non-exhaustive. First, although the relevant legislative and regulatory measures exist on the international, regional, and national levels, to make the mapping exercise feasible, the overview is restricted to Europe and to a limited extent to the international law feeding into the European law. The EU legislative measures establish the core of the legal regime of the eHealth technology and can be used as a guideline for a more detailed national analysis. The specific national rules are wide-ranging and require in-depth knowledge of each specific national legal system; they cannot be mapped in the context of this Chapter. In addition to European law, non-European law may apply in case the eHealth solutions are intended to be used or exported outside of the EU. The legal picture then becomes much more complex, as many different legal regimes will apply. Further, the overview of the regulatory landscape here is meant to illustrate the application of the mapping methodology rather than exhaustively describe and analyze the regulatory landscape. The result of the exercise is a limited overview of the regulatory issues that emerged most prominently in the course of the FI-STAR project.[1] Finally, as existing law is usually not written for ehealth applications, the applicability of some rules, such as general product safety, to eHealth is yet uncertain and needs judicial interpretation or legislative clarification (Staff Working Document, p. 3). The European Commission has launched public consultations in April 2014 in order to clear the grey areas within the relevant legal fields. The outcomes of the consultations have yet to come. At present, there are two broad areas of legislation applicable to the eHealth solutions. (1) eHealth solutions operate in

[1] www.fi-star.eu/

the sensitive area of health where the application users may be inherently vulnerable. In addition, the innovative approach to health creates new vulnerabilities. Therefore, the first area of law applicable to the eHealth is users' rights. Data protection rights guarantee that personal (health) data of the users is collected and further processed fairly and lawfully; patients' rights ensure that the patient has access to the needed information, remedies reimbursement of costs; the consumer rights and electronic commerce legislation ensure that the user of the eHealth technology is not subject to unfair commercial practices. (2) Second, many eHealth applications and platforms are intended by their manufacturers to be used for therapeutic, diagnostic, or other clinical purposes. These applications and platforms may constitute *medical devices* and hence must comply with the EU safety and performance as requirements for medical devices. Section 3.3 will analyze these two broad clusters of legislation, and briefly touch upon intellectual property.

Analysis in Sect. 3.4 serves both goal (b) and (c). Section 3.4 presents *compliance by design*, a regulatory approach where regulatory requirements are accounted for on the earliest stages of technology design and implementation. Within the current regulatory context compliance by design is an important way not only to ensure, but also to *demonstrate* compliance with the existing regulatory framework. This Section explores two instances of *compliance by design* approach useful for the eHealth stakeholders to ensure and demonstrate compliance with the requirements of data protection: the Privacy Impact Assessment ("PIA"), the feedback-loop methodology of privacy risk assessment and mitigation; and Data Protection by Design ("DPbD"), the principle of data protection that requires to shape data processing technology and processes in a way compliant with the data protection law.

Section 3.5 highlights the problems and issues that one encounters when attempting to translate the regulatory concepts into engineering requirements. Section 3.6 offers summary and conclusions.

3.2 Methodology for Mapping Laws and Regulations

When planning and assessing legal compliance, it is important for stakeholders to carefully map the regulatory field. A useful tool for this mapping exercise is *a taxonomy for descriptive research in law and technology* [20]. This taxonomy describes four steps that can be followed in making a regulatory map for a certain technology or application. First, possibly relevant norms have to be identified. For eHealth, not only legal norms are relevant, but also norms in self-regulation or soft law, such as ethical guidelines, codes of conduct, or technical standards ([20], p. 42). Stakeholders should therefore have a broad understanding of regulation, when considering how to ensure compliance with all pertaining norms. Moreover, legal norms may not only be found in national law but also in supranational (e.g., European Union) or in subnational (e.g., state-level legislation in federal countries) law. Although health law will be the primary field to look into for legal norms, relevant norms may also be

found in criminal law (e.g., criminal liability for applications that cause severe bodily harm through gross negligence of the provider), contract law (regulating contracts with ICT service providers), tort law (e.g., product liability), consumer-protection law (e.g., rules on advertising products), intellectual-property law (e.g., patented elements of an e-health application), disability law (requirements for health applications' accessibility for people who cannot use smartphones), and environmental law (e.g., rules on disposal of sensor devices).

Second, once norms have been identified and selected, they should be analyzed to determine whether and how they apply to the technology or application at issue. The legal status (i.e., level of bindingness) should be clarified; fundamental rights law (e.g., privacy, non-discrimination) and statutory norms, or in common-law jurisdictions case-law, will be more important than soft law rules or guidelines from supervisory authorities. It should, however, be borne in mind that rules at different levels interact ([20], p. 48), and that detailed lower-level rules (e.g., in codes of conduct), which may not in themselves be binding, will color in higher-level rules, for example in determining open liability norms.

Third, as the interpretation whether and how a novel application is regulated under existing rules will not always be unequivocal, it is important to put the identified norms in perspective, describing their context and purpose. This is particularly important for e-health technologies or applications that are intended for a wider geographic market, as the norms in different countries may not only differ in their literal phrasing, but particularly also in their legal and cultural background. An analysis of the context and purpose of the norms at issue might also show that they are not suitable to be applied to a novel technology or application—sometimes the disconnection between innovative technologies and existing regulation is simply too large. In those cases, it is important to raise awareness with regulatory bodies, such as health regulatory authorities, and to seek their advice on how to proceed.

The final step is relevant if there is considerable uncertainty whether and how certain rules apply to novel and innovative technologies or applications. In such case it may be necessary to analyze diverse aspects that achieve a "thick description" of the regulatory field (see [20], pp. 51–55). These include the "default setting" of a norm, which depends on whether the "regulatory tilt" ([11], p. 21) is generally permissive or prohibiting (e.g., ICT regulation will usually be permissive, while life-science regulation will usually be more restrictive as a default). Also important to consider is whether and to what extent the technology or application affects fundamental rights (such as bodily integrity) and fundamental values (such as autonomy, human dignity, or equality). Finally, and this is particularly relevant to consider when regulatory compliance is achieved through design (*infra*, section 3), hidden constraints and biases should be uncovered. For example, engineers not seldom apply "I methodology," assuming that users have the same outlook as they have and will behave similarly as they themselves would [29], which risks bringing in a gender or cultural bias in the technological (compliance) design.

Following the consecutive steps of this taxonomy thus allows stakeholders to identify and interpret relevant norms. To assist stakeholders in starting their analysis, and within the limitations discussed in the introduction, we will discuss briefly the most important regulatory areas that eHealth applications will often face.

3.3 Mapping Relevant Laws and Regulations

3.3.1 Users' Rights

3.3.1.1 EU Data Protection Framework and Requirements

One of the latest kinds of eHealth solutions, i.e., mobile health applications, assist in diagnosis, monitoring, and treatment of diseases and various clinical conditions by means of collecting and analyzing personal data of patients: health records, wearable sensor data (e.g., pulse, blood pressure, temperature, blood glucose level), answers to well-being questionnaires, etc.[2] In cases of hereditary conditions personal data of patients' family may be collected as well. Identification data of medical professionals working with the eHealth solutions may be collected and further processed for authentication and other purposes. It is imperative that these practices comply with the European personal data protection rules, with special attention for the regime of health and medical data ([14], p. 193) as enshrined in the Data Protection Directive ("DPD").[3] The Directive is being reviewed and will likely be replaced by a more strictly harmonizing Data Protection Regulation ("DPR").[4] Since the contents of the Regulation are as yet under discussion, we base our description only on the DPD. The DPD establishes general principles of data protection, introduces individual (data subject's) rights and imposes obligations on individuals and organizations who determine if and how personal data is to be processed ("data controllers," Art. 2 DPD). Only data that are truly and irreversibly anonymous are exempted from the data protection regime ([23], p. 51).

