Norms and Standards in Modular Medical Architectures

Christoph Thuemmler, Oli Mival, David Benyon, William Buchanan, Alois Paulin
Institute of Informatics & Digital Innovation; Edinburgh Napier University; Edinburgh, UK
Contact: c.thuemmler@napier.ac.uk

Samuel Fricker, Markus Fiedler
Blekinge Institute of Technology; Karlskrona, Sweden

Bert-Jaap Koops, Eleni Kosta
Tilburg University; Tilburg, The Netherlands

Astrid Grottland
University Hospital of North Norway; Tromsø, Norway

Armin Schneider
Technical University Munich; Munich, Germany

Thomas Jell
Siemens AG; Munich, Germany

Anastasius Gavras, Maria Barros
Eurescom; Heidelberg, Germany

Thomas Magedanz
Technical University Berlin; Berlin, Germany

Philippe Cousin
Easy Global Market SAS; Sophia Antipolis, France

Ioana Ispas
Ministry of National Education; Bucharest, Romania

Euripides Petrakis
Technical University Crete; Chania, Greece

***Abstract*— Recent Internet of Things (IoT) research has been aiming at interoperability of devices and the integration of sensor networks. The Future Internet – Private Public Partnership (FI-PPP) has created a whole array of different purpose-oriented modules with defined specifications, better known as Generic Enablers. This article gives an overview of legal, ethical and technical norms and standards to be considered when planning, developing and implementing modular medical architectures, integrating the Internet of Things (IoT) and Generic Enablers (GEs) in cutting edge, latest generation medical data networks.**

Keywords*— *Generic Enablers; Core Platform; Standards; e-Health; Telehealth; IoT; Governance; Medical Data Networks

I. INTRODUCTION

More and more technologies have become available for the use in medical data networks. Currently we see a parallel development of two main technical flows, which have been both subject to extensive research funded by the European Commission: On the one hand stands the evolution of smart devices driven and fuelled through Nano-technology and a general reduction of weight, size and price. In this category we find bio-sensors, artificial organs such as insulin pumps and defibrillators, pacemakers, active and passive Radio Frequency Identification (RFID) tracking devices but also smart devices used in the area of ambient assisted living, such as accelerometers, glucometers and a huge diversity of mobile computer and smart phone based applications. Over recent years these technologies were largely discussed under the heading "Internet of Things" (IOT) and prime areas of interest seemed to be grouped around interoperability, security and robustness. Public clouds seemed to be a perfect architecture to link smart devices remotely and seamlessly and solve all of the interoperability and compatibility issues. However, initiatives to establish public e-health clouds, which would be accepted by health care providers failed and the dissemination of e-health technologies stalled. New impulses might be set by the proposal of a new hybrid cloud model based on a "software to data" approach without any need to reveal patient data to cloud providers [1]. Recent communication between the European Commission and the European Parliament has identified areas, which will be tackled by future initiatives to improve the role out of e-health technology, which has currently stalled and got stuck in a hype cycle. Major problems have been identified in the areas of interoperability, governance and social-technological alignment [2].

With the arrival of new architectural concepts driven by the European Commission's Future Internet Private Public Partnership (FI-PPP) the attention has shifted towards what has become known as the Core Platform and the "Generic Enablers" (GE) which now in some respect forms the flipside of the coin [3]. The Generic Enablers need to be regarded as modules or building blocks, which can be utilized to generate

978-1-4673-5800-2/13/$26.00 ©2013 IEEE

instantiations, which generate a defined functionality. In the GE Universe functionality is primarily defined by the interaction of different GEs, whereby the interface specifications are clearly defined in a catalogue [4].
The future will show how these 2 fundamental technology flows will merge, coexist or kick-start completely new developments. However, if smart devices, sensors and mobile computers are to evolve further and are linked as part of modular medical architectures driven by GE technology a variety of norms and standards on a national, European and International level need to be considered by developers, healthcare providers and other user groups.

II. LEGAL NORMS AND FRAMEWORKS

Legal norms are found in various legal frameworks. E-health is regulated by medical law but also by many other legal domains. Specific legal requirements for specific applications will depend on the exact implementation and many contextual factors, such as which contractual relations apply (e.g., with a medical professional, a telemedicine service provider, and/or with a hospital). In this paper, we provide a generic overview of the major types of legal norms that apply, focusing on European law. It should be borne in mind that access to health care and health protection are grounded in human rights [5,6], which emphasizes the importance of legal protection in modular medical architectures.

