Samuel A. Fricker · Christoph Thümmler
Anastasius Gavras *Editors*

Requirements Engineering for Digital Health

Springer

Requirements Engineering for Digital Health

Samuel A. Fricker • Christoph Thümmler
Anastasius Gavras
Editors

Requirements Engineering for Digital Health

Springer

Editors
Samuel A. Fricker
Blekinge Institute of Technology
Karlskrona, Sweden

Anastasius Gavras
Eurescom GmbH
Heidelberg, Germany

Christoph Thümmler
Edinburgh Napier University
Edinburgh, UK

Institute for Minimal Invasive
Medical Innovation
Technical University Munich
Munich, Germany

ISBN 978-3-319-09797-8 ISBN 978-3-319-09798-5 (eBook)
DOI 10.1007/978-3-319-09798-5
Springer Cham Heidelberg New York Dordrecht London

Library of Congress Control Number: 2014952896

While the advice and information in this book are believed to be true and accurate at the date of publication, neither the authors nor the editors nor the publisher can accept any legal responsibility for any errors or omissions that may be made. The publisher makes no warranty, express or implied, with respect to the material contained herein.

Printed on acid-free paper

Springer is part of Springer Science+Business Media (www.springer.com)

Contents

Contributors

David Benyon Centre for Interaction Design, Institute for Informatics and Digital Innovation, Edinburgh Napier University, Edinburgh, UK

Karima Bourquard IN-SYSTEM, Paris, France

Gerd Stefan Brost Fraunhofer AISEC, Munich, Germany

Philippe Cousin Easy Global Market, Nice, France

Niklas Falk-Andersson Norwegian Centre for Integrated Care and Telemedicine, Tromsø, Norway

Samuel A. Fricker Software Engineering Research Laboratory, Blekinge Institute of Technology, Karlskrona, Sweden

Rainer Grau Zühlke Engineering AG, Schlieren, Switzerland

Mario Hoffmann Fraunhofer AISEC, Munich, Germany

Ioana Ispas Ministry of National Education, Bucharest, Romania

Ai Keow Lim Jumelle Institute for Informatics and Digital Innovation, Edinburgh Napier University, Edinburgh, UK

Bert-Jaap Koops TILT—Tilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands

Eleni Kosta TILT—Tilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands

Franck Le Gall Easy Global Market, Nice, France

Mats Löfdahl Blekinge Institute of Technology, Karlskrona, Sweden

Oli Mival Centre for Interaction Design, Institute for Informatics and Digital Innovation, Edinburgh Napier University, Edinburgh, UK

Nadezhda Purtova TILT—Tilburg Institute for Law, Technology, and Society, Tilburg University, Tilburg, The Netherlands

Jakob Rasmussen Living Labs Global, Copenhagen, Denmark

Urban Sedlar Laboratory for Telecommunications, University of Ljubljana, Ljubljana, Slovenia

Christoph Thümmler Edinburgh Napier University, Edinburgh, UK

Institute for Minimal Invasive Medical Innovation, Technical University Munich, Munich, Germany

Mojca Volk Laboratory for Telecommunications, University of Ljubljana, Ljubljana, Slovenia

Adrian Zwingli SwissQ Consulting AG, Zürich, Switzerland

Chapter 1
Digital Health

Christoph Thümmler

Abstract Healthcare is the biggest and fastest growing industry in the world and is one of the domains that are expected to grow significantly over decades to come. Underlying cause for this are the current demographic developments which are showing similar patterns almost worldwide with a strong growth of the population share of individuals over 65 years of age.

1.1 The Book

Healthcare is the biggest and fastest growing industry in the world and is one of the domains that are expected to grow significantly over decades to come. Underlying cause for this are the current demographic developments which are showing similar patterns almost worldwide with a strong growth of the population share of individuals over 65 years of age.

In the near future we will witness the emergence not only of groundbreaking new technologies in health and care but the emergence of completely new care systems with the need for large-scale integration of different types of technologies such as 4G and 5G, m-health applications, e-health clouds, and others. In this context requirements engineering will evolve from an expert domain initially left to a relatively small number of insiders to a critical skill set which in certain settings might well be applied by trained non-experts or informed users.

Although there can be no doubt that regional healthcare providers instantiating and implementing a new technology will in most cases seek expert advise to keep costs under control, small surgeries or pharmacies might rely on an informed decision by their owners who would probably be reluctant to invest a five-digit sum in a technology consultant. After all, following the 20–80 % rule (80 % effect out of 20 % effort) might be the only realistic and feasible approach for micro-, small-, and

C. Thümmler (✉)
Edinburgh Napier University, Edinburgh, UK

Institute for Minimal Invasive Medical Innovation,
Technical University Munich, Munich, Germany
e-mail: c.thuemmler@napier.ac.uk

S.A. Fricker et al. (eds.), *Requirements Engineering for Digital Health*,
DOI 10.1007/978-3-319-09798-5_1

medium-sized enterprises (SME). But also smaller departments and managers working with in-house consultants might be interested in exploring the basics of requirements engineering in healthcare in order to map the terrain and enable them to clearly identify those areas that might be suitable for self-management and separate them from those tasks which would require professional input.

However, expert knowledge with regard to requirements engineering in the medical domain is limited and scattered across the literature and the identification and access of suitable and relevant content is time consuming and increasingly expensive.

This book intends to give an urgently needed and guided interdisciplinary overview over key aspects of requirements engineering in health and care to non-experts, students, and those requirements engineers unfamiliar with the healthcare, wellness, and ambient-assisted living domains. The book aims in particular at providing the readers with expert know-how from the shop floors rather than plane theoretical textbook knowledge. This book is not intended to replace a comprehensive textbook on requirements engineering but should complement academic literature wherever healthcare domain-specific knowledge is required or wherever the reader might be faced with real-world challenges in the healthcare, wellness, and ambient-assisted living domain.

This chapter maps the terrain and provides an overview of digital health, its roots and origins, the evolution, the socioeconomic context, and the future outlook (*Christoph Thümmler*). In the *requirements engineering chapter* (Chap. 2) we will provide view from experienced experts on the application of methods and tools and on best practice (*Samuel Fricker*). Due to the regulative implications healthcare is fundamentally different from many other industrial domains and careful considerations of legal and ethical aspects are mandatory for successful instantiation and implementation of new technology and subsequently of utmost importance for requirements engineering processes. We will discuss these in a chapter on *laws and regulations for digital health* (*Eleni Kosta*) (Chap. 3) and a chapter on *ethics for digital health* (*Ai Keow Lim Jumelle*, *Ioana Ispas*) (Chap. 4). Due to progressive globalization and in particular to secure interoperability and compatibility standardization is becoming more and more important in order to prevent fragmentation and island solutions. Details will be discussed in the *standards for digital health* (*Karima Bourquard*) chapter (Chap. 5). Most processes these days are expected to be user driven in order to optimize uptake and ensure sustainability. This is a principle close to the heart of requirements engineering and is reflected by the chapter on *user experience for medical personal and patients* (*Oli Mival*, *David Benyon*) (Chap. 6). Safety, security, and privacy are key requirements in the health and care domain and always have high priorities in any instantiation and implementation of new technology. Although the underlying security technology is an expert domain in its own right we will discuss the basics in the *patient safety and privacy, software security, and business resilience* chapter (*Mario Hoffmann*) (Chap. 7). Technological aspects take center stage in the practical settings and details of a pragmatic approach are outlined in a chapter describing how to elicit, analyze, and check requirements for a digital health solution (*Mojca Volk*) (Chap. 8). Finally, the book takes a more abstract holistic approach on *how to plan and define a digital health product* (*Jakob Rasmussen*) to provide some guidance not only to medical professionals, patients, and clinical managers, but also to entrepreneurs and decision makers in the financial and administrative domains (Chap. 9).

1.2 Who Should Read This Book

The book provides a high-level overview about the current healthcare, wellness, and ambient-assisted living landscape and discusses the specific challenges and requirements of applying requirements engineering in this particular domain. While it is certainly an advantage if readers have a background in requirements engineering it is by no means a prerequisite. It has been the intention of the authors to create an access point for the highly diverse group of professionals typically involved in the implementation and instantiation of new technologies and the assessment of the associated requirements.

The book addresses medical practitioners, managers, engineers with little or no experience in requirements engineering, and requirements engineers with no experience in the healthcare domain.

This editorial also provides a high-level overview for decision makers in order to develop a better understanding of the processes involved in requirements engineering in the health and care domains in order to estimate implementation efforts and time lines. The book also addresses students and educators in requirements engineering, medicine, nursing, and digital health.

For researchers and academics the book will deliver background information to understand the background and the complexities of digital health and provides the required high-level knowledge for successful research funding applications. The book also provides an introduction for managers and professionals dealing with implementation and innovation processes in health and care as part of their general duties without necessarily holding an engineering degree.

The different chapters are based on the experience of practitioners in the relevant areas and provide clear practical guidance on real-world problem solving in the healthcare, wellness, and ambient-assisted living domain.

1.3 Historical Developments

Since the introduction of the Elizabethan Laws in England in the sixteenth century, which would only allow licensed recognized physicians to practice medicine in a radius of seven miles around London, the delivery of care has come a long way. Medicine has been subject to rapid progressive changes fuelled and driven by societal developments such as the industrial revolution and Bismarck's welfare legislation and historic landmark events such as the Crimean Wars, which led to the birth of the Red Cross and World War II, which ultimately led to the industrial style production of pharmaceuticals, such as penicillin. World War II also triggered the upcoming of healthcare systems as national institutions due to the high demand for care following wartime injuries and the limited financial resources of citizens almost everywhere in Europe. The British National Health Service (NHS) was never meant to be a long-term solution but was put in place as a free state-funded interims solution in 1948 to meet the needs of thousands of injured ex service men and women. The ambitious vision of free healthcare provision at the point of care ended already 4 years later in 1952 with the introduction of a prescription fee of one Shilling and a fee of one Pound Sterling for dental treatment.

In modern times the development of healthcare has been mainly driven by the microbiological revolution, the progress in nanotechnology, and the emergence of information communication technology. The upcoming of new manufacturing technologies especially in the polymer industry enabled the production of lighter and thinner materials, which boosted the surgical revolution of the 1960s. The baby boomers created a demand for mass production of pharmaceuticals in the 1970s. New microbiological manufacturing technologies enabled the synthesis of insulin and a whole range of substances in the 1980s. Genetics laid the foundation for individualized medicine and groundbreaking changes in the pharmaceutical sectors are lying ahead of us.

However, not only technological progress has shaped the evolution of healthcare. One of the main drivers has clearly been the transition from industrial and agricultural societies to service societies. Due to the postwar changes in our lifestyles the case mix in accident and emergency departments has completely changed. Acute surgical interventions have been in dramatic decline over the last 50 years or so. Through instant access to care, the recognition of the value of hygiene and the ubiquitous availability of antibiotics acute infections are either prevented or immediately recognized and treated. The problems associated with the rash and lavish prescription of antibiotics cannot be highlighted enough but is not of central relevance to the subjects addressed in this chapter.

Starting off in the 1960s there has been a major change in the healthcare paradigm shifting the focus from treatment to prevention. These days there is a clear focus on diagnostics with an ever-growing demand for digital imaging procedures, minimal invasive procedures, histopathology, and laboratory medicine. There are indications that this trend will continue to a point where profiling of the human genome as a standard procedure may soon reveal illnesses before they manifest themselves and show in the patient. This may even lead to "treatment without illness" and prophylactic procedures. However, there can be no doubt that acute medical and surgical interventions will be the exception rather than the rule and that the focus with regard to healthcare will be on monitoring, prevention, and (self-) management.

Worldwide the omnipotence of the Internet and the rapid progressive deployment of digital infrastructure are driving a process of virtualization and aggregation. This allows for the availability and accessibility of rocketing numbers of new healthcare, wellness, and ambient-assisted living services. The latest trend hereby is the emergence of applications, which may be used on smartphones and other mobile devices such as tablets and notebooks. The market volume for m-health applications has been predicted by the European Commission at 17.6 billion Euro by 2017. Currently there are around 100,000 applications available globally [1]. Although this trend is in principle not unwanted and in a way leveraged by policy makers and governments it is not without problems for all parties involved. The application of m-health technologies requires certainly a review of the relevant liability legislation as neither doctors, nurses, nor healthcare providers can be held liable for applications which are purchased by patients online. There are also concerns regarding privacy and security as applications might collect information without the knowledge of the users and make them accessible to third parties without permission. Finally, mobile health applications might not be safe or not suitable altogether and there are currently still major issues with regard to standardization and certification of these technologies.