Below follows an overview of the general principles of data protection, and a brief mapping of other data protection provisions. Specialized legal literature, e.g., Korff [22], offers a more comprehensive analysis of data protection.

Fair and Lawful Processing

Article 6(1)(a) DPD requires that personal data is processed fairly and lawfully. This means that certain legal conditions of data collection and further processing are fulfilled: data is collected and further processed for a specified purpose, under one of the legitimate grounds recognized by law (Article 7 DPD and 8 DPD, with regard

[2] 'Personal data' is "any information relating to an identified or identifiable natural person ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity" (Art. 2 (a) DPD).

[3] Directive 1995/46/EC, Official Journal 1995, L281/31.

[4] European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM(2012) 11 final – 2012/0011 (COD), 25.01.2012.

to the processing of health data), the data subject's rights (including information and control) are respected, the obligations of the data controller fulfilled (e.g., to notify a data protection authority). Moreover, "lawful processing" generally requires the data controllers to comply with all types of their legal obligations, general and specific, statutory and contractual, concerning the processing of the personal data.

Legitimate Ground

A eHealth application or platform can process personal data legitimately only if one or more of the grounds named in Article 7(a)–(f) of the DPD is present: (a) unambiguous consent by the data subject; (b) performance of a contract; (c) compliance with a legal obligation; (d) necessity to protect vital interests of the data subject; (e) necessity for a public-interest task of the controller; (f) a preponderant legitimate interest of the controller that outweighs the data subject's interest. For health data and other "special categories" of personal data, stricter requirements apply: processing is in principle forbidden, except in the cases mentioned in Article 8, which should be interpreted narrowly (WP 189, 6 [7]). The exceptions most relevant for eHealth are explicit consent of the data subject (Article 8(2) DPD) and processing in the context of a treatment relationship (Article 8(3) DPD). National laws of Member states can create additional exemptions or limitations on use of health data (Article 8(4) DPD) (WP 131 [2]).

(a) Consent

Data subject's consent, both regarding "non-sensitive" data and health data, must be freely given, specific (among others, to the particular purpose of processing) and informed. It must be an "indication of [the person's] wishes by which the data subject signifies his agreement to personal data relating to him being processed" (Art. 2(h) DPD). Some national laws require that consent is given in a particular form, e.g., written, or that subjects have a right to withdraw consent. In the latter case, withdrawing consent should be as easy as giving it.

Consent is *freely given* when it comes as a result of a "voluntary decision, by an individual in possession of all of his faculties, taken in the absence of coercion of any kind, be it social, financial, psychological or other. Any consent given under the threat of non-treatment or lower quality treatment in a medical situation cannot be considered as 'free'" (WP 131, 8). Consent to undergo a certain medical treatment does not imply consent for processing health data (ibid.), unless explicitly stated. Free consent also means that the data subject can withdraw the consent without detriment (WP 84 [1]). For processing personal data of medical professionals or other employees, it is important to note that some national data protection authorities do not regard consent as a legitimating ground in employer–employee relationships, or only if certain conditions are observed to ensure the consent is truly freely given, e.g., that employees do not face negative consequences for refusing to consent.

Consent is *specific* when it relates to a well-defined, particular situation. A "general agreement" to the processing does not constitute specific consent (WP 131, 9). For instance, in the stage of testing a eHealth solution with real data, it is important that the consent is given for the specific purpose of experimentation within a specific trial, clearly distinguishable and separate from other instances of consent, e.g., to participate in the clinical investigation.

Consent is *informed* if it is given based on an adequate understanding of the processing event(s) and their possible implications, as well as of the consequences of refusing consent. Information rights of the data subject play a key role in ensuring informed consent (ibid.).

Consent for processing health data must be *explicit*, which excludes "opt-out" solutions (Art. 8(2) DPD). However the Directive offers Member States the possibility to rule out the reliance on consent (even explicit one) for the processing of health data (Art. 8(2) DPD). Consent must explicitly relate to the sensitive nature of health data and demonstrate that data subjects are aware that they renounce the special protection (ban on processing) of health data. The controller must be able to demonstrate that the consent is valid in this respect (WP 131, 9).

(b) Context of treatment relationship

When an eHealth application involves processing of health data in the context of a treatment relationship, consent is not required. A treatment relationship means "the direct bilateral relationship between a patient and the health care professional/health care institution consulted by the patient" (WP 131, 11). The exception applies when processing must be (a) necessary (and not be merely "useful") (b) for the specific purpose of providing health-related services of a preventive, diagnostic, therapeutic or after-care nature and managing these services (e.g., invoicing, accounting, statistics), and (c) performed by medical or other staff subject to professional (medical) secrecy. Collected data cannot be passed on to other health care professionals or other third parties, unless the patient has given explicit consent or such an exception is foreseen by law.

It is important that data controllers carefully consider which legal ground suits their purposes. For instance, using a eHealth application in a hospital setting by medical professionals to collect and process health data of patients in the context of a treatment relationship may fall under the exemption and not require consent. Sat the same time, using real patient data in a test phase of the same eHealth solution is only possible with the explicit consent of the patients.

Purpose Limitation and Secondary Use

Many eHealth applications may want to rely on previously available personal health and other data, e.g., from (electronic) patient records, or to transfer collected data to the interfacing platforms/systems where the data could be used further for other purposes. This raises the issue of the so-called "secondary use" of personal data.

Personal data must be collected for "specified, explicit and legitimate purposes" (WP 203, 11–12 [9]) and cannot be further processed in ways that are incompatible with those purposes (Art. 6(1)(b) DPD). The underlying idea is not to let a one-time legitimization of a single instance of data processing provide a blank check for unlimited further uses of data. If personal data are processed further, the new purpose must be specified (WP 203, 11). Whether a secondary purpose is incompatible, depends on the interpretation—strict or flexible—under national law (WP 203, 25). In principle the initial purpose of processing can change, as long as the purpose of collection explicitly or implicitly includes the new purpose (WP 203, 22).

Data Protection Rights

The data subjects, the individuals to whom personal data pertain, e.g., patients or medical professionals, must be "in a position to learn" about the data processing operation and be given full and accurate information about the facts and circumstances of the collection of their personal data (Recital 38 DPD). The eHealth solutions must enable data subjects to exercise rights of access, rectification, erasure and the right to object to data processing or to block personal data that is incomplete, inaccurate or processed unlawfully (Arts. 12 and 14 DPD).

The Article 29 Working Party [8] issued specific recommendations on how to implement those rights in health-related apps. In particular, "apps must clearly and visibly inform their users about the existence of these access and correction mechanisms" which should be "simple but secure online access tools", available preferably "within each app, or by offering a link to an online feature" (WP 202, 25). These tools are especially important if sensitive (health) data is processed and have to be accompanied by verification mechanisms. The latter, however, should not lead to an additional, excessive collection of personal data (ibid.).

In case an automated decision is taken on the basis of the compiled data (e.g., if the patient is fit for further treatment), the data subject needs to be informed about the logic behind those decisions (ibid., Art. 15 DPD).

When data processing is based on consent, the users should be able to withdraw their consent in a simple and not burdensome manner. It must be possible for users to uninstall apps and thereby remove all personal data, also from the servers of the data controller(s) (WP 202, 25).

Data Security

In the context of the electronic patient records, the Article 29 Working Party (WP 202, 11) points out that even if all the requirements are met, such electronic health record systems "create a new risk scenario, which calls for new, additional safeguards as counterbalance." The same is true of eHealth solutions, as they involve additional actors in the health care relationships (App developers, App stores, and OS and device manufacturers). They shift the traditional boundaries of the

individual patient's relationship with a health care professional or institution. eHealth solutions introduce new ways of collecting and using medical data, create new data vulnerabilities including risks of destruction, unauthorized access, or data use for purposes other than treatment. Therefore, the requirement of data security is particularly important for eHealth.