A. Data Protection

A common element in use-case trials for modular medical architectures is that they collect and process personal data of persons, who in many cases are also patients. These trials should take into account the European rules on the protection of personal data, with special attention for the special requirements that relate to health and medical data [7].

The Data Protection Directive [8] lays down rules for the processing of personal data and recognizes specific rights of individuals on their personal data, while ensuring that such data can move freely within the internal EU market. When data can be linked directly or indirectly to an individual (the so-called data subject) they qualify as personal data. Only data that are truly anonymous are excluded from the rules [9].

The Directive contains general principles for processing personal data have to be respected, which balance the interests both of data controllers and of data subjects [10]. These principles include fairness and data quality (data should be correct and up-to-date), purpose specification and use limitation (data may only be processed for previously specified purposes), and legitimate ground (processing must be based on user consent, a contract, a legal obligation, or vital interest of the data subject). Consent will often be the legal basis for processing personal data in use-case trials and practices, but special attention must be paid to the processing of health and medical data: the processing of these is in principle prohibited, unless special grounds apply (see Article 8 of Directive 1995/46/EC) (cf. [11]).

Of special importance for medical architectures is the principle that the design of data-processing systems be aimed at processing either no personal data at all or as few as possible (data avoidance/data minimisation) [12]. The Data Protection Directive also addresses the issue of data security, imposing a statutory obligation on data controllers to ensure that personal data are processed in a secure environment, particulars of data security in e-health are beyond the scope of this paper and will be discussed elsewhere.

The Directive will be replaced with a Regulation, which harmonizes the law more strictly [13]. Although the draft General Data Protection Regulation will take several years before coming into effect, developers of modular architectures have to take into account the envisaged amendments and changes in order to make sure that the use-cases will comply with the future legislation as well. Of particular relevance are requirements to implement 'data protection by design and by default' and to execute Data Protection Impact Assessments for all operations that present specific risks.

Data protection law distinguishes between two principal actors (besides data subjects): the data controller and the data processor. This distinction is of great importance as the data controller (and not the data processor) is the party who carries the obligations described in the Data Protection Directive and also the party required to define the details of the data processing. Use-case trials raise significant challenges in identifying who are the responsible entities, in order to assign accountability obligations, since usually multiple actors are involved. Especially when several devices or GEs are combined in a use-case that transfers personal data of users in a way that leaves the control of the developer of the system, the identification of the responsible parties becomes difficult [14].

Moreover, the Directive contains rules for the transfer of personal data to third countries, an issue of great importance in all trans-border applications. Medical architectures may allow trans-border flows of personal data, which raise questions on the entities that have to take into account data protection from the design of the system and on who is responsible for the integrity and security of the data.

B. Patient's Rights (Other than Data Protection)

Medical law is largely shaped at the national level. However, EU law harmonizes some elements of patients' rights. First, the Directive 2001/20/EC regulates clinical trials, to protect human rights and the dignity of human beings with regard to biology and medicine. [15,16] It refers to Helsinki Declaration, illustrating the link between ethical principles for medical research involving human subjects and good practices in clinical trials on medicinal products for human use as regulated by the Directive. In 2012, a proposal was presented to replace the Clinical Trials Directive with a Regulation [17]. Modular medical architectures that require clinical trials for testing will have taken into account the Directive and the proposed Regulation.

Second, cross-border healthcare is regulated by Directive 2011/24/EU [18], which is particularly relevant for implementations of modular architectures that allow cross-border treatment, such as tele-monitoring or tele-care applications. It stipulates that in cross-border healthcare, the laws apply of the (foreign) country of treatment, while the (domestic) patient's country must reimburse costs according to

its insurance system and, if necessary, provide follow-up care. In telemedicine applications, the country of treatment is the country where the provider is established. Before or during cross-border healthcare, patients must have remote access to (or carry a copy of) their medical records, and afterwards, to ensure continuity of care, they are entitled to a written or electronic medical record of the treatment. National contact points must provide patients seeking cross-border healthcare with relevant information about providers, patient rights, complaint procedures, and legal remedies in the country of treatment. The Directive contains detailed rules on the reimbursement of costs, authorization systems, and administration procedures. In line with recommendations to integrate law with governance [19], the Directive also stimulates cooperation in healthcare through 'new governance' mechanisms, such as self-regulation and setting up various networks. An e-health network is to draft guidelines on data to be included in patient summaries that can be shared between health professionals across borders. This network should also help develop common identification measures to foster cross-border data transfers.