From an economic perspective healthcare is clearly the largest and fastest growing industry worldwide fuelled by demographic changes in our societies and lately another wave of groundbreaking new information communication technologies. There can be no doubt that the uncoordinated implementation of these technologies would put a devastating burden on social security systems. Successful developers and manufacturers will have to work much closer with the users in the future to demonstrate value for money and alignment with local and national health policies.

On the other hand the margins of the industries have grown progressively tighter and return of investment needs to be seen within months or years rather than in decades. Due to the links of the healthcare domain to the public sector and governments there is a growing need for strategies to estimate and facilitate social technological alignment for the benefit of all parties involved and for the sake of future prosperity. Requirements engineering has become more and more popular in recent years and has proven its usefulness. There can be no doubt that requirements engineering will play a pivotal role in the introduction to new technologies into health and care.

1.4 Socioeconomic Aspects of Health and Care

Healthcare is the largest and fastest growing industry globally. In 2013 for European countries the average GDP share spent on health has been around 10 %, and for the USA around 17 % with a widening gap between the growth of GDP and the rise in national healthcare expenditure [2, 3]. The average GDP share spent on health by the People's Republic of China has been 5.4 % in 2013 [4].

Although the current growth of healthcare expenditure has calmed down a bit primarily caused by the lapse of many pharmaceutical patents and the subsequent replacement by generic drugs, the beneficial effect has been absorbed by weak GDP growth data. The relationship between the overall GDP growth rate and the growth

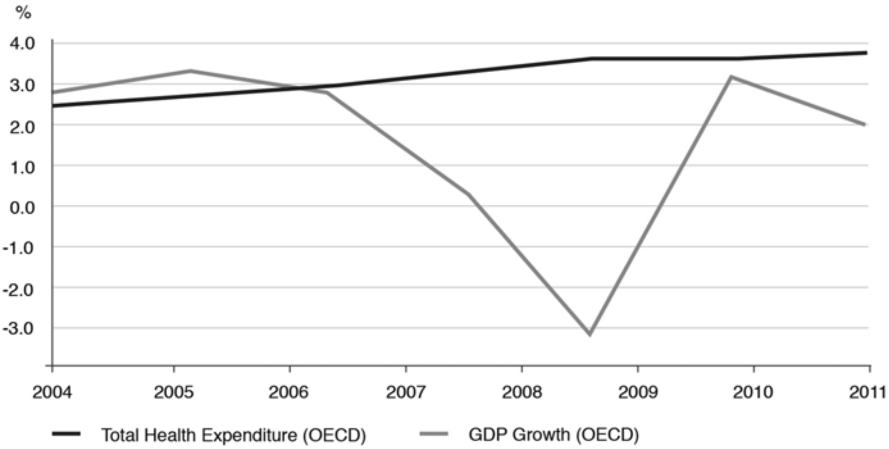


Fig. 1.1 GDP vs. health expenditure in OECD countries

rate of the health GDP share in OECD countries is depicted in Fig. 1.1. Health expenditure in China is expected to grow from 357 billion USD in 2011 to 1 trillion USD in 2020 [5].

These developments must not be regarded as liner processes as the current demographic developments in all industrial nations suggest seismic changes, which will continue to drive healthcare costs globally at least until the end of the twenty-first century [6]. On the other hand there can be no mistaken that technological progress in all areas relevant to medicine will offer new solutions to improve health and well-being and extend the individual life-span. This will boost the demand for health and care even further. Overall spending on medicines grew in the USA to an overall of 320 billion USD in 2011 of which patients with insurance paid 49 billion USD out of pocket. The availability of new generic drugs in a number of chronic therapies contributed to lower patient out-of-pocket spending, and a minimal real per capita increase in total spending on medicines [7]. Inevitably, this will change with the upcoming of new products. At this point in time a stagnation of spending on healthcare can be observed in all OECD countries, although there are a lot of indicators suggesting that this trend is not sustainable, especially with regard to the current demographic developments and the extended average life-span [8] (Fig. 1.2). The current dip in health care spending needs to be understood more as a delay in spending due to general austerity rather than a reverse of the overall trend.

It is safe to say that through the digitalization of our societies, the Internet and the (digital) media, the individual awareness levels for health and disease are at an all-time high. People expect healthcare providers to deliver top quality and on top of this individuals are prepared to pay additional money for their well-being.

A groundbreaking health economic development seems to be the willingness of health insurers to pay for therapeutic software applications. BEK, one of Germany's

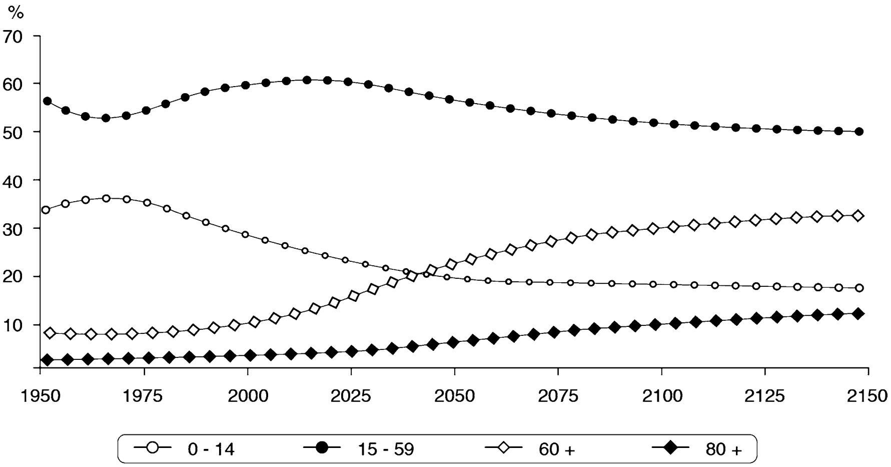


Fig. 1.2 Percentage of world population by age group, medium scenario, 1950–2150

largest statutory health insurance companies, has recently agreed to reimburse the costs of applying software for the treatment of amblyopia in children, if prescribed by a specialist [1]. The relative share of the costs of treatment of amblyopia in children compared to overall healthcare spending is small but the meaning of the first-time approval of reimbursement of costs for therapeutic applications in Europe must not be underestimated. However, on the other hand recent changes in medical product legislation in most countries now require software products to be rigorously assessed and their benefits clearly proven before applications can be sold and their reimbursement can be approved by health insurers.

Although early days, the fast-growing domain of m-health has recently been mapped out by the European Commission in an Infographic: by 2017 3.4 billion people will own one or more smartphones and by then the global m-health market is estimated to be worth 17.6 billion Euro [3]. Although this is still a very moderate amount compared to overall healthcare costs the potential is huge and spending in real terms is likely to grow significantly over the coming decade.

Overall there is a growing evidence base for a development towards Internet-based self-management and personalized care in order to reduce independence, increase mobility, and improve flexibility among patients, informal carers, and medical professionals. In particular in European countries, which historically have been running socialized healthcare schemes over most of the twentieth century (contrary to the US private care-dominated system), there is also hope that an increased pickup rate of e-health and m-health technologies might optimize the utilization of healthcare and mobilize efficiency reserves which will defuse the growing tensions around the continuously rising burden to society as a result of rising costs of national healthcare systems.

Modern digital infrastructures do have the capability to enable a variety of highly sophisticated services such as financial services (online banking, cash machines), legal/governmental services (payments to the government, consumption of services such as passport applications, etc.), and even election services (enrollment into electoral registers and online voting). There can be no doubt that these technologies hold the potential to increase the effectiveness and efficiency in the healthcare domain by enabling the virtualization of care and facilitate the integration of formal, informal, and social care. According to Buckner and Yeandle the value of informal care in the UK in 2006 has been roughly 87 billion GBP—almost the same amount as the UK National Health System budget as a whole for the same period of time [6].

The use of the Internet and progressive ICT solutions for virtualization of care and the creation of individual, patient-centric health ecosystems consisting of real world and virtual elements is a declared target of politicians globally. Virtualization of care is currently pushed forwards especially in remote and rural regions of the world. This is supported by a strong growth of mobile telephone networks and the provision of improved bandwidth and communication protocols such as 3G, 4G, and soon 5G. According to Huawei 5G is expected to provide 1,000-fold gains in capacity with download speeds up to 10 Gb/s supporting at least 100 billion devices by 2030 [9]. High-speed connectivity and new software technologies certainly hold the key to new user-driven market opportunities in order to fundamentally change the way healthcare will be delivered which might also reduce the financial exposure of national governments.

However, due to healthcare and ambient-assisted living being understood as a heavily regulated market with tight political control, return of investment (ROI) is typically expected within the same financial year. This might be one reason why the pickup rate of e-health technology in Europe has been rigid and behind target [10]. Future business models need to reflect these requirements in order to exploit the full market potential.

As important for the understanding of the economic relevance of healthcare, wellness, and ambient-assisted living and in order to comprehend the potential overall value of requirements engineering in these particular domains a slightly more abstract but extremely important socioeconomic aspect shall be mentioned in order to complete the picture, namely social capital. Social capital has been brought into the focus of the public discussion mainly through a monographic analysis of the postwar US American society [11, 12]. Also subject to slightly different definitions, the concept of social capital might for the purpose of this chapter follow the definition of Putnam, Leonardi, and Nanetti as "*features of social organization, such as trust, norms, and networks that can improve the efficiency of society by facilitating coordinated actions*" [13]. If ICT including e-health and m-health technologies can manage to virtualize these features and integrate them into a generally accepted holistic approach, then this would add significant value to healthcare systems globally. This approach could be integrated into and utilized by social networks which by using Putnam's, Leonardi's, and Nanetti's description could potentially generate significant amounts of social capital. However, so far it has been difficult to quantify the value that could potentially be released and further research work on this will be needed [14].

1.5 The Emergence of New Models for Health and Care

Healthcare models are changing. Changes to the way healthcare is delivered have a huge impact on technology requirements. The implications of putting the user at the center of the care model and shifting the point of care to the periphery have to be understood in order to conduct a meaningful requirements engineering process in the healthcare, wellness, and ambient-assisted living domain.

Ever since the government led implementation of structured public healthcare in Europe in the sixteenth century healthcare systems used to be hospital centered and expert driven. Patients were put at the periphery of the system with a clear focus on the requirements of the state or the ruling class. Experts were needed to maintain the functionality of the system and subsequently the health of the nation. Their knowledge and expertise, which was then passed on from generation to generation, from master to apprentice secured them a pivotal role.

Despite spectacular and dramatic historical errors such as the rejection of Semmelweis' discovery of the relevance of hand hygiene the hospital-centered, expert-driven approach lasted almost all through the twentieth century. Hungarian physician Ignaz Semmelweis (1818–1865) proposed hand hygiene with chlorinated lime solution to stop the spread of puerperal fever in 1847 while working at the obstetrics' department of Vienna's General Hospital. Puerperal or "childbed" fever then was associated with fatalities of 10–30 % in pregnant women and their newborns. Despite clear evidence that hand hygiene would reduce the mortality of childbed fever by magnitudes (from 10–30 % down to less than 1 %) Semmelweis' views were rejected by the established elite.

An important driver for the change of the way healthcare is going to be delivered has clearly been the transition from industrial and agricultural societies to service societies. Due to the postwar changes in our lifestyles the case mix in accident and emergency departments has completely changed. Acute surgical interventions are in dramatic decline. Acute trauma following industrial accidents, farming accidents, and motor-vehicle accidents was the original driver for the implementation of the concept of the accident and emergency departments. According to the UK Reporting of Injuries, Diseases and Dangerous Occurrences Regulations the number of fatal occupational accidents dropped between 1974 and 2013 by 85 % and the reported nonfatal injuries between 1974 and 2012 dropped by 77 % [15]. In 2012–2013 road accidents accounted for 1.3 %, assaults for 0.9 %, and sports injuries for 1.8 % of a typical case mix in English accident and emergency departments, all together accounting for not more than 4 % of all cases [16]. Major trauma accounted for just 0.2 % of all cases presented to accident and emergency departments in England in the period 2009–2010 [17]. This trend is consistent across most European countries.

Since the 1980s, the number of hospital beds in Europe has been systematically reduced partly in an effort to curb the costs of the provision of care, partly because technological and pharmaceutical progress made hospitalization unnecessary or reduced the average length of stay and allowed for outpatient treatment (Fig. 1.3: hospital beds, Fig. 1.4: average length of stay).