The data controller has an obligation to take organizational and technical measures in order to ensure the adequate protection of personal data from any kind of unauthorized processing, including destruction, alteration, disclosure, and loss (Art. 17 DPD), both at the design stage and during the processing itself (e.g., Recital 46 of the DPD). The measures must be in proportion to the risks involved in the data processing and "the state of art and the cost of their implementation" (Art. 17(1) DPD). For eHealth applications, particularly strong security measures are called for, given the high sensitivity of data involved and possible high risks in case of a security breach. Security measures should already be incorporated when designing the processing system and the processing itself (Recital 46 DPD). Moreover, security requires "an ongoing assessment of both existing and future data protection risks." (WP 202, 18).

A controller also has an obligation to ensure, by way of a contract or other legal act (Art. 17(3) DPD), that those acting on his behalf—the "data processors"—provide sufficient technical and organizational security guarantees (Art. 17(4) DPD). As eHealth applications such as mobile health Apps often involve multilayered structures, security measures have to be taken by all actors on all levels: App developers, App store, and operation system and device manufacturers (WP 202, 18).

Several guidelines are available regarding security in general and security of mobile apps in particular (see, e.g., [15], WP 202, the ISO 27000 series of standards, and others). The Art. 29 Working Party recommends a number of specific security measures for the Health App developers (WP 202, 18–20):

- Recommendations regarding the choice of the storage models (on the device vs a client–server architecture);
- To clearly address security issues in the policies;
- To implement the "least privilege by default" principle, enabling the apps to access only the data they really need for functionality.
- To warn and remind users of good user practices, like updating software, using different passwords across different services, etc.
- To employ the so-called sandboxes—security mechanisms to separate running programs to reduce the consequences of malware/malicious apps.
- To use available mechanisms that allow users to see what data are being processed by which apps, and to selectively enable and disable permissions. The use of hidden functionalities should not be allowed.
- Not to use persistent (device-specific) identifiers but, instead, low entropy app-specific or temporary device identifiers to avoid tracking users over time;
- To employ privacy-friendly authentication (management of user-ids and passwords);
- To develop and provide to the users fixes or patches for security flaws, etc.

Other Provisions

Many other requirements in the DPD also need to be taken into account when developing and implementing eHealth applications. We mention a few here:

- The role of the *data controller* has to be clearly assigned. The controller bears most of the data protection obligations. In multi-actor eHealth applications, it can be a significant challenge to identify the responsible entities ([25], 223). Multiple controllers may share data protection obligations with regard to one processing operation. In determining the actors' roles and responsibilities, the emphasis should lie on the factual influences rather than on formal arrangements (WP 169 [4]);
- *notification* (Art. 18 DPD). The data controller must notify the Data Protection Authority of the processing operation and of the purpose(s) that this process serves. Some exemptions or simplified notification procedures may apply;
- data *quality* (Art. 6(1) DPD). Personal data should be valid, relevant and complete with respect to the purposes of processing ([12], 62). Data must be "accurate and, where necessary, kept up to date" (ibid.);
- *deletion* of data after use (Art. 6(1) DPD). Data can be processed only as long as it is necessary for the purposes for which the data were collected or for which they are further processed. As soon as the purpose has been fulfilled, the data should be deleted or (irreversibly) anonymized;
- *transfers to third countries* (Arts. 25 and 26 DPD). When health or other personal data is transferred outside of the European Economic Area (EEA),[5] a special regime applies. The recipient country must have an adequate level of data protection, or else the data controller must ensure adequate safeguards, e.g., through "appropriate contractual clauses" or so-called "Binding Corporate Rules" ("BCRs"). Certain derogations may apply according to Art. 26(1) DPD.

3.3.1.2 Patients' Rights Specific to Health Care

In contrast to the data protection rights that apply across contexts, as long as personal data processing is involved, the EU law also guarantees rights specific to the health care context. When eHealth solutions which are medical device[6] are tested before they are made available to medical practitioners ("device intended for clinical investigation"), patients' rights specific to the context of the clinical investigations have to be guaranteed before, during and after such investigation. When eHealth applications involve health care providers from more than one EU Member State, they may constitute instances of cross-border health care. Then the EU requirements on cross-border health care apply, in particular, Directive 2011/24/EU ("the Patients' Rights Directive").[7]

[5] EEA includes all EU member states (except Croatia, whose accession to the EEA is not yet finalized at the moment of writing) and Norway, Liechtenstein, and Iceland.

[6] Sect. 3.3.2.1 for the definition of the medical device.

[7] Directive 2011/24/EU (Patients' Rights Directive), Official Journal 2011, L88/45.

Clinical Investigations

Clinical investigation refers to "any systematic investigation or study in or on one or more human subjects, undertaken to assess the safety and/or performance of a medical device" (SG5/N1: 2007). Therefore, when an eHealth application or platform is tested that is intended by its manufacturer to be a medical device, a number of guarantees exist for the patients participating in the study.

The rights stem from the Helsinki Declaration ("HD") establishing Ethical Principles for Medical Research Involving Human Subjects,[8] and from the Council Directive 93/42/EEC on medical devices ("*MDD*") which incorporates the Helsinki principles.

The most important guarantees include the following:

- The requirement to assess and document risks and burdens to the patients compared with foreseeable benefits. With medical devices, serious adverse events must be recorded and notified to national competent authorities (s. 2.3.5 Annex X MDD).
- The investigation plan should provide measures of compensation and treatment in case subjects are harmed as a result of participating in research (Art. 15 HD). Provisions should be made for post-trial access for all participants to the positively tested eHealth solution (Art. 34 HD).
- Participation in the study, with some exceptions, is conditional on the subject's *informed and freely given consent*, guaranteed by a number of requirements and procedures (see Art. 27 HD). A freely given informed consent can be obtained and the information requirements can be met by means of a written consent form (Art. 26 HD). The subjects should be informed about their right to refuse or to withdraw from participation at any time without reprisal (Art. 26 HD).
- The trial can start after the ethical approval by an independent research ethics committee (Art. 23 HD). The clinical investigation of eHealth solutions classified as high-risk medical devices can begin 60 days after notification (Art. 15(2) MDD). In the course of the trial, the research ethics committee should be provided with all monitoring information, especially about any serious adverse effects (Art. 23 HD).

Patients' Rights in Cross-Border Health Care

eHealth applications often involve health care providers from more than one EU Member State and hence may constitute instances of cross-border health care. Then the EU requirements on cross-border health care apply, in particular, Directive 2011/24/EU ("the Patients' Rights Directive").[9]

---

[8] Helsinki Declaration establishing Ethical Principles for Medical Research Involving Human Subjects adopted by the 18th World Medical Assembly in Helsinki, Finland, in 1964, as last amended by the World Medical Assembly (the 'Helsinki Declaration').

[9] Directive 2011/24/EU (Patients' Rights Directive), Official Journal 2011, L88/45.

Cross-border health care means health services provided by health professionals to patients to assess, maintain, or restore their state of health, including the prescription, dispensation, and provision of medicinal products and medical devices—provided or prescribed in a EU Member State other than the patient's Member State (Art. 3 Patients' Rights Directive).

The *Member State of Treatment*, i.e., the Member State where treatment is provided, has an obligation to ensure that the health care providers supply to the patient the following information (Art. 4(2) Patients' Rights Directive):

- the relevant information to help individual patients make informed choices on treatment options, their availability, their quality and safety;
- information on price;
- information on the registration status, insurance cover, and other means of personnel or collective protection with regard to professional liability.