Third, depending on the application, other specific legislation may apply. For example, one of the FI-STAR use-cases involves 2D barcoding to offer real-time reverse supply chain modeling of pharmaceuticals. In this case, the European Commission guidelines on good distribution practice of medicinal products for human use must be taken into account. The guidelines aim at establishing adequate controls to ensure the quality and the integrity of medicinal products. The Guidelines have recently been revised and will enter into force in September 2013 [20].

C. Liability

Directive 2011/24/EU also provides that in cross-border healthcare, the country of treatment must ensure that systems of professional liability insurance are in place. For domestic healthcare, national liability regimes apply, which can differ significantly in relation to medical treatment; it has been recommended that rules on compensation for damages be harmonized in the EU [21]. In one respect, liability is already harmonized, namely in product liability. [22] Producers are held liable for damages caused by defective products that do not provide the safety that can be expected of the product [21]. This underlines the importance for implementations of medical architectures to comply with general standards and requirements.

For modular architectures, liability provides complex challenges because they involve multiple actors. There is a risk that lack of legal certainty concerning the liability distribution between medical professionals, e-health service providers, e-system developers, and patients hampers the development of e-health architectures. Legal systems should strive for a careful balance in stimulating trust in e-health systems, both protecting patients in liability claims and ensuring confidence in developers and practitioners that they will not be held liable for unforeseen effects. [23] Particularly in tele-monitoring applications, the responsibility of patients themselves to comply with the monitoring schemes should be factored in as well in liability distribution. [23]

D. Intellectual Property

Intellectual property rights protect the interests of creators by giving them property rights over their creations. This may raise barriers in the dissemination of e-health systems and applications, as usually high costs are involved in getting access to proprietary products and processes (compare [24]). Several intellectual property issues may arise when developing GEs, these will have to be tackled within the FI-PPP program, such as patent issues in telemedicine [25]. A major issue is the copyright protection granted to the developers of GEs, especially as regards the modification of the GE source code. Another key issue that will arise concerns the right to patent GEs, as they probably can be seen as new inventions that involve an inventive step and are capable of industrial application.

E. Internal Market Regulation

We have already listed some regulations aimed at the free movement of persons and services in the EU internal market. Many other regulations may also apply, depending on the type of application being developed.

Some implementations may constitute information society services, i.e., services normally provided for remuneration, at a distance, by electronic means at the individual request of a recipient. This can apply, e.g., to services allowing patients to electronically ask advice of physicians or to online medicine purchases. [21] The E-Commerce Directive imposes obligations on service providers to provide various kinds of information to users, including registration and applicable professional rules for regulated (including the medical) professions. Commercial communications should be allowed for providers in regulated professions, subject to professional rules such as professional secrecy. [26] Alternatively, implementations might constitute electronic communication services, if they provide a service for users with telecommunications functionality (without the provider exercising editorial control over conveyed signals). These services involve various obligations concerning universal access, user rights, and data protection. [27]

More likely, modular medical architectures may be qualified as medical devices, i.e., an instrument, apparatus, appliance, software, material or other article, intended to be used for diagnostic and / or therapeutic purposes, which does not function through pharmacological, immunological or metabolic means. General software, including Generic Enablers, used in e-health is not a medical device, but software manufactured or specifically adapted for medical purposes is a medical device. [21] The Medical Devices Directive imposes obligations on product safety, CE-conformity marks, and clinical evaluation [28]. Another area of internal market regulation is competition (or antitrust) law. Countries are autonomous in organizing public health care, and EU competition law does not apply if health systems are based on solidarity, but countries that introduce some market organization in their public health system will have to take competition rules into account. [29] This affects, for example, pricing schemes for pharmaceuticals, medical devices, and related services, and also has implications for procurement

procedures. It requires a very case-specific analysis to determine to what extent these rules apply. [30]

Similarly, the regulation of the free movement of people and services within the internal market might apply to (modular-based) medical architectures, in which (combinations of) the provider, the service, or the recipient can move between countries. We refer to [31] and [19] for discussions of these legal norms.