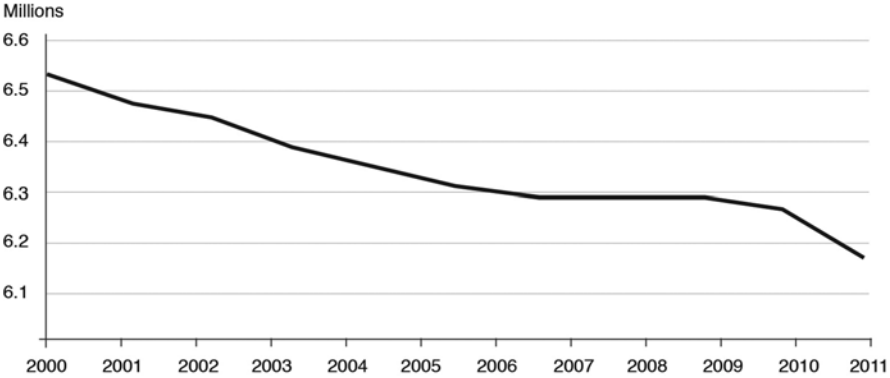


Fig. 1.3 Hospital beds in OECD countries

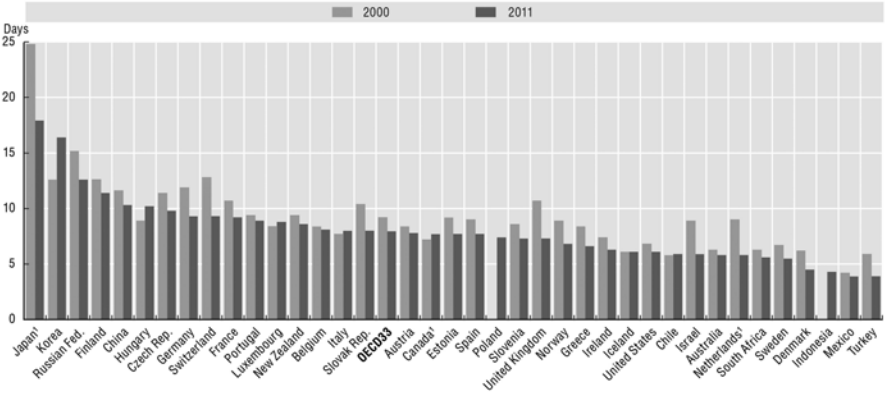


Fig. 1.4 Average length of stay in hospital, 2000 and 2011

At the same time a reciprocal trend can be observed with regard to day cases where patients only stay for several hours after a surgical procedure and are discharged home on the same day. The figures have been rising consistently across Europe and the USA over the last decade. Examples for surgical interventions, which used to involve several hospital bed days and are now performed selectively as day cases are cataract operations depicted in Fig. 1.5 and tonsillectomy depicted in Fig. 1.6. The difference in case numbers between 2000 and 2010 is highlighted.

Another important factor contributing to the shift of care models surely lies within the major societal changes, which have been triggered by the demographic challenges the majorities of countries and in particular the more developed countries have been facing since the 1980s. The population in these countries is ageing at an unprecedented rate and the fertility rates are in decline. According to Eurostat the average fertility rate in Europe was around 1.6 in 2012. To maintain population growth the fertility rate needs to be well above 2. Even migration at the current level is

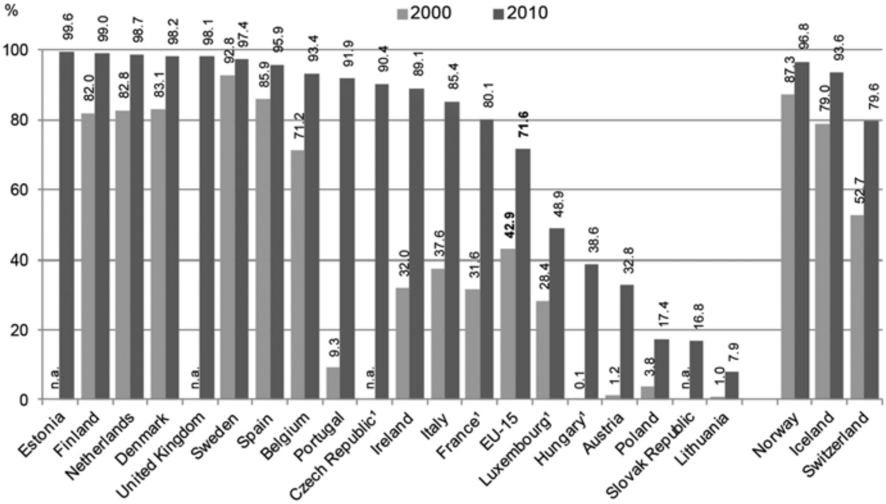


Fig. 1.5 Share of cataract surgeries performed as day cases, 2000 and 2010

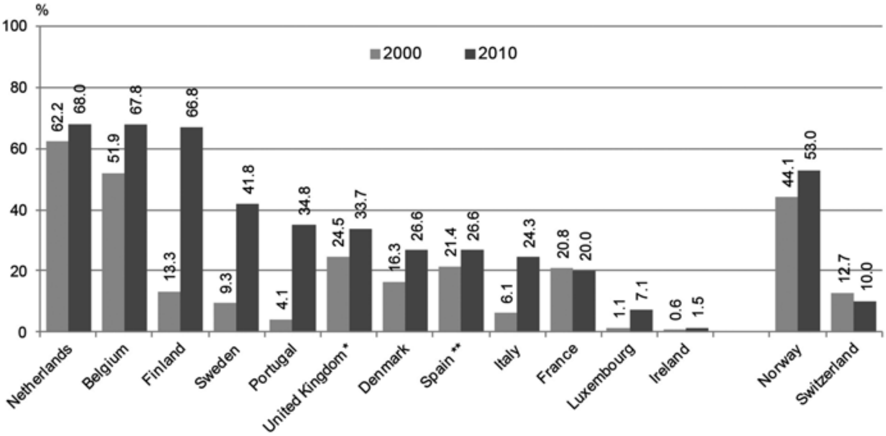


Fig. 1.6 Share of tonsillectomies carried out as day cases, 2000 and 2010

not able to compensate for this development and to stabilize the population. This trend will become more severe over the next two decades and will dramatically increase the demand for health and care. There are already signs in some European countries that the reduction of hospital beds which seemed to be the key to efficiency savings is unsustainable given the changing demographics of our societies. Political efforts are under way to establish elements of self-care supported by new information communication technologies.

With the recently emerging technologies such as superfast broadband and superfast mobile connectivity, mobile health applications (m-health), and remote diagnostic

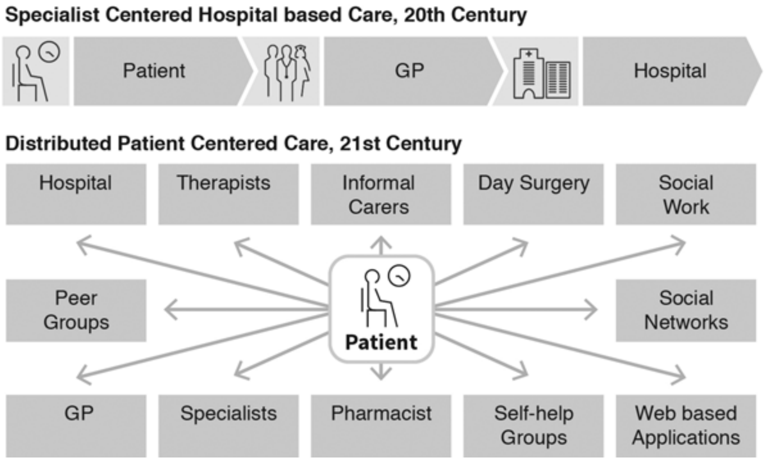


Fig. 1.7 Global shift in care models

and treatment schemes the stage is set for a phase transition which is about to revolutionize the provision of healthcare. In some European countries digital treatment is already available on prescription [10]. All of this is meant to support the shift from a hospital-centered, specialist-focused system to a distributed patient-centered approach. Instead of creating hierarchical models with the point of care close to the professionals the care model of the future will be based on patient-centric health ecosystems where patients, formal and informal carers, and other stakeholders will be hyperlinked in order to provide care on an appropriate level at anytime, anywhere, anyhow using digital communication technologies and virtualization. This will shift the point of care towards patients and will meet the needs of an older, less "physically" mobile society.

Distributed patient-centered care will put the patient in the center of the treatment process from a logical perspective while the need of physical contact between patients and professional will be reduced to the appropriate level. This will also meet the requirements of communities in remote and rural locations who so far have experienced some serious inequalities with regard to access to healthcare.

The transition from the hospital-based expert-focused care model to the distributed patient-centered care model is well under way, but it will certainly not be an easy ride. It will require the design, development, and implementation of new technologies on all levels and also the integration of these new technologies in existing complex social systems (social-technological alignment). Requirements engineering will play a major role in this process in order to shorten development cycles, improve pickup rates, and reduce implementation costs.

However, there is evidence that the care model, which has been unchanged for 400 years, has started to undergo groundbreaking changes. It seems that the care model is in a transition from a hospital-focused expert-centered healthcare approach to a distributed patient-centered model. Figure 1.7 illustrates.

1.6 The Evolution of Digital Health

Digital health is a technical term summarizing a variety of undefined and sometimes synonymously used expressions for interventional and diagnostic technologies based on the use of information communication technologies for the healthcare, wellness, and ambient-assisted living domains. The term digital health might be regarded as the best fitted largest denominator and seems to be most suitable for the purpose of summarizing ICTs applied in the healthcare, wellness, and ambient-assisted living domain. The most popular expressions are currently e-health and m-health but there are also the terms tele-medicine or tele-health which used to refer to face-to-face online consultations between patients and professionals or between different professionals. With videoconferencing becoming more and more embedded into society through services such as “skype” the technical terms tele-medicine or tele-health have lost specificity.

The evolution of digital health is rapidly progressive. While spending on pharmaceuticals has come down recently through the loss of patent protection of major brands, the spending on ICT in healthcare is predicted to grow to 18 billion Euro globally until 2017 [1, 2].

The evolution of digital health has not been a linear process but has been unfolding at different paces hardly depending on technological possibilities alone but more on social-economic and political factors [12]. Figure 1.8 gives an overview of the time lines of digital health.

Historically the starting point of digital health lies back in the 1960s where mainframe computers were introduced to support the management of quickly growing hospitals and health care providing organizations to process staff payments, the

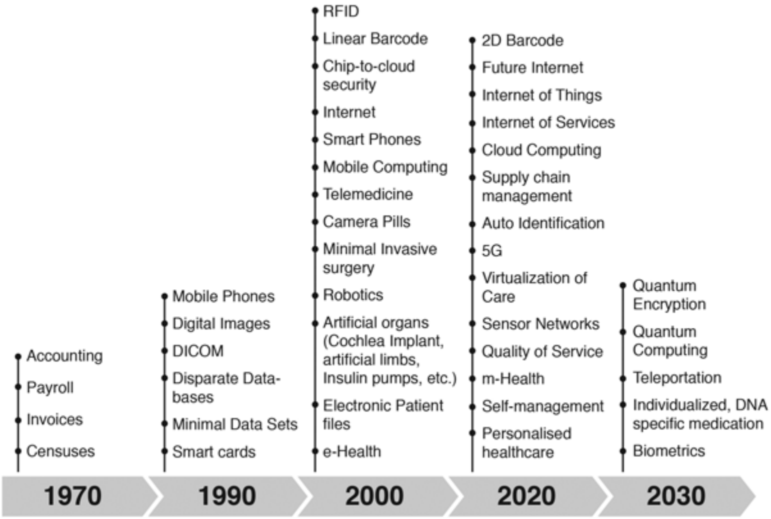


Fig. 1.8 Evolution of digital health

management of human resources and the management of stock orders. Due to the fast-growing populations in the 1960s and 1970s healthcare became a commodity consumed by masses. The growing populations generated not only a demand, but also an imperative for healthcare providers to process patient data quickly. Hospitals emerged in numbers and with this came an exponential increase in the number of employees. Over the years more effective administrative strategies emerged in order to bring together patients, healthcare professionals, and insurance companies. Fast flow of information is required to establish seamless workflows and guarantee the timely "cash flow" along the value chain. Also, operational processes in hospitals such as selection of food, management of health insurance memberships, and orders to vendors and suppliers started to be electronically processed. In the 1970s big mainframe computers processed data encoded on thousands of punch cards.

The next evolutional cycle was triggered by the emergence of the DICOM standard and the use of computing power to process digital images leading up to the computer—and magnet resonance tomography and positron emission tomography, but also digital subtraction angiography, doppler sonography, and ultrasound. The DICOM standard was essential for healthcare providers to manage the rapidly increasing numbers of the different digital imaging techniques.