Patients' Member State must ensure that before or during cross-border health care, patients must have remote access to (or carry a copy of) their medical records. After treatment, to ensure continuity of care, they are entitled to a written or electronic medical record of the treatment (Art. 5 Patients' Rights Directive). These requirements may be implemented on the level of the eHealth application or platform architecture.

The Directive contains detailed rules on the reimbursement of costs, authorization systems, and administration procedures. Cross-border health care services also have to meet quality and safety standards laid down by the Member State of treatment, and Union legislation on safety standards[10] (Art. 4 Patients' Rights Directive).

3.3.2 Safety and Performance Requirements to Medical Devices

Safety and performance of products on the European market are regulated either by Directive 2001/95/EC[11] on general product safety ("General Product Safety Directive"/"*GPSD*"), or by specialized legislation applicable to a specific kind of products like the medical device directive. The GPSD applies when or to the extent the specific legislation is insufficient or absent.

The Commission Staff Working Document explains that it is unclear if and to what extent apps (and presumably other software) that do not qualify as medical devices are subject to GPSD, as the latter "appli[es] to manufactured products," (2014, 3) and presumably, not software. While the definition of a medical device explicitly includes software, the software is not mentioned in the definition of a

[10] See Sect. 3.3.2 for safety and performance requirements to medical devices.

[11] Directive 2001/95/EC of the European Parliament and the Council of 3 December 2001 on general product safety, Official Journal 11 l11/4, 15.1.2002.

product in Article 2(a) GPSD. In addition, lifestyle and well-being apps (and other software) may be beyond the scope of GPSD as one of the Directive's goals is "ensuring a consistent, high level of consumer health and safety protection," (Recital 26 GPSD) while the Commission Staff Working Document points out that "[i]t is not yet clear if and to what extent lifestyle and wellbeing apps could pose a risk to citizens' health" (2014, 3). The analysis below will be thus limited to the safety and performance requirements specific to medical devices under the Medical Device Directive (currently, being reformed).[12]

3.3.2.1 Defining a Medical Device

A eHealth solution, including software, is subject to MDD regime when it meets the legal criteria of the formal definition of a medical device or accessory to a medical device. The accessories to medical devices are treated as medical devices in their own right (Art. 1(1) MDD).

Importantly for eHealth, Atrt. 1(2)(a)MDD explicitly includes software into the definition of a medical device. A medical device is *"any instrument, apparatus, appliance, software, material or other article, whether used alone or in combination, including the software intended by its manufacturer to be used specifically for diagnostic and/or therapeutic purposes and necessary for its proper application, intended by the manufacturer to be used for human beings for the purpose of:*

- *diagnosis, prevention, monitoring, treatment or alleviation of disease,*
- *diagnosis, monitoring, treatment, alleviation of or compensation for an injury or handicap,*
- *investigation, replacement or modification of the anatomy or of a physiological process,*
- *control of conception,*

and which does not achieve its principal intended action in or on the human body by pharmacological, immunological or metabolic means, but which may be assisted in its function by such means."

There are no binding EU rules but Guidelines[13] concerning the delimitation between lifestyle/well-being apps (not subject to the MDD) and apps that are medical devices (subject to the MDD).

A key factor defining a medical device is the manufacturer's intent to have an app (or another device) used specifically for one of the health care purposes listed in Article 1(2)(a) MDD, to be judged by "the data supplied by the manufacturer on the labelling, in the instructions and/or in promotional materials." (Art. 1(2)(g) MDD, MEDDEV 2012, 11 [18])

[12] See the Proposal for a Regulation on medical devices and a Proposal for a Regulation on in vitro diagnostic medical devices (available at http://ec.europa.eu/health/medical-devices/documents/revision/index_en.htm), to replace the existing three directives.

[13] Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, MEDDEV 2.1/6 January 2012 ('MEDDEV 2.1/6 January 2012').

3.3.2.2 Requirements

Under Article 3(1) MDD, all applications that are medical devices must meet the *essential safety and performance requirements* which apply to them in light of their intended purpose. The essential requirements are listed in Annex I MDD.

The *essential requirements are the same* for the devices on the stage of development (intended for clinical investigation,[14] and not yet aimed at the final user) and for the devices ready for the end user (ready to be placed on the European market[15] and/or be put into service[16]), unless the device's intended use (Art. 3(1) MDD) renders some requirements not applicable.

In contrast, the *procedures to assess conformity with the essential requirements are different* for the devices intended for clinical investigation and devices to be placed on the European market and/or be put into service. The conformity assessment procedures are beyond the scope of this Chapter. In short, medical devices must bear the CE marking of conformity when they are placed on the market (Art. 17 MDD). Article 11 MDD prescribes which procedures should be followed to assess conformity with the standards ("essential requirement"). These procedures vary in intensity according to the type of the device. Devices intended for clinical investigation and custom-made devices do not need to bear the CE marking to ascertain that they are safe, but still have to go through relevant conformity assessment procedures. The degree of intensity of the conformity assessment procedures depends on a class assigned to an application (MDD Preamble): Classes I, IIa, IIb, and III; Class I being the lowest and Class III highest level of risk.[17] The eHealth applications and platforms will often be classified as Class I, lowest risk, devices.

The Compliance with the essential requirements is presumed when applications are in conformity with the relevant national standards adopted pursuant to the harmonized European standards (Art. 5 MDD).[18]

---

[14] 'Device intended for clinical investigation' means any device intended for use by a duly qualified medical practitioner when conducting investigations as referred to in Section 2.1 of Annex X in an adequate human clinical environment (Article 1(2)(e) MDD).

[15] meaning 'the first [made] available in return for payment or free of charge of a device other than a device intended for clinical investigation, with a view to distribution and/or use on the Community market, regardless of whether it is new or fully refurbished' (Article 1(2)(h) MDD).

[16] meaning 'made available to the final user as being ready for use on the Community market for the first time for its intended purpose' (Article 1(2)(i) MDD).

[17] Annex IX MDD establishes the criteria of classification. In June 2010 the Commission adopted guidelines on classification of medical devices (European Commission, "Medical devices: Guidance document – Classification of medical devices," Guidelines relating to the application of the Council Directive 93/42/EEC on medical devices, MEDDEV 2. 4/1 Rev. 9 June 2010, available at http://ec.europa.eu/health/medical-devices/files/meddev/2_4_1_rev_9_classification_en.pdf).

[18] The most recent list of the harmonized standards is to be found in the Commission communication in the framework of the implementation of the Council Directive 93/42/EEC of 14 June 1993 concerning medical devices of 24 January 2013, Official Journal of the European Union 2013/C 22/02 (at http://ec.europa.eu/enterprise/policies/european-standards/harmonised-standards/medical-devices/index_en.htm).

According to the general requirements, an eHealth application—as any medical device—must be safe in use, i.e., when used as intended, not compromise the clinical condition or safety of patients. The design of the ergonomic features of the application and of the environment, in which the application is intended to be used, should minimize the risk of use error. The design of the application should account for the technical knowledge, experience, education and training, the medical and physical conditions of intended users (section 1 Annex I MDD).

The solutions adopted in the application design must be safe within "the generally acknowledged state of the art." The choice of the solutions adopted in the application design must eliminate or reduce risks as much as possible, and must include protection measures against the risks that cannot be eliminated. The users have to be informed about any residual risks (section 2 Annex I MDD).

The combination of the application with other devices and equipment must be safe and must not impair specified performances of the devices. The application must not compromise safety or impair specified performance of other devices and equipment in the combination, or interfere with other medical devices (section 9.1 and 9.2 Annex I MDD).