F. Global regulation

While the above provides a high-level overview of European law, developers of modular medical architectures may also need to consider whether non-European law applies, in case the architectures can be used or exported outside of the EU. The legal picture becomes much more complex and fragmented, as many different legal regimes will apply. Global regulation is beyond the scope of this paper (see [32] for a discussion). We do want to point out that e-health law and policy risks becoming entrenched in local, national visions that hamper the development of e-health applications that could benefit the global community, including developing countries. Development of modular medical architectures should therefore also be embraced as an opportunity by regulators to join forces and come up with supranational solutions to the regulatory challenges of e-health systems [33].

III. ETHICAL NORMS AND CONSIDERATIONS

For the majority of information and communication technologies moral issues are either technology or context dependent. Number and details of ethical issues of the different Information Communication Technologies (ICTs) vary depending on their level of progressiveness and public visibility. The Internet of Things changed radically the relationship between humans and the interconnected autonomous objects, giving those objects autonomy towards the interaction with human beings. The concept of autonomy for objects and humans has to be deeply analyzed, as well as security (dual use, freedom, liberty), equity, equality, justice, fairness, discrimination, and discriminatory interfaces [34].

In accordance with recent research on the subject ethical issues in emerging ICTs might be categorized [35, 36]. By far the most difficult concept in ICTs is privacy as at his moment there is no consistent definition of what privacy is [37, 38]. The privacy concept is not universal but is adapting to the necessities and constraints of society. The scope of the concept of privacy and its interpretation for emerging ICT must be seen against a background of technical and social developments [39]. Privacy is progressively challenged by intrusive ICTs. This clearly is not only affecting the relationships of computers and humans but also on social interaction and society [40]. In keeping with recent research results privacy should be understood as a fundamental right covering the need for safety of personal data, the right to data deletion and the right to control the use of portable data [37, 41]. Individuals need to be able to consent and withdraw the consent at any given time. Currently changes in the perception of privacy are mostly understood in terms of decrease in the importance of privacy value or a gap between privacy as a value and a displayed self-revealing behavior. According to recent findings by the PRACTIS project (FP7) three kinds of potential impacts of emerging ICTs on privacy are: threats to privacy, privacy enhancement and changes to the individual perception of privacy. It only seems reasonable to consider these ethical issues early in the technological development stage. However, doing so, we will find ourselves confronted with Collingrindge's dilemma implying that ethical issues cannot be addressed in very early stages of technology design as technological and social consequences can typically only be fully understood once the development process is far advanced [42]. The benefit of privacy impact assessment has been described elsewhere and privacy impact assessment should be considered good practice [43,44,45].

IV. TECHNICAL STANDARDS

A. Background, Motivation, and Approach

In the healthcare industry standards and regulations are frequently perceived as limitations or hurdles, which need to be overcome in order to establish trust in new technologies. Some of these regulations are global, while others are applicable just for some types of systems and regions. Although especially with regards to health and safety reasons the necessity of standards and regulation is undisputed, regulations on the other hand make product development risky and costly, hence discourages software and electronic companies to contribute to value creation and innovation.

Software ecosystems, such as the "Core Platform" and its modular design consisting of a variety of GEs provide an opportunity to reduce this hurdle for software product companies. Interfaces, data models, and protocols can be integrated into enabling components ready for use by application developers. Application stores are able to embed rules for assuring compliance and provide certification mechanisms. Such hiding of regulatory rules and procedures allows software companies to focus on value creation for the customer and on differentiation towards competitors, while benefiting from central services to learn how to address regulation and to check application compliance.

The first step in the design of such support is a mapping of relevant standards and regulations. The map enables identification of responsibilities, services, and rules that are to be delivered by the software ecosystem. Such support will reduce cost and risk of new software development and offer more consistent level of compliance across software products.