Through the emergence of the client-server computer technology in the 1980s the digitalization of hospitals made rapid progress. However, over the years this rapid unstructured growth created patchwork hospital IT systems and let to island solutions, fragmentation, and lack of interoperability. In a way we are now paying the price for this development and overcoming of fragmentation and providing interoperability is one of the key challenges in todays Internet of Things, e-Health and m-Health research domains.

Until the 1990s digitalization was mainly driven by the requirements of the administrations of the key stakeholders, such as hospitals, health insurers, and public health organizations. The rollout of the mobile phone technology in the early 1990s and the emergence and explosive deployment of wireless networks paved the way for what has now become known as m-health. Significant progress with regards to smart devices could be noticed in the early 2000.

However, digital health is still regarded as fragmented and based on island solutions and the European Commission is putting considerable financial and political effort into harmonization in order to establish a unified market and to meet the needs of the European citizens [12, 18, 19]. Harmonization is also boosted by recent trends to collect and analyze large amounts of individual unstructured data, a process, which has become known as "Big Data." Unstructured in this context refers to the fact that big data sets are typically obtained from third parties with limited information about the consistency of data sets. Although there are some popular areas of interest such as research on the human genome in order to enable earlier and more effective "personalized" care or integration of "unidentifiable" data for pharmaceutical research there are many open questions associated with the mass collection and processing of unstructured data sets, such as who owns this data and how reliable is this data. However, it can be expected that "Big Data" technologies will be used in areas such as public health to monitor the impact of environmental factors and to speed up the process of pharmaceutical research.

There can be no doubt that over the last decade information communication technologies, microbiology, and nanotechnology have created a massive boost in digital health innovation. Unfortunately there is a staggering backlog in implementation and validation of new technologies although some of them certainly do carry the potential to change the way healthcare will be delivered. Over the last 10 years or so austerity measures have prevented a rapid progressive change of healthcare systems due to shortening of jobs and resources. However, meaningful large-scale changes are needed in order to guarantee access to high-quality healthcare for everybody in years to come, which has been acknowledged by the governments [12, 19].

One of the flipsides of a rapid expansion of hospital information technology (IT) systems in the face of tight resources since the late 1970s is the fact that IT systems have never been radically renewed. Typically, IT systems in hospitals have been extended database by database surrounded by another and yet another firewall rather than to instantiate a new system from scratch. This is also due to the fact that these days a hospital would not function without a fully operational IT system. It would be unthinkable to shut the system down even if it was only for several days to install new hardware. This idea might also be underlined by the fact that with regard to strategic planning by governments, hospitals and their affiliated networked infrastructures fall under the category “Critical Infrastructures” highlighting the relevance of these systems for the seamless day-to-day functionality of public live and the running of states.

Nowadays, nanotechnology and embedded systems are widespread and a reality of everyday life. Digital health technology can be found in a huge variety of mobile diagnostic and therapeutic devices from ECG machines which monitor heart activity and insulin pumps which replace part of pancreas organ function to help people to manage their diabetes problem to implanted pacemakers and defibrillators, which intervene on demand in case of cardiac malfunction. The number of applications, especially of embedded systems in the healthcare, wellness, and ambient-assisted living industry, is uncountable. However, most of these systems are closed-loop systems, which cannot be accessed easily. On the other hand the lack of interoperability and “open” interfaces prevent the seamless collection of data, which if done in keeping with the existing guidelines, regulations, and standards could be of large benefit with regard to the development of future diagnostics and therapies. The pros and cons and problems associated with a potential “Internet of Things” in the healthcare domain have recently been subject to discussions and consultations by the European Commission [20].

The most relevant future trends at this point in time are clearly related to the development and implementation of m-health-based self-management tools, which would see patients using their smartphones to monitor their chronic conditions, their medication, and their individual wellness data and share information with selected users using social media. Security and privacy issues are at the heart of upcoming technologies. Potential solutions reach from strategic ideas such as “federated identity” and encryption to new hardware-based encryption (chip to cloud) and futuristic ideas such as quantum computing. Although it is unlikely to appear in this decade quantum computing could also be used to form a logical continuation of the 3D printing technology which could see objects being instantly replicated at any given place using quantum physics effects. In the upcoming decades this could be used for remote implantation of molecules (pharmaceutical substances, devices) into the human body using a transducer connected to a mobile phone. Although this idea might seem somewhat far-fetched the teleportation of molecules is already a reality [21]. There can be no doubt that biometrics and individual real-time data analysis will play an increasing role in personalized healthcare and the application of individualized medication. The key drivers for digital health over the coming decades will be the virtualization of care in order to improve but at least maintain the accessibility of healthcare for ageing populations, but also the introduction of completely new ways of treatments consisting of a combination of personalized drugs and the mining and processing of a large quantity of individual and environmental data (Big Data). The rollout of 4G and 5G technologies will catalyze these trends. However, new technologies are needed to ensure that individuals are in control of their data and that data security and privacy legislation can be enforced all across the value chain.

1.7 Social Technological Alignment

ICT is progressing rapidly and many new technologies are readily available. However, there have been reports of very limited uptake of these technologies in the healthcare, wellness, and ambient-assisted living domains compared to sectors such as finances, manufacturing, and logistics [12]. In other words the available technologies are not implemented and integrated into the clinical work flows and there is clearly a massive market opportunity assuming that health care systems will globally have to dramatically increase effectiveness and efficiency in order to meet the demands without putting additional financial burden on the national economies. The challenge for requirements engineering in health and care is clearly to identify new and efficient ways to catalyze social technological alignment in order to open global markets with enormous growth potentials.

The dichotomy of innovation namely in a technological and social context has been subject to controversial discussions since the 1970s [22, 23]. While some argue that innovation is a self-driven, linear process (technological determinism) others are adamant that innovation is a social process and that it is entirely up to society to either accept or reject technology (social determinism). Analyzing the existing literature so far it seems that neither of the defenders of extreme positions is able to make a convincing case. While new technologies are typically presented to society by a small number of visionary researchers and entrepreneurs there can be no doubt that it is up to society to accept or reject the proposed technology. Acceptance of the preposition might result in societal change and in many cases also to a subsequent change of the technology. Innovation can thus be understood as a social process driven by an interactive discourse between technology and society.

From an application researcher's perspective social technological alignment may be understood as a process of proactive mediation between technological and social determinism in order to improve compatibility and reduce resistance towards any given implementation process. Requirements engineering in the healthcare, wellness, and ambient-assisted living domain can be understood as the first step in the mediation process in order to clarify the actors, their roles, the internal and external interfaces of the system in question, and the requirements of all actors, be it humans or machines. Requirements engineering aims at establishing a shared understanding between the social context and the software domain and at selecting the right technological solution to solve the problems patients, medical personnel, healthcare organizations, and or society have [24–25].

Healthcare is typically delivered by a multiprofessional team with a heterogeneous and diverse background; hence from practical experience it is highly recommended to clarify technical terms before entering requirements engineering processes in the healthcare, wellness, and ambient-assisted living domain to avoid misunderstandings. In fact, one of the roles of requirements engineering in healthcare, wellness, and ambient-assisted living is the establishment of transparency of processes and the provision of communicative semantic interoperability to all actors, which typically starts with the analysis of systems, their components, and their interactions.

Social technological alignment as a factor is of huge importance when creating business plans and preparing technologies for rollout. Due to progressively shorter product cycles and quickly emerging "me-too" products quick adaptation of innovative technology will increasingly be the factor to tell between success and failure; hence tools to measure and anticipate social technological alignment are highly desirable. Lately, parameters and key performance indicator have been proposed for the early detection of potential resistances and incompatibilities, which could help to avoid premature releases of technologies and increase the success and implementation rate. Table 1.1 shows a recently proposed social technological alignment matrix (STAM) for the speedy and standardized assessment of relevant factors in the social technological alignment process in health and care settings.

1.8 Challenges for Requirements Engineers in the Healthcare Domain

Requirements engineering is aiming to bridge the gap between the social and the technical worlds [27]. In order to achieve this effectively and efficiently requirements engineers and those who wish to act in a similar capacity should have a considerable amount of background knowledge specific to the healthcare domain. In the context of the previous Sects. 1.1–1.6 we have discussed the political, historical, demographical, and socioeconomic dimensions of healthcare and have elicited the current trends with regard to digital health. What does this mean for individuals

Table 1.1 The social technological alignment matrix (STAM)

Parameters	Technological	Social
Readiness levels: Increase the success rate of technology transition and likelihood of people's adoption of the new technology.	The Technology Readiness Levels (TRLs) are a technology management tool developed by the United States National Aeronautics and Space Administration (NASA) to evaluate the maturity of a technology prior to integrating this technology into a system [22].	The Technology Readiness Index (TRI) is a multiple-item scale to measure readiness to embrace new technologies [23, 26].
Shared values: Having shared goals and purpose will ensure that new technology is fully interoperable and compatible with other technologies and meet the highest standards of ethical compliance.	Conformance with open interoperability standards such as ISO 13407 (human-centred design for interactive systems), ISO 13485, ISO 14971, and IEC 62304 (development process quality for medical device software) and ISO/IEC 27002 (information security management) and the NASA Reuse Readiness Levels (RRLs).	Societal acceptance of new technology requires sound ethical reflection and adherence to laws and regulations guided by individual, organizational, regional, national, and international code of ethics and laws. Some ethical areas of concern relevant to health technology assessment include benefit and harm, autonomy, equity, stakeholder values, acceptability, quality of life, and impact on family and caregivers.
Motivation: Social acceptance of new technology is the primary success factor of the new technology.	As an economic entity, the inner motivation of technological innovation for an organization is its profitability (in normal and rational economic environment). The decision of innovation then depends on the expected benefit from technological innovation, which can only be realized in market competition.	The Technology Acceptance Model (TAM) [18, 24, 25] and Unified Theory of Acceptance and Use of Technology [19] measure the perceived usefulness and perceived ease of use. Extrinsic motivation is captured by the perceived usefulness construct in TAM [18]. Intrinsic motivation can be measured by assessing an individual's level of computer playfulness [18].
Elasticity: Elasticity is a key priority in new technology acceptance.	Technology needs to be scalable in order to allow adjustment in keeping in user needs and demands (ISO 9241).	The higher the level of flexibility in user groups, the higher the chance of acceptance of a new technology—openness [27].
Control: Improved control will ensure effective software acceptance.	The Unified Theory of Acceptance (UTAUT) is a tool for managers to assess the likelihood of success for new technology introductions and helps them understand the drivers of acceptance I order to implement interventions such as training and marketing for the target population of users who may be less likely to adopt and use new systems [25].	The ability to determine the rate of change and the fear, threats, and trust of new technology can be measured by perceptions of internal control (computer self-efficacy [28]) and perceptions of external control [18].

involved with a requirements engineering project in the healthcare wellness or ambient-assisted living domain? What are their roles? What can they expect?

In recent years co-design strategies have been regarded as imperative for the development of new technologies and consequently requirements engineering has moved into the focus of technology providers and user groups. There is evidence that requirements engineering is a potentially powerful tool, which deserves to be sufficiently funded throughout the development process. The current cost share may be valued as high as 50 % and still releasing efficiency reserves and delivering value for money across the project board.

Requirements engineering is typically related to clearly structured and technical domains such as the software industry. In general requirements engineers, stakeholders, technology owners, and developers share the same vocabulary and the technologist point of view. Processes are frequently deterministic and based on well-understood models and concepts. The requirements engineer has to have expert knowledge and a clear understanding of the interdependencies of technology and economics; however in the healthcare domain as a politically controlled and regulated market special rules apply.

The economy of providing healthcare is still based on socialized medicine, which means that the type of treatment can in most European systems not be chosen freely by the individual patient but depends on statistical data on the efficiency of treatments for any given condition. Similar models are valid for some US health maintenance organizations (HMOs). However, a lot of the recent developments suggest that this is about to change. Governments are pushing towards remote self-management strategies in order to curb the costs of our ageing societies. Technologies, which will enable this transition are in principle available but have yet to be implemented.

In the healthcare, wellness, and ambient-assisted living domain the challenges for requirements engineers and those who are seeking to develop an understanding for requirements engineering in this particular domain might be further reaching and more complex. Experience clearly shows that it is mandatory not only to understand the diverse health and care processes but also to understand the driving forces behind the way how healthcare is delivered in any given region or country. This might involve political and cultural aspects as well as socioeconomic factors. On the other hand the requirements engineer in healthcare needs to be aware of standards, rules, and regulations on national, international, and global level, which are typically expressed by legislation, recommendations, and standards, for example ISO standards or ETSI standards for telecommunication. Interoperability has been identified as in particular challenging as over recent years ICT in health and care grew fragmented as island solutions, a process which has been proven difficult to reverse.