Some of the most relevant specific safety and performance requirements include:

- The application that monitors clinical parameters must have an alarm system to alert the user of situations that could lead to death or severe deterioration of the patient's state of health (section 12.4 Annex I MDD).
- Under Section 12.1a Annex I MDD, when a medical device incorporates software or is software in itself, the software must be validated according to the state of the art taking into account the principles of development lifecycle, risk management, validation and verification. The FI-STAR applications are software and must comply with the state of the art requirement.

3.4 Compliance by Design

Compliance with the legal and regulatory framework relating to eHealth can be achieved by applying the "compliance by design" approach. In contrast to compliance by detection, where requirements are formulated and compliance is checked during or after the execution of the relevant process and necessitate technology or process redesign in case of violations, in compliance by design the rules are already taken into account when designing technologies and processes [24]. Employing compliance by design thus saves costs and risks of enforcement action. In addition, it provides tools to demonstrate compliance in case of audit. For instance, this is the approach to data protection accountability adopted by Article 29 Working Party and in the data protection reform.[19]

Standards can play facilitating role in compliance by design. Developed for the industry, they reduce the gap between the regulatory language and concrete compli-

[19] Section 3.4.2.

ance goals and steps understandable by the technology developers. Hence, they contribute to the compliance being engineered into technology. Compliance with the essential requirements for safety and performance of medical software including eHealth applications can be ensured and demonstrated by reference to standard IEC 62304: 2006 Medical device software—Software life-cycle processes regarding the process of manufacturing and replication of software that guides software design and provides for compliance goals for audit.

Below follows an overview of two compliance by design strategies for ensuring data protection. The Privacy Impact Assessment ("PIA") is a feedback-loop methodology of privacy risk assessment and mitigation; PIA ideally leads to certain requirements being engineered in the technology and/or the process. Data Protection by Design ("DPbD") is a principle of data protection that requires shaping data processing technology and processes in a way compliant with the data protection law. The deployment of Privacy by Design can be assisted by Requirements Engineering. Both strategies are endorsed by the regulator. Similar strategies may be developed in other fields.

3.4.1 Privacy Impact Assessment ("PIA")

3.4.1.1 Importance and Implementation So Far

Compliance with data protection laws and mitigation of data privacy risks are key indicators of quality of eHealth solutions, considering that such solutions involve processing of sensitive health data. Privacy Impact Assessment ("PIA") provides a tool to both *ensure* and *ascertain* that an eHealth product, service, or process does not present or effectively mitigates data privacy risks.

PIA refers to both methodology and a process ([33], 55). As a process, PIA should begin on early stages of design and last throughout the entire lifecycle of technology, application or process so that the latter can be changed to account for data privacy and security risks (ibid.). The PIA process should be ongoing and repeated in case any change is made in the product or process.

Currently, there is no general EU legal requirement to conduct a PIA.[20] Nevertheless, conducting a PIA brings a number of benefits ([33], 55) characteristic to a compliance by design approach. Most importantly,[21]

- PIA is an early warning system. It alerts about data privacy risks and allows to account for them on time;
- PIA aids demonstrating compliance with data protection legislation, among others, via a PIA report. A well-executed PIA may mitigate or even exclude civil liability under particular circumstances [17].

[20] Although Article 20 of the Data Protection Directive on prior checking when data processing presents specific risks is considered a predecessor to PIA.

[21] The overview below is based on the list of benefits described by Wright [33].

- PIA can aid in gaining public's—medical professionals' and patients'—trust in eHealth technology.
- PIA educates organization's employees and partners about the organization's respect of and similar expectations towards employees and partners concerning privacy.
- An industry or organization initiating a PIA may avoid undesired regulatory interference ([33], 55).
- Ultimately, the resulting high level of data protection, low level of data risks and trust may have a positive effect on adoption of relatively new eHealth technologies.

PIA has been widely used by businesses like Nokia, Siemens, Vodafone, and others [34] as a self-regulatory mechanism to ensure compliance with data protection. So far, two PIA frameworks have been submitted by industries for endorsement by the Article 29 Working Party—the EU data protection advisory authority: the PIA Framework for RFID Applications[22] and the Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems ("DPIA Template"). The latter has been denied endorsement (WP 205 [10]). The endorsed RFID PIA Framework [30][23] and the Working Party opinions regarding the framework ([5], WP 175)[24] have certain persuasive authority to structure PIA efforts in other sectors, with the necessary adjustments for the contexts of a given sector like health care.

The RFID PIA process consists of the initial analysis and risk assessment phases. The *initial analysis* phase allows to determine if and which intensity of PIA—"full scale" or a "small scale"—is needed (RFID PIA Framework, 7).

The *risk-assessment* includes (1) identifying privacy risks caused by an RFID application, and (2) planning and documenting organizational and technical measures to mitigate those risks (RFID PIA Framework, 7–8). The risk-assessment phase is executed in four steps:

Step 1: a comprehensive description of the application, its system boundaries, interfaces with other systems, personal data flows, operation and strategic environment, e.g., stakeholders involved in information collection, the system's mission. (RFID PIA Framework, 9).

Step 2: mapping "conditions that may or compromise personal data," using Data protection legislation as a guide to identify privacy targets to be protected. Annexes II and III to the RFID PIA Framework contain a list of nine privacy targets and risks. The RFID operator should consider the significance and likeli-

[22] Privacy and Data Protection Impact Assessment Framework for RFID Applications, transmitted to Article 29 Working Party on 12 January 2011 ('RFID PIA Framework'), available online at www.cordis.europa.eu

[23] The RFID PIA framework endorsed by the Art 29 WP (Opinion 9/2011 on the revised Industry Proposal for a Privacy and Data Protection Impact Assessment Framework for RFID Applications, WP 180) and was officially signed on 6 April 2011, www.ec.europa.eu/information_society/policy/rfid/documents/rfidpiapressrelease.pdf

[24] The RFID framework was endorsed after a round of revision, incorporating the feedback given in WP 175.

hood of privacy risks occurring, as well as the magnitude of the impact if such risks occur (ibid).

Step 3: analysis of measures (to be) taken to mitigate or eliminate the risks identified in Step 2: technical measures, implemented into the application's architecture ("privacy by design") like default settings, encryption, authentication, etc.; non-technical measures include management and operational procedures (RFID PIA Framework, 10).[25]

Step 4: documentation of each PIA step and the final resolution concerning: approved, with relevant risks identified and addressed and no significant residual risks remaining, or not approved in its current state, requiring corrective action). Step 4 ends with a PIA Report, documenting both stages and their results and made available to the data protection authority (ibid).

To support the execution of the PIA process, the RFID PIA Framework established a number of internal procedures, like scheduling and review of PIA, documentation, identifying triggers for a PIA revision, and stakeholder consultations (RFID PIA Framework, 5).

3.4.1.2 PIA Methodology for eHealth

Article 29 Working Party's feedback and approval of the RFID PIA framework and the feedback on the rejected smart grid PIA template provide insights into endorsed PIA methodology.

A PIA should be based on a risk-management approach (WP 175, 5; WP 180, 7 [6]). Hence, a PIA framework should include a *risk assessment stage* as a key component, also to enable evaluation of the respective risk-minimizing measures (WP 175, 7). As an option, the risk assessment can be done in the four steps adopted in the RFID PIA Framework. In identifying the risks, it is important to fully consider all risks: both intended and unintended or unauthorized uses and misuses of technology[26] (WP 175, 9; WP 180, 5). Risks should not be confused with threats (WP 205, 7), where risks are "the *potential* that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm"[27] and threats refer to "*the ability* to exploit vulnerabilities" (WP 205, 7). A PIA framework should give specific guidance on how to calculate and prioritize risks, choose appropriate "controls" (risk mitigating measures) and assess the residual risks. The guidance should be sufficient on its own for the implementing organizations to use, without the need to refer to external documents (WP 205, 8).