This section gives an overview of standards that are applicable for the healthcare, wellness and ambient assisted living sectors and outlines the implications of these standards on ecosystem design. Enabling such transparency regarding which standards are applicable allows generating a debate on the scope of regulations to be considered, creates the fundament for implementation of the ecosystem, and provides a baseline for road-mapping how standardization should evolve.

To identify the here presented standards, we have selected two different solutions conceived by healthcare providers and have elicited their needs for compliance. Furthermore relevant

standards have been identified in the literature. Included were are the standards of relevance for software products to be used in health care, wellness and ambient assisted living environments comprising of software products, professional users such as nurses and doctors, and the general public such as patients and caregivers. Overall, the presented standards apply to infrastructures, which are generally referred to as "medical data networks". Excluded were standards that relate to the design and construction of physical equipment only. Also excluded were national regulations and standards under development.

B. Overview of Standards

Analysis of standards showed four groups of standardized aspects: development of a software product, interoperability of the product with other products, usage of the product by a human user, and resilience to protect from harm. These four groups of regulated aspects assure good-enough quality for the software to be used in a mission-critical care environment. The remainder of the section gives an overview of the four regulated aspects of a software product intended for care.

The standards focused on are typically regulating one aspect at a time. However, in practice the boundaries are blurred. For example, the technical aspects of interoperability affect the human aspects of perceived usability [46]. Also, as indicated in ISO/TR 16982, usability affects not only the design, but also the process used to develop the software product and trust in the released software product.

Software Development. IEC 62304 regulates the development of software for medical devices. It adds the aspects of risk and quality management to the established good practices suggested by frameworks like CMMI and ITIL and development lifecycle models such as waterfall and agile. It constrains development, maintenance, risk management, configuration management, and problem resolution practices based on an assessment of safety criticality of the software. IEC 62304 compliance contributes to FDA [47] compliance.

ISO 13407 specifies the processes of designing interactive systems from a usability perspective, and ISO/TR 16982 specifies the use of usability engineering methods as part of such development processes. IEC 62366 defines the corresponding process to be followed for engineering medical devices.

Further guidance for software development can be obtained by other IEEE and ISO/IEC standards, which are applicable for software engineering in general and not for healthcare, wellness, and ambient assisted living in particular. Standards of relevance are the IEEE Standard Glossary of Software Engineering Terminology 610.12 and ISO/IEC 25010 for Systems and Software Quality Requirements and Evaluation.

Interoperability. A software product embedded in a solution has to communicate with other software products and medical devices. To enable independence from the manufacturer of these products, ISO/IEEE 11073 specifies how the products interact. It is a family of standards that defines the application domain, terms, information model, types of devices, applications, data transport, and data encoding. ETSI ES 202 975, even-though not specific for the health domain, further constrains communication of text, speech, and video in a network.

Information that is of particular relevance in the care sector is the patient profile. CEN/TC 251 has developed a collection of standards on health informatics for health interoperability. CEN/ISO 13606 is of particular importance as it specifies electronic health record communication. It captures a reference model that allows the formulation and aggregation of statements of relevance for the health record, an archetype model that defines health concepts and their meaning, and allows defining data protection rules that govern the access to the data the health record contains. ISO/TS 19218 specifies coding practices for describing adverse events relating to medical devices. ISO 15225 defines a medical device nomenclature data structure for exchange of data used by regulatory bodies.

Usability. Much work was invested in standardizing the interaction between humans and software-based systems with the goal of simplifying the interaction between users and software and of enabling effective support of these users. The multi-part standard ISO 9241 defines the design of input and output devices that allow users to interact with software-based systems, the interaction process, and the physical context such as the workplace in which users interact with the systems.

Software user interfaces are used to present a wide variety of functionality and information to users. The multi-part standard ISO 14915 establishes design principles for the interaction of professional users with text, graphics, audio, animations, video, and media related to other sensory modalities. IEC TR 61997 defines guidelines for multimedia interfaces that are used by the general public without any special previous training. ISO 15223 defines symbols and the development of such symbols to be used to convey information on the safe and effective use of medical devices.

Safety, Resilience and Trust. A new software product may not only produce new value, but also destroy or endanger existing value. The new product may harm people or existing processes or generate fear of such harm. ISO/TR 16142 provides guidance on the selection of safety and performance-related standards for medical devices that allow establishing trust that the new product will not produce harm.