Of particular importance for a requirements analysis in the healthcare, wellness, and ambient-assisted living domain is also an awareness of social factors and relevant models, such as the biomedical or bio-psycho-social model of health and disease. Until the 1970s this seemed to be very simplistic. Health processes were sought to be deterministic and there was the idea that pathological processes could be easily objectivized by measuring agreed core parameters. The measurement of a blood pressure for example would easily show the significance of the pathological problem "hypertension" (high blood pressure). The higher the blood pressure—the higher the individual risk. Or in the case of obesity (overweight) it was a clearly understood concept that the more an individual eats the more they will gain weight—the more excessive the problem. This so-called *biomedical model* had been established over hundreds of years and seemed beyond any doubt. However, since the 1960s there was growing dissatisfaction with this model. Doubts with regard to the general validity of the biomedical model came from psychiatrists who would not be able to find any abnormal physiological measurements in their patients although there was no question that their patients would suffer from an illness. Also, the biomedical model struggled to explain psychosomatic conditions where psychological and social factors would trigger physical symptoms. In 1977 Engel proposed an extended model, the so-called *bio-psycho-social model*, which has since found increasing acceptance from a large number of scientists and medical practitioners [28]. The bio-psycho-social model has also obtained the full backing of the World Health Organization (WHO).

During assignments in the healthcare, wellness, and ambient-assisted living domain requirements engineers will inevitably be confronted with both models, the biomedical model and the bio-psycho-social model, and should carefully examine the implications of the application or rejection of any of the both models for each individual scenario. Processes might gain a lot of additional layers of complexities if social and psychological aspects are to be considered. So the requirements for a system to detect suicide risks in patients could be quite complex and may contain social and psychological elements and relatively sophisticated tools for operationalization in order to be very sensitive while on the other hand a relatively simplistic depression screening score might be easy to implement and very specific but lacks the sensitivity to detect that patients might hide their self-harm intend.

Another important challenge is clearly the fact that requirements engineers will frequently be dealing with healthcare professionals or healthcare managers who might have a completely different understanding or attitude towards technology compared with the point of view of the trained engineer. Problems frequently arise not so much on a logical level but on a semantic level. A good example is the term "*implementation*" which in the software industry typically is understood as the process of *coding* or more general as *programming*. However, in most industries including the healthcare industry the term "implementation" is normally understood as the process of integrating a technology, frequently new application systems, into the work flow of particular groups.

For requirements engineers it is crucial to verify almost permanently that there is a shared understanding with regard to the terminology and in particular the technical terms used. Jargon should be avoided to reduce the risk of misunderstandings.

Another important area which might create problems or even tension during the requirements engineering process is the very specific and distinct value set typically shared by medical professionals. Healthcare workers are frequently highly motivated individuals with idealistic and altruistic mindsets. Emotional and ethical factors certainly do matter and problems during requirements engineering workshops might arise from different interpretations due to the lack of a shared set of values.

Assumptions with regard to shared values and common ground especially during requirement workshops should be avoided. The far safer practice seems to be a proactive approach whereby the requirements engineer should initiate an open discussion in order to establish a shared semantic understanding and include frequent reassurance during the assessment process. These self-reflective elements are part of the interaction on the shop floor when conducting structured assessments.

In our practice voice and video recordings have been proven as helpful whereas notes seem to be less reliable. In any case the requirements engineer should be aware that dialogues with a selected group of representatives might not represent the opinion and the opinion of the majority of the users and stakeholders. In fact it can only be recommended to maximize the group of interviewees in order to collect a broad spectrum of requirements.

Selection of functional requirements should be pursued by following a standardized algorithm. However, data should never be collected randomly but there should be a clear aim and objective associated with the decision to explore and capture data in order to keep the process of requirements engineering lean, effective, and efficient.

1.9 Lessons Learned

This book enhances and facilitates relevant knowledge about requirements engineering in the healthcare, wellness, and ambient-assisted living domains. It is well suited for the non-expert but also addresses the needs of requirements engineering students, decision makers, and medical professionals. Multidisciplinary information is presented by experts in the relevant field in an easy-to-understand and easy-to-digest format. The following chapters will elaborate on different aspects of requirements engineering in healthcare and will take into account experience from real-world cases.

The following key messages should be remembered:

- Health and care are heavily regulated markets and are exposed to a variety of external, nontechnical influences which may well be more relevant than the actual technical issues (compare Tom Peters “Hard is Soft and Soft is Hard” [26]).
- The average share of GDP spent on healthcare in 2013 was around 10 % in Europe and 17 % in the USA, and 5 % in China. The trend shows that these figures are set to grow as the populations are ageing and the reproduction rate continues to drop [3–5].
- The spending on medication by health insurers and out-of-pocket spending has stopped growing over recent years in the USA and OECD countries due to the expiry of patent protection on many brands and a subsequent shift towards cheaper generic drugs. In China spending on healthcare is continuously growing and expected to double in the next decade to one trillion USD in 2020. This means that in principle consumers have the means to spend on future digital technologies such as m-health where strong global growth has been predicted [1, 5].

- In order to maintain current levels of care virtualization of care will have to progress rapidly. The rollout of digital health is worldwide high up on the agendas of national governments in order to release efficiency reserves and curb the still growing healthcare budgets [19].
- Successful requirements engineering in healthcare requires an integrated multidisciplinary approach to facilitate social technological alignment on different social and technological levels.
- In health based self-management is expected to soar. The global turn-around is expected to reach 18 billion Euro by 2017.

References

1. European Commission (2014). http://ec.europa.eu/digital-agenda/en/news/mhealth-what-it-infographic
2. Centre for Medicare and Medicaid Services (CMS), NHE Fact Sheet 2012. http://www.cms.gov/Research-Statistics-Data-and-Systems/Statistics-Trends-and-Reports/NationalHealthExpendData/NHE-Fact-Sheet.html
3. OECD, Health at a Glance 2013 (2013) ISBN 978-92-64-205024
4. The World Bank (2013) Health expenditure, total (% of GDP). http://data.worldbank.org/indicator/SH.XPD.TOTL.ZS
5. Le Deu F, Parekh R, Zhang F, Zhou G (2012) Healthcare in China: entering 'uncharted waters'. McKinsey, New York
6. Buckner L, Yeandle S (2007) Valuing carers—calculating the value of unpaid care. Carers UK, London
7. IMS Institute for Healthcare Informatics (2012) The use of medicines in the United States: review of 2011. http://www.imshealth.com/ims/Global/Content/Insights/IMS%20Institute%20for%20Healthcare%20Informatics/IHII_Medicines_in_U.S_Report_2011.pdf
8. http://www.oecd.org/els/health-systems/health-spending-continues-to-stagnate-says-oecd.htm
9. Mirkin B, Weinberger MB (1999) The demography of population ageing, United Nations 1999. http://www.un.org/esa/population/publications/bulletin42_43/weinbergermirkin.pdf
10. https://www.barmer-gek.de/barmer/web/Portale/Versicherte/Rundum-gutversichert/Leistungen-Beitraege/Lexikon_20Leistungen/Alle_20Eintr_C3_A4ge/App-auf-Rezept.html
11. Huawei (2013) 5G. A technology vision. Huawai Technologies CO., LTD
12. European Commission (2011) Report on Public Consultation on eHealth Action Plan 2012–2020
13. Putnam RD (1995) Bowling alone. America's declining Social Capital. J Democracy 6:65–78
14. Putnam RD (2000) Bowling alone. The collapse and revival of American community. Simon and Schuster, New York
15. UK Government health and Safety Executive (2013). http://www.hse.gov.uk/STATISTICS/history/index.htm
16. Health & Social Care Information Center (2014) Hospital episodes statistics, accident & emergency attendances in England 2012–2013
17. National Audit Office (2010) Major trauma care in England. http://www.nao.org.uk/wp-content/uploads/2010/02/0910213.pdf
18. Digital Agenda for Europe, Europe 2020, Action 75: Give Europeans secure online access to their medical health data and achieve widespread telemedicine deployment. https://ec.europa.eu/digital-agenda/en/content/action-75-give-europeans-secure-online-access-their-medical-health-data-and-achieve

19. European Commission (2012) Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the regions eHealth Action Plan 2012–2020—Innovative healthcare for the 21st century
20. European Commission (2014) Green paper on mobile health (mHealth). http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth
21. Ursin R, Jennewein T, Aspelmeyer M, Kaltenbaeck R, Lindenthal M, Walther P, Zeilinger A (2004) Quantum teleportation across the Danube. Nature 430:849
22. Williams R, Edge D (1996) The shaping of technology. Res Policy 25:865–899
23. Berg M (1998) The politics of technology: on bringing social theory into technological design. Sci Technol Human Values 23:456
24. Glinz M, Fricker S (2014) On shared understanding in software engineering: an esseay. Computer Science - Research and Development. doi 10.1007/s00450-014-0256-x. See also: http://link.springer.com/article/10.1007/s00450-014-0256-x
25. Nuseibeh B (2001) Weaving together requirements and architectures. Computer 34(3):115–119
26. Peters T (1987) Thriving on chaos: handbook for a management revolution. Macmillan, London
27. Pohl K, Rupp C (2011) Requirements engineering fundamentals: a study guide for the certified professional for requirements engineering exam-foundation level-IREB compliant. Rocky Nook, Santa Barbara, CA
28. Engel GL (1977) The need for a new medical model: a challenge for biomedicine. Science 196(4286):129–136

Chapter 2
Requirements Engineering: Best Practice

Samuel A. Fricker, Rainer Grau, and Adrian Zwingli

Abstract Many software solutions have failed because they did not meet stakeholder needs. In response to this problem a massive amount of techniques were developed to elicit stakeholder needs, to analyze the implications of these needs on the software, to specify proposed software products, and to check acceptance of these proposals. However, many of these techniques did not become industrial practice because they were not practicable or ineffective when used in real-world projects. To obtain an overview of what common practice is and to understand which techniques reflect best practice because they are particularly effective, we have surveyed a large number of industry projects. Based on 419 valid answers, this chapter gives an overview of commonly used requirements engineering techniques. It also shows which of the techniques, when used in a software project, correlate with requirements engineering success. The chapter concludes with recommendations for software projects and future research to improve requirements engineering practice.

2.1 Introduction

In 1995 the consultancy company Standish Group International published results of an industry survey that showed that only 16 % of the software projects were successful, 53 % were challenged, and 31 % complete failures [1]. Successful projects were those that completed on time and budget and produced a software product with all features and functions as initially specified. The low success rates described in the Standish report generated substantial attention by industry and politics.

S.A. Fricker (✉)
Software Engineering Research Laboratory, Blekinge Institute of Technology,
Karlskrona, Sweden
e-mail: samuel.fricker@bth.se

R. Grau
Zühlke Engineering AG, Schlieren, Switzerland
e-mail: rainer.grau@zuehlke.com

A. Zwingli
SwissQ Consulting AG, Zürich, Switzerland
e-mail: adrian.zwingli@swissq.it

S.A. Fricker et al. (eds.), *Requirements Engineering for Digital Health*,
DOI 10.1007/978-3-319-09798-5_2

The Standish survey pointed to software project practices that needed improvement. According to the respondents, the most frequently stated factors that influenced project success were user involvement, executive management support, and a clear statement of requirements. These factors show that requirements engineering is crucial to achieve project success. User involvement is critical for building a software that will be understood by the users, that will be used appropriately, and that creates joy [2]. Management support is critical to align the software with the strategic goals of the organization [3]. Clearly stated requirements contribute to a shared understanding between the project team and the software product's users, management, and other stakeholders. The shared understanding reduces the risk of unsatisfactory outcome and rework of project results [4]. Influenced by these insights, software engineering practice matured over time. Thirty-two percent of the software projects were successful according to the Standish survey published in 2009 [5].

Even though many requirements engineering techniques exist for involving users, for obtaining management support, and for achieving shared understanding, we lack an understanding of whether these techniques make requirements engineering successful. Some researchers believe that no technique would do and claim that good requirements practices are neither sufficient nor necessary [6]. The best we can say today is that the techniques are used inconsistently: some techniques get used by some projects but not by others [7, 8]. Companies that care about requirements engineering seem have a preference for Quality Function Deployment, prototyping, Data Flow Diagrams, role playing, and decision trees [9]. However, we do not know whether any of these techniques correlates with requirements engineering success, thus should be used systematically.

This chapter intends to develop an understanding of what practice makes requirements engineering successful by reporting the results from an own large-scale industry survey. The survey investigated whether the use of requirements engineering techniques differed between projects with successful and unsuccessful requirements engineering. The results show that a few techniques indeed correlated with success. In addition, also the ability to apply a broad variety of requirements engineering techniques is important. These results imply that best practice would be to utilize the few effective techniques and pragmatically select complementing techniques that suit well the type of software being developed and the situation that requirements engineering is confronted with.