[25] Some examples of 'controls' are given in Annex IV to the RFID PIA Framework.

[26] WP 180, p. 5, e.g., unauthorized monitoring of RFID tags (WP 175, p. 9).

[27] ISO/IEC 27005:2008 definition of risks cited in WP 205, p. 7.

A PIA should be industry-specific and not generic, both in identifying the risks and the mitigating measures (ibid)[28]. A PIA should directly address: the potential impact on a data subject (a patient, medical professional or other technology user) and the privacy and data protection targets. Addressing the targets alone is not a sufficient element of a risk-based approach (ibid., 7).

Yet, identifying privacy targets may help channel the PIA and compliance efforts in general (ibid). The RFID PIA Framework identifies nine privacy targets, based on the General data protection directive 95/46/EC. These nine targets can be used as a model and changed to accommodate a specific context of the technology subject to PIA: (1) safeguarding quality of personal data; (2) legitimacy of data processing; (3) legitimacy of processing special categories of personal data; (4) compliance with the data subject's right to be informed; (5) compliance with the data subject's right of access to data, correct and erase data; (6) compliance with the data subject's right to object; (7) safeguarding confidentiality and security of processing; (8) compliance with notification requirements; (9) compliance with data retention requirements (RFID PIA Framework, Annex II).

The identified risks should be directly matched to the mitigating measures, like in the information security standard ISO/IEC 27002: 2005 (WP 205, 7). A risk assessment approach can build on the methodology of various national and international standards, like information security management standards (e.g., ISO/IEC 27005[29]), and recommendations of the European Network and Information Security Agency (ENISA) (WP 175, 7).

When assessing the risks, a special attention should be paid to what may or may not be considered personal data and hence, if data processing takes place. Thus, if a unique identifier is associated to a person, it is personal data even though it does not reveal that person's social identity (WP 136 [3]). Identifying whether or not *special categories* of personal data are to be processed, and the uses of such data should be part of the risk assessment, with a special attention to how it can be processed lawfully and securely (WP 175, 10).

A PIA should provide guidance to determine who bears various data processing and data protection responsibilities, e.g., by means of mapping relevant actors in a given sector and helping to identify who acts as a controller or processor (WP 205, 8).

A *PIA procedure* should include stakeholder consultations with interested parties. This stage should result in suggestions and improvements of both a PIA procedure and the technology (WP 175, 10; WP 180, 5). Each PIA framework will likely require adjustment through experience and stakeholder feedback (WP 180, 6).

In addition to drawing up a PIA Report and making it available to a competent authority, a concise and easy to understand information policy should be published including a summary if the PIA (ibid.).

[28] The endorsed RFID PIA Framework could be used as a model of a comprehensive PIA framework. It provides guidance how to describe the technology subject of evaluation (Annex I); privacy targets based on the Data protection directive 95/46/EC (Annex II); possible privacy risks in the area of RFID (Annex III); and a list of examples of RFID application controls and mitigating measures, both technical and organizational (Annex IV).

[29] ISO/IEC 27001:2005, Information technology—Security techniques—Information security management systems—Requirements.

A PIA methodology should suggest the most appropriate time for conducting a PIA in order to account for the privacy risks on the stage of designing a system to truly implement the principle of privacy by design (WP 175, 10).

3.4.1.3 Future Data Protection Impact Assessment

At the moment, the EU data protection framework, including its approach to Privacy Impact Assessment, is going through a reform process, but it is likely that Data Protection Impact Assessment (the term used instead of "Privacy Impact Assessment") will be an important aspect of compliance with future European data protection law. This overview refers to the latest version of the proposed General Data Protection Regulation [13] ("GDPR")—to substitute the DPD—the European Parliament legislative resolution of 12 March 2014.[30]

The most important change (should the Parliament amendments make it to the final text) will be that the DPIA will be mandatory if certain triggers provided by law occur (Art. 33 GDPR). The initial risk assessment is always mandatory.

The DPIA in the GDPR has an in-built *feedback loop* to adjust the data processing practices/technology and the DPIA processes depending on the DPIA's outcomes. The difference is that the DPIA is only one part of that loop labelled the "Lifecycle Data Protection Management"—a process of managing personal data from its collection to deletion (Recital 61, GDPR).

The Lifecycle Data Protection Management is executed in the following stages:

1. *Risk analysis* of intended data processing, aiming to establish the potential impact on the rights and freedoms of the data subjects, and if the intended processing is likely to present specific risks (Art. 32a GDPR).

Considering the results of the risk analysis a controller or, where appropriate, a processor:

2. *designates* a data protection officer; and/or
3. *consults* the data protection officer; and/or
4. *carries out DPIA* (Art. 33).

The DPIA under the reform contains, among others, a comprehensive description and purposes of the intended data processing; assessment of its necessity and proportionality; description of the measures to mitigate the risks, with due regard to the context of data processing, etc. The DPIA is followed by a periodic compliance review aiming at demonstrating compliance with the Regulation (Art. 33a GDPR). The review results in recommendations either by the data protection officer or the national data protection authority on how to achieve full compliance.

[30] European Parliament legislative resolution of 12 March 2014 on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)).

3.4.2 Data Protection by Design ("DPbD")

Data protection by design is an instance of compliance by design soon to become a new principle of the European data protection law (Art. 23 GDPR). It sets out the obligation of the controller both at the time of the determination of the means for data processing and at the time of the processing itself, to implement appropriate technical and organizational measures and procedures to meet the requirements of the Regulation and ensure the protection of the rights of data subjects. DPbD is an integral part of strengthening accountability for data processing in the new GDPR, i.e., recountability does not only require actual implementation of the data protection requirements but also the ability to demonstrate compliance (Art. 22 GDPR).

The concept of privacy by design originates in Canada. In 1990 Cavoukian developed 7 Foundational Principles to provide guidance on privacy by design.[31] The principles aim to: "proactively make privacy the default setting in all areas of technological plans and business practices and explain how privacy should be embedded into the design of systems, in a positive-sum manner—that does not detract from the original purpose of the system."[32]

The GDPR establishes a clear link between data protection by design and data protection impact assessments: Article 23 GDPR explicitly states that if a data protection impact assessment has been carried out, the results hereof need to be taken into account in developing the measures and procedures required on the basis of data protection by design. Importantly for eHealth stakeholders in public health care, the GDPR text also introduces data protection by design as a prerequisite in public tenders according to the Directive on public procurement and the Utilities Directive.[33]

3.5 Discussion: Contribution to the State of Art Scholarship and Challenges for Legal Requirements Engineering

The following Section is a discussion of the contribution of this Chapter to the state of art research regarding engineering legal and regulatory norms into eHealth technology and processes.

[31] For an overview of all 7 principles: IESO (2011), 12–13.

[32] IESO(2011), 5.

[33] Directive 2004/17/EC of the European Parliament and of the Council of 31 March 2004 coordinating the procurement procedures of entities operating in the water, energy, transport and postal services sectors, OJ L 134, 30.4.2004, p. 1–113.

Directive 2004/18/EC of the European Parliament and of the Council of 31 March 2004 on the coordination of procedures for the award of public works contracts, public supply contracts and public service contracts, OJ L 134, 30.4.2004, p. 114–240.