IEC 80001 specifies the perspective of the care provider by defining how to manage safety, effectiveness, and security of an integrated healthcare system. It defines roles and responsibilities, and risk management policies and processes for medical IT networks and for enhancement and change of these networks. The ISO 27000 family of standards establishes vocabulary, requirements, and processes for managing security and security-related risks of such integrated systems.

The product supplier perspective is covered by ISO 14971 that IEC 80001 now integrates. ISO 14971 specifies the risk management practices to be followed by a medical device manufacturer. ISO 13485 defines regulatory requirements for medical devices, including documentation, management, product realization, and quality assurance processes. IEC

60601 standardizes safety practices for medical electrical equipment.

C. Impact of the Standards

The presented standards are embodied in many national regulations, are common practice of experienced software product suppliers, and are part of awarding the CE label for products intended for the care sector. This is also important for compliance with the Medical Devices Directive [28]. To help new software products to reduce cost and risk associated with compliance, the provided overview of standards represents a starting point to identify roles, responsibilities, and services in a compliance-enabling software ecosystem.

V. Discussion

This article gives an overview of relevant norms and standards for the development and instantiation of technologies in the health care, wellness and ambient assisted living domains and the implementation of medical data networks. Special consideration has been given to governance requirements expressed through legal and technical norms and standards on the interface of the "Core Platform" which is also known as the Generic Enabler concept and the "Internet of Things". Technical standards have been named and highlighted in this paper. Citations of text elements of technical standards or the cross reference to "full texts" are generally not possible as definitions of the standards are typically not in the public domain and copyright protected. Full versions of these standards may be purchased for further reading.

Legal norms and ethical considerations have been discussed with focus on the relevance to the healthcare, wellness and ambient assisted living domains. Due to the magnitude of the subject it was not possible to cover national legislation for the different European member states. US standards such as those published by HIPAA (Health Insurance Portability and Accountability Act of 1996) and overseen by the US Department of Health and Human Services and rules and regulations established and overseen by the FDA (Food and Drug Administration) have not been considered in the context of this paper. It should be mentioned that in recent years the medical product regulations in many countries have been extended and do now cover software products, as well as hardware, which has not always and everywhere been the case. This means that typically software has to comply in full with national medical product legislation.

There is good evidence that future "medical" architectures will be modular and follow European wide defined specifications. Health care providers have rejected public e-health cloud approaches in Europe and elsewhere and single standing solutions are unlikely to continue due to regulations and cost aspects. There has been good progress fueled by EC funded research with regards to the cross border transfer of medical data sets within Europe [48]. Our future work under FI-STAR will include a mapping of the standards discussed in this paper onto Generic Enablers and Usage Specific Enablers. As part of our progressive work we will also map those standards, which so far could not be considered, such as the US standards and legislation in different European national states. Another important part of our work will be to look into commercial distribution strategies and business models in order to establish application distribution platforms (app-stores).

The technical targets of FI-STAR will be the validation of domain relevant Generic Enablers and Usage Specific Enablers in the healthcare, wellness and ambient assisted living domain.

VI. Conclusions

Legal norms, ethical opinions and technological standards have to be considered when planning, designing and implementing medical modular architectures based on IoT elements and Generic Enablers. In principle these norms and standards do not distinguish between hardware and software technologies or IoT and the Core Platform. In most countries software products now have to comply fully with the national medical product legislation, which has not always been the case. Although regulations are complex and diverse and might be perceived as hurdle or obstacle on the way to the development of new technologies staff and patient's rights have to be considered and health and safety must have first priority. A detailed requirements analysis is inevitable in order to assure full compliance with regulations of new technologies and to avoid unexpected costs for adjustments and adaptation at a late stage in the development process.

VII. Acknowledgment

The authors are members of the Future Internet – Social Technological Alignment Research (FI-STAR) project, which is part of the Future Internet Private Public Partnership (FI-PPP) run by the European Commission. FI-STAR is a FI-PPP phase 2 project, which commenced on 1.April 2013 and will conduct at least seven early clinical and non-clinical digital-health use-case trials in seven or more European countries. FI-STAR is partly funded by the European Commission [49]. This paper is based on a requirements' analysis conducted as part of FI-STAR.