The remainder of this chapter is structured as follows. Section 2.2 gives an overview of requirements engineering state of the art that was studied in the industry survey. Section 2.3 describes the survey methodology. Section 2.4 characterizes the projects that have responded to the survey, gives an overview of the requirements engineering practice of these projects, and shows the correlation of requirements engineering practice with success. Section 2.5 discusses the obtained results, gives recommendations for practice, and suggests implications for research. Section 2.6 summarizes and concludes.

2.2 Requirements Engineering State of the Art

2.2.1 Requirements Engineering Techniques

There is a long tradition of research and practice in requirements engineering. One of the early influential works describes requirements engineering as inquiry [10]. During an inquiry the requirements engineer asks questions about a future software product to stakeholders and turns the obtained answers into a specification. While doing so, new questions emerge that are posed again to the stakeholders to initiate the next inquiry.

Since these early days, a large number of techniques have been investigated to advance requirements engineering state of the art [11]. Still, Potts's inquiry remains a good model of how to think of requirements engineering in a software project. Today, a requirements engineer is expected to elicit needs and expectations from stakeholders, to model and analyze the impact of these inputs on the system together with the development team, and to check proposed implementations for acceptance by the stakeholders [12]. Once both the stakeholders and the development team agree, the requirements are used to steer development and, upon release of the solution, check whether the developed product fulfils the agreement. If the inquiry is done well, one can observe that a shared understanding emerges, requirements stabilize, and the stakeholders become satisfied [13, 14].

During elicitation the requirements engineer aims at understanding the project vision and constraints, the context that the product will be deployed into, and the stakeholders that will need to accept the product [15, 16]. Such requirements elicitation results in an overview of users, external systems, and other stakeholder viewpoints and a description of their respective background, interests, and expectations. A large number of techniques are known to elicit such information about the system requirements [17–19]. Table 2.1 gives an overview of selected elicitation techniques.

During analysis the requirements engineer aims at understanding how the requirements will be implemented by the software system [30], how they will be considered in the development plan [31], and how they will be used for the testing of the system [32]. Requirements analysis typically results in one or more prototypes, a definition of project scope or release plan, and a requirements specification for the system. Table 2.2 gives an overview of selected analysis techniques, Table 2.3 of planning techniques, Table 2.4 of relevant requirements types, and Table 2.5 of specification techniques.

During requirements checking, the requirements engineer checks that the right approach has been selected for fulfilling the vision and achieving the system goals and that the system will be accepted by the stakeholders. Requirements checking initiates a new inquiry cycle if the checked requirements turn out to be not good-enough. Requirements checking marks the agreement of the stakeholders on

Table 2.1 Selected requirements elicitation techniques

Technique	Description
Archaeology	Analysis of existing systems to understand their functionality, quality, and usage [20].
Creativity	The generation and selection of ideas to innovate or solve a difficult problem [21, 22].
Data mining	Search and filtering of requirements databases to identify relevant knowledge about stakeholder needs [23].
Interview	Meeting between a requirements engineer and a stakeholder to discuss topics of relevance for the system [24].
Introspection	Use of domain knowledge in combination with reflection and empathy to base requirements on experience [25].
Observation	Study of system use, possibly in the target environment and by real users, to understand usage processes and strengths and weaknesses of a current system [26].
Questionnaire-based survey	Paper or electronic form with questions and space for answers distributed to stakeholders to obtain an overview of stakeholder opinion [27].
Reuse	Use of existing specifications to avoid reinvention of requirements that already are adequate [28].
Workshop	Meeting between a requirements engineer and stakeholders to reach agreement between the workshop participants [29].

Table 2.2 Selected system analysis techniques

Technique	Description
Domain-driven development	Specifying the concepts of relevance in the context the system will be deployed into that are to be implemented or respected by the system [33].
Formal specification	Use of mathematical or formal-logic expressions to enable automated checking of completeness consistency, and correctness [34].
Informal Modeling	Sketching a model of something of relevance to reflect and discuss how the parts of that thing interrelate [35].
OOA	Specifying the structure, functionality, and behavior of the system usually with the object-oriented analysis language UML [36].
Prototyping	Paper- or tool-based approximation of the end-systems to increase the tangibility and authenticity of the planned system [37].
Quality checks	Checking whether the system fulfils its goals and whether functionality and quality are adequate and needed [38].
SA	Specifying the structure, functionality, and behavior of the system with a structured analysis language [39, 40].

contents and scope of the development project if the checking has been successful. Table 2.6 gives an overview of selected checking techniques.

The inquiry cycle leads to a dialogue between stakeholders and development team that can be seen as a negotiation [64]. The negotiation results in an agreement between the stakeholders and the development team about the product to be developed. This agreement, represented by the approved requirements specification, is then

Table 2.3 Selected requirements planning techniques

Technique	Description
Business case	Evaluating whether a set of requirements has to good return-of-investment and should be included into project scope [41].
Prioritizing	Ranking the requirements to obtain an order of how they shall be addressed by the project work [42].
Release planning	Defining the contents of one or more releases to define the scope of the software system [43].
Road mapping	Coarse-grained, long-term planning to agree with stakeholders and suppliers for how the software system shall evolve [44, 45].
Triage	Filtering the requirements to determine what requirements are relevant and what requirements are not [46].
Vision	Defining the problem that is addressed, the key idea of the solution, and how the solution improves state of the art to align the work of developers and stakeholders [47].

Table 2.4 Selected requirement types

Type	Description
Behavior	Behavior is a sequence of states that determine how a system, artifact, or class reacts to events [48].
Formal property	A formal property can be tested for correctness, completeness, and consistency with automated tools [49].
Function	Function is a reaction to inputs or an action of a system [50].
Glossary	A glossary defines terms, abbreviations, acronyms, synonyms, and homonyms [12].
Interface	An interface connects a system with its environment. Typical interfaces are user interfaces [51] and interfaces to other software systems [52].
Process	A process is a series of actions or operations implemented by people, organizations, or software to achieve a goal [53].
Quality	Quality is a characteristic of a software system such as performance, reliability, security, compatibility, portability, usability, and maintainability [54].
Scenario	A scenario is a story of how users and systems interact to achieve a goal [55].
Stakeholder	A person, group, or organization who gains or loses something with the software [56]. May be denoted agent [57] or actor [36].
Structure	Structure refers to entities or systems with their attributes and relationships [36].

Table 2.5 Selected specification techniques

Technique	Description
i* or KAOS	Specifying agents, goals, and formal properties with formal languages to enable reasoning about goals and goal-achievement [57].
Natural language	Specifying requirement with words and sentences to achieve specification flexibility and understandability. Language templates may be used to improve precision [58].
SA diagrams	Specifying functions, processes, structure, and behavior with one of the graphical notations proposed by structured analysis to achieve precision and make structure visible.
Tables	Specifying concepts to achieve an understanding of the terminology [59] and or rules for how conditions affect system behavior [60].
UML diagrams	Specifying functions, scenarios, processes, rules, relations, behavior, and deployment with graphical notations from the Unified Modeling Language to increase precision and show structure.
User screens	Specifying the user interface with paper or tool-based mock-ups to increase the tangibility and authenticity of the planned system.

Table 2.6 Selected checking techniques

Technique	Description
Automated checking	Testing a formal specification of the system to detect conflicting and missing requirements [61].
Inspection	Review of the requirements specification by all relevant stakeholders with a formal process that is effective at discovering problems and leads to in-depth understanding of the specification [62].
Peer review	Feedback by one or more requirements engineers to support and assure the quality of the specification work.
Prototype review	Discussion and use of the prototype, for example in a role-play, to explore uses and check acceptance of the system.
Simulation	Approximation and review of the behavior of the system with an appropriate tool to check correctness of the behavior [63].
Walk-through	Efficient review of the requirements specification by discussing the requirements specification in their sequence with stakeholders.

Table 2.7 Selected requirements negotiation techniques

Technique	Description
Conflict management	Discovering and resolving conflicts among stakeholders and between stakeholders and development team [12].
Handshaking	The review and discussion of implementation proposals to align the planned implementation of the software system with stated and unstated stakeholder needs [65].
Negotiation analysis	Analyzing possible negotiation outcomes and selecting a value-creating, fair agreement [66].
Power Analysis	Analyzing power and influence of stakeholders and planning how to interact with them[67].
Prioritizing	Ranking the requirements to obtain an order of how they shall be addressed by the project work [42].
Strategy alignment	Aligning requirements with company strategy, for example through explicit traceability [3].
Variant analysis	Analyzing and selecting alternative features or ways of solving a problem [68].
Win-win negotiation	Structured, possibly tool-supported approach to identification of options for agreement and selection of the appropriate option [69].

baselined and used to manage the development project and the release of the developed product. Table 2.7 gives an overview of selected requirements negotiation techniques and Table 2.8 of requirements management techniques.

2.2.2 *Requirements Engineering Success*

For evaluating requirements engineering practices, one needs to understand how to measure requirements engineering success. The most thorough study that answered this question was a survey that tested 32 indicators with 30 requirements

Table 2.8 Selected requirements management techniques

Technique	Description
Baselining	Versioning requirements and specifications and communicating these as a baseline to stakeholders [70].
Change management	Controlled process of collecting change requests, analyzing impact, and deciding about the change [71].
Process measurement	Measuring requirements engineering and implementation efficiency, for example in the form of value stream analysis [72].
Progress tracking	Monitoring the life cycle of requirements from discovery to selection, implementation, and release [73].
Report generation	Generation of reports, such as requirements specifications, from a database of requirements.
Traceability management	Maintaining relationships between requirements and possibly other artifacts to express dependencies, conflicts, and synergies [74].

Table 2.9 Success measurements for requirements engineering [75]

Quality of RE service	Quality of RE products
Business-technical alignment: fit with strategy, ability and willingness to make business changes, and management support.	*Quality of cost–benefits analysis*: completeness and coverage of cost–benefit analysis, new benefits created by the new solution, and sufficient accuracy of cost estimates.
Stakeholder acceptance: awareness of business changes, extent of consensus, willingness to defend solution, and relationship to users.	*Argumentation of impact*: diagnosis of existing solution, traceability of supported processes to problem to be solved and to system goals, and traceability of strengths and weaknesses of new solution to replaced solution.

engineering experts [75]. It showed that requirements engineering success can be measured with *quality of requirement engineering service* and *quality of requirements engineering products*. Table 2.9 gives an overview of the indicators.

The quality of requirements engineering service refers to the effects a requirements engineer wants to achieve. These concern the alignment of the software product with business objectives and the alignment of it with stakeholder needs and expectations. Such alignment can be checked by asking the concerned stakeholders of whether they agree that system will deliver the desired impacts.

The quality of requirements engineering products refers to the work results delivered by the requirements engineer. These should include a comprehensive cost–benefit analysis and a description of impact with detailed traceability to supported processes, system goals, and the replaced solution. Such work results are tangible and can be easily inspected if they are presented in the form of a requirements specification.

In this chapter we use El Emam and Madhavji's success measurements to inquire what requirements engineering goals were important and whether these goals were achieved. This way of assessing the quality of requirements engineering service and products allows taking into consideration the many possible variations of what is important in given projects. It allows the respondents to judge whether requirements engineering was successful according to their own specific contexts.

El Emam and Madhavji's success measurement have the advantage of being measurable immediately when requirements engineering is concluded. However, they fall short in capturing the ultimate objective of requirements engineering. No measurement has been proposed to assess whether the specified system will be successful. For that reason, we extend the measurement framework outlined in Table 2.9 with the additional dimension of requirements engineering outcome. In the survey we thus ask the respondents whether the specified product met the goals the product was conceived for.

2.3 Industry Survey

We investigated the use of requirements engineering techniques and how much they contributed to requirements engineering success with an online survey [76]. We distributed an online questionnaire to people involved in software projects in an attempt to answer the following main research questions.

- RQ1: What requirements engineering techniques are used in software projects?
- RQ2: What are the goals pursued in requirements engineering?
- RQ3: Which requirements engineering techniques correlate with requirements engineering success?

The answers to RQ1 show how frequently each of the requirements engineering techniques is used, thus allows us to say what common practice is. Besides benchmarking practice, these results allow judgment whether techniques that were investigated in research were successfully transferred or not. The answers to RQ2 tell us what requirements engineers try to achieve with their work and with the systems they specify. The results show the priorities that are set for requirements engineering work. The answers to RQ3, finally, tell us what requirements engineering techniques matter most because they are associated with success more than other techniques do.

We built the questionnaire by first basing it on requirements engineering state of the art [11, 12] and then adjusting it based on suggestions from practitioners with broad overview on the software industry. A focus group with experienced practitioners evaluated adequacy, coverage, and understandability of the questionnaire. We then tested and further improved the form by letting respondents fill it in and give feedback in interviews.