3.5.1 Contribution to Legal Requirements Engineering

This Chapter has presented an integrated approach to legal requirements engineering in the context of eHealth, bringing together a methodology for mapping existing legal and regulatory landscape and the strategies to interface the identified rules and design of the eHealth technology and processes. Drawing on earlier works of Koops [20], we provide the eHealth stakeholders with a toolkit to map, analyze and apply the laws and regulations in order to achieve compliance. Further, we elucidate the role that the compliance-by-design strategies have in engineering legal requirements into the eHealth technology design and processes. In particular, as discussed in Sect. 3.4, in addition to saving costs and risks of enforcement action, the compliance by design approach forces the eHealth stakeholders to think about compliance issues on the earliest stages of developing and applying eHealth technology; and make architectural and design choices from the compliance perspective. This is a key value of compliance by design for the undertaking of the legal requirements engineering. Some instances of compliance by design strategy, such as Privacy Impact Assessment and Data Protection by Design, have been developed and embedded in the current compliance practice. This Chapter also emphasizes the role of standards in compliance by design and legal requirements engineering. Developed for the industry, standards reduce the gap that exists between the regulatory language/generally stated compliance goals on the one hand and concrete technology requirements easily transferrable into technology design. The work on standardization of eHealth technology should be continued both to make the laws and regulations more effective, but also to ease the process of adopting the laws and regulations into technology design.

3.5.2 Recommendations to eHealth Stakeholders

Next to recommendations to the policymakers and researchers active in the field of eHealth (in the following Sect. 3.5.3), the research that this Chapter presents has allowed us to formulate a number of recommendations for the eHealth stakeholders—developers, sellers, service providers, etc.—when they use the integrated approach presented in this Chapter for legal requirements engineering for compliance:

- The laws and regulations relevant for eHealth are country/region specific. It is recommended that—on the earliest stages of design—the stakeholders consider where in the world they want to market/use a given eHealth solution, and proceed mapping and applying legal rules accordingly. Although considerable efforts have been taken to harmonize laws in Europe and—to a limited extent—internationally, the requirements in every given country may differ significantly enough to affect technology design.
- The laws and regulations relevant for eHealth are context-specific. Different circumstances of the eHealth implementation, targeted users, and use settings may have a decisive effect on the application of the rules. Therefore, no universally

applicable matrix of legal and other regulatory rules exists. Therefore, the mapping and analysis of the laws and regulations should be done by a legal expert.
- Once the applicable rules are mapped, they need to be translated into technology design as early as possible in the development process. A system of continuous monitoring and audit should be in place to verify if the design still achieves compliance goals when design features are modified. Privacy Impact Assessment process is a useful tool to achieve this in the area of data protection.
- Use of harmonized standards may aid in bridging the gap between the laws and regulations and concrete technology design choices.

3.5.3 Challenges

While mapping and analyzing the legal and regulatory landscape of eHealth, and attempting to translate them into requirements for design, we have encountered a number of challenges that need to be addressed by policymakers and research. The eHealth stakeholders engaging in compliance by design and engineering compliance with the legal and regulatory requirements in the design of the eHealth technology and processes, face two important challenges: first, identifying the full range of the applicable norms, and analyzing the norms in order to infer concrete requirements for technology; second, translating laws and regulations to policies and software to achieve compliance targets. Both can be challenging.

3.5.3.1 Mapping and Assessing Rules

The mapping of laws and regulations for eHealth shows the legal and regulatory landscape relevant for engineers, systems developers and auditors of eHealth applications when designing, implementing and auditing eHealth technology and its implementation. However, the eHealth technology functions within the existing context of legal and regulatory rules not drafted for the innovative eHealth technology. Therefore, it is challenging to identify with certainty whether or not some areas of law and regulation apply to eHealth, and if yes, how exactly. For instance, some rules may be applicable to the app stores selling the eHealth applications and not to the developers and the applications themselves, and the applicability of other rules may depend on whether or not an eHealth solution is targeted at the patients of a particular hospital or is publicly available. Here are some examples.

The application of some rules is very context-specific. The *Consumer Rights Directive*[34] and *eCommerce Directive*[35] are relevant for ensuring EU-wide level of protection when a consumer buys a lifestyle and well-being app online (Staff Working Document, 7).

[34] Directive 2011/83/EC on consumers' rights repealing Directive 97/7/EC as of 13 June 2014.

[35] Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market.

The Consumer Rights Directive (Arts. 1 and 3(1)) replaces, as of 13 June 2014, Directive 97/7/EC on the protection of consumers in respect of distance contracts[36] and Directive 85/577/EEC to protect the consumer in respect of contracts negotiated away from business premises.[37] It establishes information rights of the consumer relevant before the conclusion of a contract whether or not it is concluded at a distance. If eHealth applications are not purchased or offered to the users online, but at the hospitals (pharmacies) providing the eHealth service, the rules on the distance contracts do not apply. However, when the off-line contact is not within the scope of functionality of the application, the distance contract provisions are of direct relevance.

The Consumer Rights Directive does not apply to health care services (Art. 3(3)(b)), i.e., services provided by health professionals to patients to assess, maintain or restore their state of health (Art. 3 Patients' Rights Directive). However, the Directive does apply to the app stores selling eHealth applications, or to the eHealth service providers who are not medical professionals, and to the eHealth applications which are not meant for therapeutic, diagnostic, and other clinical purposes but rather aim at a healthy lifestyle.

The *eCommerce Directive* aims to approximate the national legislation in order to ensure free movement of information society services. The issues of approximation include information rights, rules of concluding contracts by electronic means, liability of intermediaries, etc. Information society services are defined as services normally provided for remuneration, at a distance, by means of electronic equipment for the processing and storage of data, and at the individual request of a recipient of a service (Art. 1(1) and 1(2)). The Commission regards the app stores selling health and well-being apps, and app developers selling the apps directly, information society service providers (Staff Working Document, p. 9). However, not all eHealth applications constitute information society services, e.g., the applications not provided at the individual request of the users but are a part of prescribed treatment (e.g., the rehabilitation application). The activity of the application stores, on the other hand, does constitute information society services and therefore the eCommerce directive applies.

Competition (or antitrust) law may be of relevance in countries that introduce some market organization in their public health system [31]. This affects pricing schemes and has implications for procurement procedures. The extent to which these rules apply depends on the particular case ([26], 337). Similarly, the regulation of the free movement of people and services within the internal market might

[36] Directive 97/7/EC of the European Parliament and of the Council of 20 May 1997 on the protection of consumers in respect of distance contracts, OJ L 144, 04/06/1997, p. 19–27, available at http://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:31997L0007.

[37] Council Directive 85/577/EEC of 20 December 1985 to protect the consumer in respect of contracts negotiated away from business premises, Official Journal L 372, 31/12/1985 P. 0031 – 0033, available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31985L0577:en:HTML.

apply to (modular-based) medical architectures, in which (combinations of) the provider, the service, or the recipient can move between countries [27, 19].

The application of other rules to the area of eHealth still needs to be clarified by the regulator. As discussed earlier, it is unclear if and to what extent apps (and presumably other software) that do not qualify as medical devices are subject to GPSD, as the latter "appli[es] to manufactured products," (Staff Working Document 2014 [16], 3) whereas software is not explicitly mentioned as a product. For the same reason, it is also unclear if the European rules on liability for damages caused by a defective product apply to the eHealth domain.[38] For modular architectures, liability provides complex challenges because they involve multiple actors responsible for not only patient apps, but also interfacing platforms: clouds, hospital environments, smartphones, etc. Some argue that in telemonitoring applications, the responsibility of patients themselves to comply with the monitoring schemes should be factored in liability distribution [32]. Developers and providers of eHealth applications are recommended to make a risk assessment of liability risks in the framework of their national liability regime.

3.5.3.2 Interfacing Laws and Regulations with eHealth Technology

The engineering of legal and other regulatory rules into eHealth systems and processes is a core of compliance by design, a regulatory approach that is praised for cost-efficiency, effectiveness and preventive effect. Including data protection considerations in design of eHealth systems that process personal data will likely become an obligation under the data protection law. In reality, the translation of laws and regulations to policies and software rules that are necessary to achieve compliance remains a major challenge for requirements engineering ([28], 5), as the hard-coding of certain types of laws often goes beyond the simple transformation and representation of rules ([21], 4). The broad range of documents and the dependencies between various rules that have to be considered for the identification of legal requirements can prove to be an impossible task for software developers to handle ([28], 6).