References

[1] Christoph Thuemmler, Julius Mueller, Stefan Covaci, Thomas Magedanz, Stefano de Panfilis, Thomas Jell and Anastasius Gavras, Applying the Software-to-Data Paradigm in Next Generation E-Health Hybrid Clouds, ITNG2013, Proceedings of the 10th International Conference on Information Technology, IEEE Computer Society, ISBN 978-0-7695-4967-5

[2] European Commission, "Communication from the European Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – e-health action plan 2012-2020 – Innovative healthcare for the 21st Century", 2012

[3] http://www.fi-ppp.eu

[4] http://catalogue.fi-ware.eu

[5] J. Legemaate, "Integrating health law and health policy: a European perspective", Health Policy, vol. 60, 2002, pp. 101–110.

[6] J. McHale, "Fundamental rights and health care," in Health Systems Governance in Europe, E. Mossialos, G. Permanand, R. Baeten and T. Hervey, Eds. Cambridge etc.: Cambridge UP, 2010, pp. 281-314.

[7] J. Dumortier and C. Goemans, "Privacy protection and identity management", in Security and Privacy in Advanced Networking Technologies, B. Blažic and W. Schneider, Eds. IOS Press, 2004, p. 193.

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

[9] C. Kuner, European Data Protection Law – Corporate Compliance and Regulation, Oxford: Oxford University Press, 2008, p. 51.

[10] I. Walden, "Data Protection", in Computer Law, C. Reed and J. Angel, Eds., 5th edition. Oxford: Oxford University Press, 2003, p. 432.

[11] Luca Compagna, Paul El Khoury, Alžbeta Krausová, Fabio Massacci, Nicola Zannone, "How to integrate legal requirements into a requirements engineering methodology for the development of security and privacy patterns", Artif. Intell. Law, vol. 17, pp. 1–30, 2009.

[12] B. Holznagel and M. Sonntag, "A Case Study: The JANUS Project", in Digital Anonymity and the Law – Tensions and Dimensions, C. Nicoll et al, Eds. The Hague: TMC Asser Press, 2003.

[13] Proposal for a General Data Protection Regulation, COM(2012) 11 final, 25.01.2012.

[14] H. Löhr, A.-R. Sadeghi, and M. Winandy, "Securing the e-health cloud," in Proceedings of the 1st ACM International Health Informatics Symposium, ser. IHI '10, 2010, p. 223.

[15] 2001/20/EC (Clinical Trials Directive), Official Journal 2001, L121/34.

[16] F. Lemaire and an ESICM Task Force, "A European Directive for clinical research", Journal of Intensive Care Medicine, vol. 29, pp. 1818 ff, 2003.

[17] Proposal for a Regulation on clinical trials on medicinal products for human use, and repealing Directive 2001/20/EC, COM(2012) 369 final, 17.7.2012.

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

[19] T. Hervey and G. Trubek, "Freedom to Provide Health Care Services within the EU: An Opportunity for a Transformative Directive", Columbia Journal of European Law, vol. 13, pp. 624ff, 2007.

[20] Guidelines of 7 March 2013 on Good Distribution Practice of Medicinal Products for Human Use, Official Journal 2013, C68/1, 08.03.2013.

[21] S. Callens, "The EU legal framework on e-health", in Health Systems Governance in Europe, E. Mossialos, G. Permanand, R. Baeten and T. Hervey, Eds. Cambridge etc.: Cambridge UP, 2010, pp. 561-588.

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

[23] A.H. Vedder and P. Vantsiouri, "Building trust in E-Health Services", unpublished.

[24] B. Blobel, P. Pharow and M. Nerlich, e-health: combining health telematics, telemedicine, biomedical engineering and bioinformatics to the edge (Global Experts Summit book), IOS Press, 2008.

[25] Yasumitsu Tomioka, Isao Nakajima, Hiroshi Juzoji, Toshihiko Kitano, "Patent Issues in e-health, Especially of North and South Problems on Telemedicine", Proceedings of IEEE Helathcom 2009, Sydney, Australia,16 – 18 December 2009, pp. 181ff.