To know who was answering, the questionnaire asked respondents to characterize their most recent software project. To answer RQ1, the questionnaire asked multiple-choice questions about requirements-related inquiry, specification, and management techniques in the characterized project. To answer RQ2, it asked multiple-choice questions about the goals of requirements engineering in the project and of the specified product. To answer RQ3, it asked questions about the requirements engineering success. Free-text areas allowed expanding or qualifying the answers.

The theoretical population of the survey was all software projects that were recent when the survey was administered in 2012. The sampling frame was the industrial contacts of our partners in academia and industry. To increase the reach of the survey we encouraged subjects to recommend the questionnaire to their own contacts.

Six hundred twenty-five respondents, about 10 % of the invited persons, answered the online questionnaire. Filtering for completeness and plausibility reduced the data to 419 valid answers. This number of answers makes this requirements engineering survey by far the largest ever published. The obtained number of samples allowed describing requirements engineering practice with a margin of error smaller than ±5 % for 95 % confidence.

We answered the research questions with statistical analysis. Descriptive statistics of proportions were used for answering RQ1 and RQ2. The difference of proportions test, a variation of the independent samples *t* test, was used for answering RQ3. To control the accumulation of type I error, Holm's step-down method [77] was used to prune the *t* test results for statistical significance. Wilcoxon's rank-sum test, finally, allowed us to explore an additional angle to answer RQ3, whether the number of requirements engineering practices that are used in a software projects would correlate with success.

2.4 Requirements Engineering Practice and Success

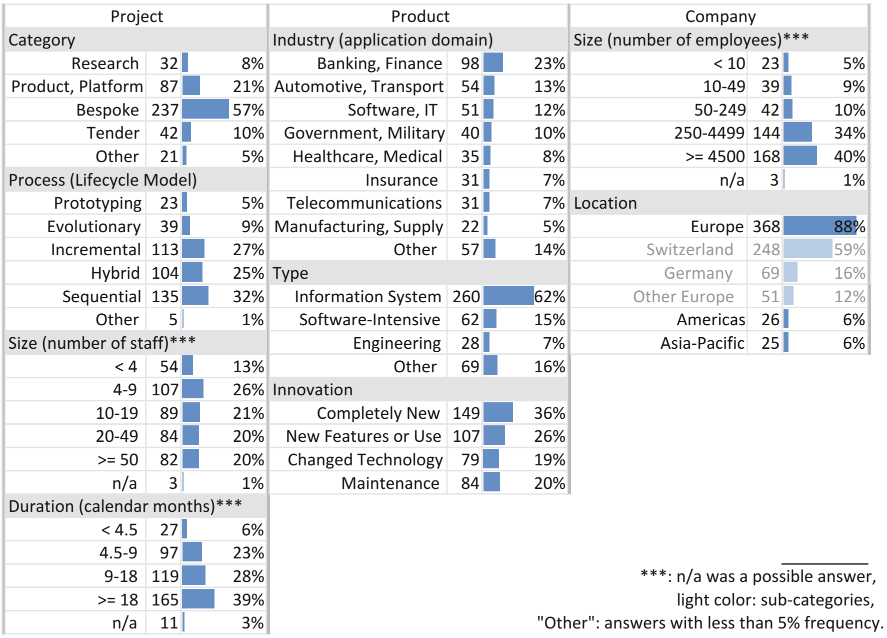
2.4.1 Responding Projects

A diverse mix of software projects answered the survey. Figure 2.1 gives an overview of the answering projects, the kinds of software products they developed, and the companies they belonged to.

Many projects were performed at large companies in Switzerland and developed information systems. This distribution is consistent with the Switzerland-oriented contact networks we used for soliciting responses. The key employer in this country is the service sector with IT departments that produce information systems.

A wide spread of industries were addressed with the developed products. Thirty-five responses, 8 % of all responses, were given by projects that developed products for health care. Thus the results reflect practice across industries and are not specific to one of them, for example health care. Product novelty was relatively evenly spread.

A majority of the projects were bespoke and developed tailor-made solutions. The projects used a sequential, incremental, or hybrid development process. Only few did research or used a process like the Spiral model that is designed for experimentation. The long duration of the projects may be explained by the prolonged relationship that IT departments have with the business units they support. The same relationship can also explain the bespoke nature of the projects. Information systems developed for business units are used by a predetermined set of users that can be actively involved into the requirements engineering process.



Project		
Category		
Research	32	8%
Product, Platform	87	21%
Bespoke	237	57%
Tender	42	10%
Other	21	5%
Process (Lifecycle Model)		
Prototyping	23	5%
Evolutionary	39	9%
Incremental	113	27%
Hybrid	104	25%
Sequential	135	32%
Other	5	1%
Size (number of staff)* **		
< 4	54	13%
4-9	107	26%
10-19	89	21%
20-49	84	20%
>= 50	82	20%
n/a	3	1%
Duration (calendar months)* **		
< 4.5	27	6%
4.5-9	97	23%
9-18	119	28%
>= 18	165	39%
n/a	11	3%

Product		
Industry (application domain)		
Banking, Finance	98	23%
Automotive, Transport	54	13%
Software, IT	51	12%
Government, Military	40	10%
Healthcare, Medical	35	8%
Insurance	31	7%
Telecommunications	31	7%
Manufacturing, Supply	22	5%
Other	57	14%
Type		
Information System	260	62%
Software-Intensive	62	15%
Engineering	28	7%
Other	69	16%
Innovation		
Completely New	149	36%
New Features or Use	107	26%
Changed Technology	79	19%
Maintenance	84	20%

Company		
Size (number of employees)* **		
< 10	23	5%
10-49	39	9%
50-249	42	10%
250-4499	144	34%
>= 4500	168	40%
n/a	3	1%
Location		
Europe	368	88%
Switzerland	248	59%
Germany	69	16%
Other Europe	51	12%
Americas	26	6%
Asia-Pacific	25	6%

***: n/a was a possible answer,
light color: sub-categories,
"Other": answers with less than 5% frequency.

Fig. 2.1 Demography of projects that responded to the survey

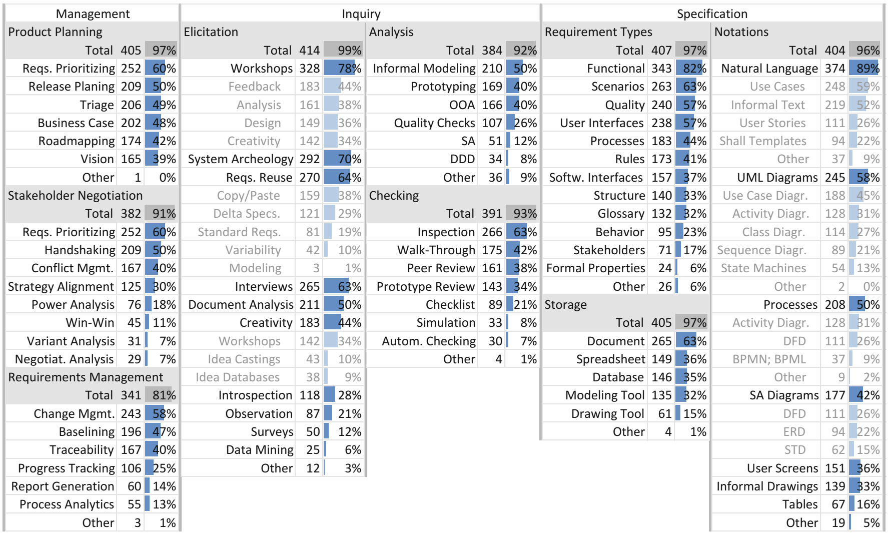
2.4.2 *Common Practice*

Our data shows that requirements engineering was widely established. However, there was not one way of doing requirements engineering. While only few of the techniques are employed by almost all projects, e.g., workshops, many of the techniques are used by some of the projects only. This result indicates a wide variety of how requirements engineering is done. Figure 2.2 gives an overview of how frequently each requirements engineering practice was used.

Almost every project elicited requirements. The projects tended to do with stakeholder workshops, by studying existing systems, or by reusing specifications. Workshops dominated requirements elicitation practice. Only few projects used techniques like observation, ethnography, surveys, or data mining. These techniques are thus used in special situations only.

Almost every project planned the product to be developed, often by prioritizing requirements. Often a mix of planning techniques was used. No technique was dominant.

Almost every project analyzed requirements. Often a mix of informal modeling, prototyping, and object-oriented analysis was used. No analysis technique was dominant. Historically important techniques like structured analysis, quality function deployment, and decision trees or specialized techniques such as domain-driven development were uncommon.



Management		
Product Planning		
Total	405	97%
Reqs. Prioritizing	252	60%
Release Planing	209	50%
Triage	206	49%
Business Case	202	48%
Roadmapping	174	42%
Vision	165	39%
Other	1	0%
Stakeholder Negotiation		
Total	382	91%
Reqs. Prioritizing	252	60%
Handshaking	209	50%
Conflict Mgmt.	167	40%
Strategy Alignment	125	30%
Power Analysis	76	18%
Win-Win	45	11%
Variant Analysis	31	7%
Negotiat. Analysis	29	7%
Requirements Management		
Total	341	81%
Change Mgmt.	243	58%
Baselining	196	47%
Traceability	167	40%
Progress Tracking	106	25%
Report Generation	60	14%
Process Analytics	55	13%
Other	3	1%

Inquiry					
Elicitation			Analysis		
Total	414	99%	Total	384	92%
Workshops	328	78%	Informal Modeling	210	50%
Feedback	183	44%	Prototyping	169	40%
Analysis	161	38%	OOA	166	40%
Design	149	36%	Quality Checks	107	26%
Creativity	142	34%	SA	51	12%
System Archeology	292	70%	DDD	34	8%
Reqs. Reuse	270	64%	Other	36	9%
Copy/Paste	159	38%	Checking		
Delta Specs.	121	29%	Total	391	93%
Standard Reqs.	81	19%	Inspection	266	63%
Variability	42	10%	Walk-Through	175	42%
Modeling	3	1%	Peer Review	161	38%
Interviews	265	63%	Prototype Review	143	34%
Document Analysis	211	50%	Checklist	89	21%
Creativity	183	44%	Simulation	33	8%
Workshops	142	34%	Autom. Checking	30	7%
Idea Castings	43	10%	Other	4	1%
Idea Databases	38	9%			
Introspection	118	28%			
Observation	87	21%			
Surveys	50	12%			
Data Mining	25	6%			
Other	12	3%			

Specification					
Requirement Types			Notations		
Total	407	97%	Total	404	96%
Functional	343	82%	Natural Language	374	89%
Scenarios	263	63%	Use Cases	248	59%
Quality	240	57%	Informal Text	219	52%
User Interfaces	238	57%	User Stories	111	26%
Processes	183	44%	Shall Templates	94	22%
Rules	173	41%	Other	37	9%
Softw. Interfaces	157	37%	UML Diagrams	245	58%
Structure	140	33%	Use Case Diagr.	188	45%
Glossary	132	32%	Activity Diagr.	128	31%
Behavior	95	23%	Class Diagr.	114	27%
Stakeholders	71	17%	Sequence Diagr.	89	21%
Formal Properties	24	6%	State Machines	54	13%
Other	26	6%	Other	2	0%
Storage			Processes	208	50%
Total	405	97%	Activity Diagr.	128	31%
Document	265	63%	DFD	111	26%
Spreadsheet	149	36%	BPMN; BPML	37	9%
Database	146	35%	Other	9	2%
Modeling Tool	135	32%	SA Diagrams	177	42%
Drawing Tool	61	15%	DFD	111	26%
Other	4	1%	ERD	94	22%
			STD	62	15%
			User Screens	151	36%
			Informal Drawings	139	33%
			Tables	67	16%
			Other	19	5%

Multiple answers were possible, light color: sub-categories, "Other": answers with less than 5% frequency

Fig. 2.2 Common requirements engineering practice

Almost every project specified requirements. A majority specified functionality, quality, use scenarios, and user interfaces of intended solutions. Functional requirements dominated. Concepts commonly used for formal reasoning, such as agents, goals, and formal properties, were rare. For specifying the requirements, natural language dominated as the notation. Natural language was often complemented with UML diagrams. The use of other diagram types, user screens, and informal drawings varied. Formal-logic and goal-oriented languages like i* or KAOS were almost never used.

The frequency of notations that match requirements analysis techniques was inconsistent with requirements analysis practice. Object-oriented and structured diagrams were much more common than the use of corresponding analysis techniques. User screens were much less frequently documented than prototypes created. Formal specification languages were used as rarely as the corresponding formal methodology.