In relation to the engineering of data protection and privacy requirements, which will probably be soon required by law, Koops and Leenes have identified three complicating issues. First, it is difficult to delineate the scope of data protection requirements: the data protection rules can be found both at the European and the national level, while they can be general as well as domain-specific. Second, the data protection rules play different roles in systems that process personal data and can reflect requirements at different engineering levels, e.g., at system level, runtime requirements or language requirements. Third, data protection is developed around the central principles of purpose specification and use limitation. However, any purpose of data processing defined in a natural language is prone to a variety of interpretations ([21], 5–7).

[38] Council Directive 85/374/EEC on liability for defective products, Official Journal 1985, L210/29.

3.6 Summary and Conclusions

This Chapter has made first steps towards creating an interface between the content of the laws and regulations in the field of eHealth and the requirements that can be engineered into the eHealth technology and processes. The analysis was structured to satisfy three needs of the eHealth stakeholders: First, in order to aid mapping the landscape of laws and regulations, a taxonomy for descriptive research in law and technology was presented as a tool to map the regulatory field in their specific domain. To illustrate how the taxonomy approach is to be applied, a high-level overview of the laws and regulations in the field of eHealth was given, with a special emphasize on the rights of the eHealth users and safety and performance requirements to the eHealth applications and platforms that are medical devices. Further, in order to facilitate compliant technology design and aid demonstrating compliance, this Chapter outlines some compliance by design strategies, with a special attention to Privacy Impact Assessment and Data Protection by Design that are quickly becoming a necessary element in the new European approach to data protection enforcement and accountability. The Chapter concluded with a discussion of the challenges of mapping and translating laws and regulations into the eHealth architecture and processes, some recommendations to the eHealth stakeholders engaging in the rules mapping and compliance by design, and the regulators involved with the eHealth domain. Finally, some needs for future research have been identified.

The research preceding writing of this Chapter has shown that compliance with laws and regulations is an exercise that does not always result in certain outcomes. The main reason is that the eHealth solutions present a new approach to health care, but also create new risks and vulnerabilities and the regulator is unaware of them (e.g., risks of eHealth apps for consumer health are uncertain) or has not come up with a position. We call the research in the domain of eHealth to support the regulator in these important challenges.

References

1. Article 29 Working Party (2001) Opinion 8/2001 on the processing of personal data in the employment context. (WP 84)
2. Article 29 Working Party (2007) Working document on the processing of personal data relating to health in electronic health records (EHR). Adopted on 2007 (WP 131)
3. Article 29 Working Party (2007) Opinion 4/2007 on the concept of personal data (WP 136)
4. Article 29 Working Party (2010) Opinion 1/2010 on the concepts of controller and processor (WP 169)
5. Article 29 Working Party (2010) Opinion 5/2010 on the industry proposal for a privacy and data protection impact assessment framework for RFID applications (WP 175)
6. Article 29 Working Party (2011) Opinion 9/2011 on the revised industry proposal for a privacy and data protection impact assessment framework for RFID applications (WP 180)
7. Article 29 Working Party (2012) Working document 01/2012 on epSOS. Adopted on 25 January 2012 (WP 189)

8. Article 29 Working Party (2013) Opinion 02/2013 on apps on smart devices. Adopted on 27 February 2013 (WP 202)
9. Article 29 Working Party (2013) Opinion 03/2013 on purpose limitation. Adopted on 2 April 2013 (WP 203)
10. Article 29 Working Party (2013) Opinion 04/2013 on the data protection impact assessment template for smart grid and smart metering systems ('DPIA Template') prepared by Expert Group 2 of the Commission's Smart Grid Task Force. Adopted on 22 April 2013 (WP 205)
11. Brownsword R (2008) Rights, regulation and the technological revolution. Oxford University Press, Oxford
12. Bygrave L (2002) Data protection law: approaching its rationale, logic and limits. Kluwer Law International, New York, NY
13. Committee on Civil Liberties, Justice and Home Affairs (2013) Report on the proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD)) 21 November 2013
14. Dumortier J, Goemans C (2004) Privacy protection and identity management. In: Blažič B, Schneider W (eds) Security and privacy in advanced networking technologies. Ios Press, Amsterdam
15. ENISA (2011) Smartphone secure development guideline. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/smartphone-secure-development-guidelines
16. European Commission (2014) Commission staff working document on existing EU legal framework applicable to lifestyle and wellbeing apps, Accompanying the document Green Paper on mobile Health ("mHealth"), COM(2014) 219 final, Brussels, 10 April 2014 ('Staff Working Document')
17. Gellert R, Kloza D (2012) Can privacy impact assessment mitigate civil liability? A precautionary approach. In: Schweighofer E, Kummer F, Hötzendorfer W (eds) Transformation juristischer Sprachen, from Tagungsband des 15. Internationalen Rechtsinformatik Symposions IRIS 2012. Osterreichische Computer Gesellschaft, Vienna, pp 497–505
18. Guidelines on the qualification and classification of stand-alone software used in healthcare within the regulatory framework of medical devices, MEDDEV 2.1/6, January 2012 ('MEDDEV 2.1/6 January 2012')
19. Hervey T, Trubek G (2007) Freedom to provide health care services within the EU: an opportunity for a transformative directive. Columbia J Eur Law 13:624ff
20. Koops B-J (2013) A taxonomy for descriptive research in law and technology. In: Palmerini E, Stradella E (eds) Law and technology: the challenge of regulating technological. Pisa University Press, Pisa, pp 37–57
21. Koops B-J, Leenes R (2013) Privacy regulation cannot be hardcoded. A critical comment on the 'privacy by design' provision in data-protection law. Int Rev Law Comp Tech 28(2):159
22. Korff D (2008) Data protection laws in the European Union. FEDM
23. Kuner C (2008) European data protection law – corporate compliance and regulation. Oxford University Press, Oxford
24. Lohmann N (2013) Compliance by design for artifact based business processes. Inf Syst 38(4):606
25. Löhr H, Sadeghi A-R, Winandy M (2010) Securing the e-health cloud. In: Proceedings of the 1st ACM international health informatics symposium, ser. IHI'10. ACM, New York, NY
26. Lear J, Mossialos E, Karl B (2010) EU competition law and health policy. In: Mossialos E, Permanand G, Baeten R, Hervey T (eds) Health systems governance in Europe. Cambridge UP, Cambridge
27. Mossialos E et al (eds) (2010) Health systems governance in Europe. Cambridge UP, Cambridge, Chapters 10–12
28. Otto PN, Anton IA (2007) Addressing legal requirements in requirements engineering. In: 5th IEEE international requirements engineering conference (RE 2007). IEEE, Washington, DC

29. Oudshoorn N, Rommes E, Stienstra M (2004) Configuring the user as everybody: gender and design cultures in information and communication technologies. Sci Tech Hum Val 29(1):30–63
30. Article 29 Working Party (2011) Privacy and data protection impact assessment framework for RFID applications. Transmitted on 12 January 2011 ('RFID PIA Framework'). Available from: www.cordis.europa.eu
31. Prosser T (2010) EU competition law and public services. In: Mossialos E, Permanand G, Baeten R, Hervey T (eds) Health systems governance in europe. Cambridge UP, Cambridge, pp 315–336
32. Vedder AH, Vantsiouri P. Building trust in E-Health Services, unpublished
33. Wright D (2012) The state of the art in privacy impact assessment. Comp Law Secur Rev 28:54
34. Wright D, De Hert P (eds) (2010) Privacy impact assessment. Springer, Dordrecht