[26] Directive 2000/31/EC (Directive on electronic commerce), Official Journal 2000, L178/1.

[27] Directive 2009/136, amending Directives 2002/22/EC and 2002/58/EC, Official Journal 2009, L108/41.

[28] Directive 2007/47/EC, amending Directives 90/385/EEC, 93/42/EEC and 98/8/EC, Official Journal 2007, L247/21.

[29] T. Prosser, "EU competition law and public services", in Health Systems Governance in Europe, E. Mossialos, G. Permanand, R. Baeten and T. Hervey, Eds. Cambridge etc.: Cambridge UP, 2010, pp. 315-336.

[30] J. Lear, E. Mossialos and B. Karl, "EU competition law and health policy", in Health Systems Governance in Europe, E. Mossialos, G. Permanand, R. Baeten and T. Hervey, Eds. Cambridge etc.: Cambridge UP, 2010, pp. 337-378.

[31] E. Mossialos, G. Permanand, R. Baeten and T. Hervey, Eds., Health Systems Governance in Europe, Cambridge etc.: Cambridge UP, 2010, Chapters 10-12.

[32] J.D. Blum, "The role of law in global e-health: a tool for development and equity in a digitally divided world", St. Louis U.L.J., vol. 46, pp. 85-110, 2002.

[33] M. Mars and R.E. Scott, "Global E-Health Policy: A Work in Progress", Health Affairs, vol. 29, pp. 239-245, 2010.

[34] EGE, opinion 26, 2012 .Ethics of Information and Communication Technologies available at: http://ec.europa.eu/bepa/european-group-ethics/docs/publications/ict_final_22_february-adopted.pdf

[35] Stahl B.C. IT for a better ethics. How to integrate ethics,politics and innovation. in Rene von Schomberg (ed.). Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. Luxembourg Publications Office of the European Union, 2011.

[36] Deliverable 2.2 Normative issues Report. Available from FP7 ETICA project: www.etica-project.eu

[37] Cf.Flash Eurobarometer 241 on"Information Society as seen by the EU citizens (2008) as Special Eurobarometer 359" Attitudes on Data Protection and Electronic Identity in the European Union (2011).

[38] Guagnin D.,Hempel L., Ilten C. Privacy, practices and the claim for accountability in Rene von Schomberg (ed.). Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. Luxembourg Publications Office of the European Union, 2011

[39] Kleve, Pieter, and Richard de Mulder. 2008. "Privacy protection and the right to information. In search of a new balance." Computer Law & Security Report 24 (3):223–32.

[40] Hautaptman A.,Sharon Y,Soffer T. Privacy Perception in the ICT era and beyond in Rene von Schomberg (ed.). Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. Luxembourg Publications Office of the European Union, 2011

[41] Peissl W. Responsible research and innovation in ICT.The case of privacy in Rene von Schomberg (ed.). Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. Luxembourg Publications Office of the European Union, 2011.

[42] Collingridge D (1981).The Social Control of Technology. Paligrave Macmillan

[43] Warren,Adam,Robin Bayley,Colin Bennett ,Andrew Charlesworth, Roger Clarke and Charles Oppenhamn.Privacy impact assessment-International experience as a basis for UK Guidance,Computer Law and Security Report,vol 24,20908,pg 233-242.

[44] Cavoukian, A., 2009, Privacy by Design ....take the challenge, Toronto: Information and Privacy Commisioner of Ontario, Canada <http://www.privacybydesign.ca/pbdbook/ PrivacybyDesignBook.pdf>.

[45] Wright D.,Gellert R., Gutwirth S.,Friedewald M. Precaution and privacy impact assessment as modes towards risk governance in Rene von Schomberg (ed.). Towards Responsible Research and Innovation in the Information and Communication Technologies and Security Technologies Fields. Luxembourg Publications Office of the European Union, 2011

[46] M. Ullah, M. Fiedler, and K. Wac., On the ambiguity of Quality of Service and Quality of Experience requirements for e-health services. 2012 6th International Symposium on Medical Information and Communication Technology (ISMICT), La Jolla, CA, March 2012, pp

[47] http://www.fda.gov/

[48] http://www.epsos.eu

[49] https://www.fi-star.eu/home.html