Almost every project stored requirements. Requirements documents were the most common type of storage. The use of spreadsheets, requirements databases, and modeling tools varied. Drawing tools, wikis, and cards for capturing requirements backlogs were uncommon.

Almost every project checked requirements. Projects tended to prefer manual requirements checking, preferably with rigorous inspections. Simulation and automated formal checking were uncommon.

Almost every project negotiated requirements. To reach an agreement on requirements, most common was requirements prioritization. Uncommon were analytical techniques such as power, variant, and negotiation analysis, and advanced techniques such as win-win negotiations.

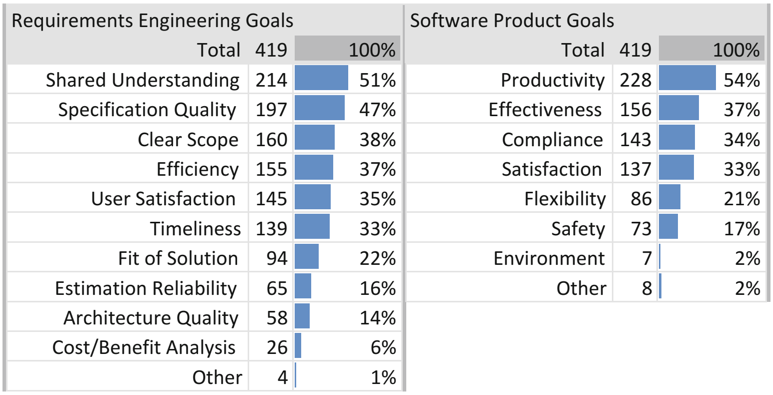
Four out of five projects managed the requirements. This means at the same time that one out of five projects did not use the requirements once they were inquired. Requirements management tended to focus on the handling of requirements. Most common was change management. Requirements were rarely used for analyzing project progress, for reporting, or for measuring the development process.

Overall, the large variety of techniques indicates that there was no one-size-fits-all in requirements engineering practice. Still, there are a few practices that could be seen in a large majority of projects. These include the use workshops to discuss requirements with stakeholders, the specification of functional requirements, and the use of natural language for specification. Among the established methodologies, object-oriented analysis and specification appears to be widely adopted, although not dominating. The older counter-parts, for example structured analysis, were much less important in comparison. Extremely rare were formal techniques. Even-though they are widely researched, they have hardly found their way into current practice.

2.4.3 *Requirements Engineering Success*

The data from the responding projects showed that there was no dominant way of judging requirements engineering success. Figure 2.3 gives an overview.

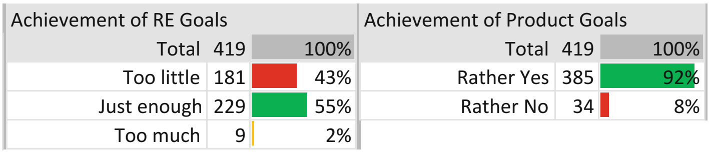
The most important requirements engineering goals were shared understanding between the project team and its stakeholders and good quality of the requirements specification. These two objectives of requirements engineering were often complemented with the need for a clear scope for the development, for using little time and



Requirements Engineering Goals		
Total	419	100%
Shared Understanding	214	51%
Specification Quality	197	47%
Clear Scope	160	38%
Efficiency	155	37%
User Satisfaction	145	35%
Timeliness	139	33%
Fit of Solution	94	22%
Estimation Reliability	65	16%
Architecture Quality	58	14%
Cost/Benefit Analysis	26	6%
Other	4	1%

Software Product Goals		
Total	419	100%
Productivity	228	54%
Effectiveness	156	37%
Compliance	143	34%
Satisfaction	137	33%
Flexibility	86	21%
Safety	73	17%
Environment	7	2%
Other	8	2%

Fig. 2.3 Success factors for requirements engineering process and outcome



Achievement of RE Goals		
Total	419	100%
Too little	181	43%
Just enough	229	55%
Too much	9	2%

Achievement of Product Goals		
Total	419	100%
Rather Yes	385	92%
Rather No	34	8%

Fig. 2.4 Requirements engineering success

resources for requirements engineering, for satisfying the users, and for delivering the requirements engineering work results in time.

The most common goal pursued by the software products that were specified with the requirements was productivity improvement. This goal was complemented by a variety of goals that included effectiveness, e.g., to enable users to do things they could not do before, compliance with laws and regulations, and satisfaction of users and stakeholders with the product. Important societal topics, like environmental or societal challenges, were rarely considered to be a goal of the software product.

Figure 2.4 shows how many projects were successful and how many have not been successful when judged according to the criteria summarized in Fig. 2.3. A bit more than half of the projects judged that they fulfilled the requirements engineering goals. A bit less than half judged they did too little. Almost none stated they would have done too much. While positive and negative satisfaction with requirements engineering were rather balanced, product goal achievement was a sharp success. About nine out of ten of the specified products were judged to be a success. Only few were considered failures.

These success rates appear to contradict the success rates identified in other studies. In comparison, Standish presented 32 % project success rate in 2009 by taking into consideration scope, time, and budget adherence [5]. The staggering success rate of 92 % for product goal achievement we observed thus says that while the project may have been problematic, the outcome of the project was not. Also, 55 % satisfaction with the requirements engineering experience is significantly larger than then 32 % project success rate. This may indicate that requirements engineering practice had matured and was less problematic than other disciplines.

2.4.4 Success-Correlating Practice

To identify effective requirements engineering practice we correlated technique use with requirements engineering success. The result of this analysis indicates the techniques that are used in projects with successful requirements engineering significantly more often than in projects that did not meet requirements engineering goals or produced products that did not achieve their goals. Whether practice use leads to success or whether good projects select these practices cannot be concluded from these results and needs to be investigated in future research.

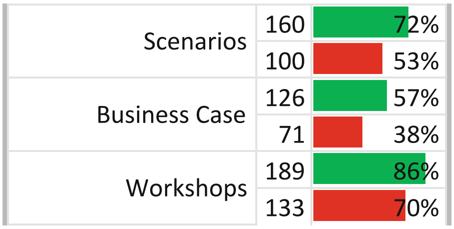


Fig. 2.5 Techniques that correlated with requirements engineering success (*upper rows*: successes, *lower rows*: failures)

Our survey data showed 221 projects with successful requirements engineering and 189 failures according to our success criteria. Only three techniques correlated with requirements engineering success with $p < 0.05$ significance after pruning the results with Holm's step-down method to remove false positives. None of the other techniques correlated significantly with success, and no technique correlated negatively. Figure 2.5 gives an overview.

Scenarios are exemplary sequences of system usage [55]. In requirements engineering, they are used to describe concrete stories of how users and external systems interact with the system under consideration to achieve goals that are of value to the user. Scenarios make the functionality of the system concrete and thus enable users to judge whether they feel to be able to use the system meaningfully and whether they like it. Scenarios also allow capturing interaction design knowledge from user experience experts. A common format used to document scenarios is the use case template [78].

Business cases are used to document predicted financial results and other business consequences for one or multiple alternative ways of how a product is built, deployed, and maintained [41]. The business case planning work and results that are obtained with it are determinant for selecting what is in the product scope and what not and for evaluating whether a chosen scope is attractive for the customer of the project. The understanding of a business case allows to stop work on a product that does not make sense or to re-scope the product to make it more attractive.

Workshops create an efficient, controlled, and dynamic setting for quickly eliciting, prioritizing, and agreeing on requirements [29]. The discussion of requirements by the critical stakeholders makes a requirements workshop to be one of the most efficient techniques to perform inquiry and to achieve shared understanding. No other technique allows exposure and resolution of conflicts between stakeholders so efficiently. The same applies for discovery and resolution of misunderstandings.

We also studied whether the number of techniques used and the number of requirement types documented in a project correlates with requirements engineering success. Figure 2.6 shows the distributions with box plots.

According to the Wilcoxon's rank-sum test, successful projects use a significantly larger number of requirements engineering techniques and specify a significantly larger number of requirement types than unsuccessful ones.

Again, the causes for these correlations should be investigated with future research. A hypothesis that should be tested is whether there is a large variety of project context that require more techniques to be used. The observed large variety

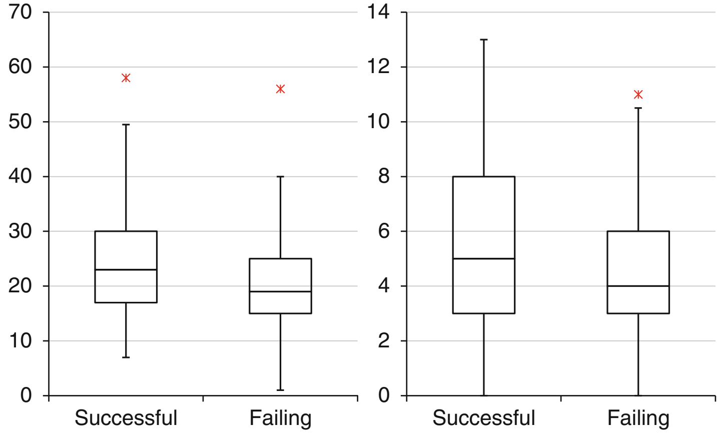


Fig. 2.6 Number of requirements engineering techniques (*left*) and number of requirements types (*right*) used in projects with successful, respectively failing requirements engineering

of requirements engineering techniques used across projects would support this claim. Another hypothesis may be that the experience of a requirements engineer may lead to both greater use of techniques and greater likelihood of project success. Experienced requirements engineers will use more techniques and specify more types of requirements than less experienced requirements engineers. At the same moment they are the better guarantors of requirements engineering success.

2.5 Discussion

2.5.1 Contribution

This chapter has provided an overview of common and best practice in requirements engineering. Based on answers from 419 projects, it has shown how frequently the many requirements engineering were used and which of these techniques correlated with requirements engineering success. The presented frequencies of requirements engineering technique use extend the results from earlier surveys [7, 8] with an updated set of practices. For example, prior surveys did not evaluate whether common requirements engineering research such as i* or KAOS had been transferred to practice. Our results showed that these two techniques were not. The presented results also extend prior research with a number of samples that is by far larger than any previous requirements engineering survey was based on. We could indicate state-of-practice with a level of accuracy that previous surveys could not.

Earlier surveys did not have enough data to correlate requirements engineering practice with success, thus gave others fertile grounds to claim that no technique would lead to requirements engineering success [6]. The results shown in this chapter

Fig. 2.7 Requirements workshop for exploring scenarios and business case (participants shown in photograph from *left* to *right*: development manager, project leader, requirements engineer, domain expert, domain expert, quality of experience expert, lead engineer, user, developer)

provide counter-evidence. While we could not demonstrate sufficiency or necessity of any requirements engineering practice, we could show that there are indeed a few requirements engineering techniques that are associated with significantly higher success rates. The relevant techniques were scenarios, business cases, and workshops. Interestingly, the three techniques we identified were not the same that were used by companies that valued requirements engineering [9]. The latter included prototyping, data flow diagrams, and techniques like quality function deployment and decision trees that are hardly used according to our data. To understand why the identified techniques correlate with success, while others do not, future research should investigate what causes the correlations.

The presented results are relevant for education and practice. They enable comparison of own practice and competences with common practice. Requirements engineers should be well versed in the use of the techniques that are used frequently. According to our data, almost any requirements engineer will be requested to perform workshops and specify functional requirements in natural language. The larger number of techniques used and requirements types specified in successful requirements engineering also shows that a requirements engineer should know many practices, rather than few. Comparison of the frequencies of the various requirements engineering techniques may be used to guide the development of needed competencies. For example, object-oriented analysis techniques should be learned before structured analysis techniques because the former are much more common in real-world projects than the latter.

The presented results can be used for advice about effective practice. If the three success-correlating techniques cause requirements engineering success, they should be used whenever possible. Accepting this assumption, we started utilizing requirements workshops systematically. We integrated scenarios into the workshops by role-playing and discussing the intended system use with the participating real-world stakeholders. We integrated business case by discussing whether and why each of the product's features is needed and by estimating feasibility and cost. Figure 2.7 shows a photograph from one of these workshops, which involved real stakeholders, users, project members, and experts.

2.5.2 Threats to Validity

Any research results should be considered with caution because none is free from threats to validity. We discuss here the threats to conclusion, internal, construct, and external validity that were suggested for empirical software engineering research by Wohlin et al. [79].

Conclusion validity is concerned with the relationship between treatment and outcome. The here presented results are based on a survey with a large-enough number of samples that were analyzed by keeping the accumulation of the probability of false positives in mind. As a result we can claim that there is a statistically significant relationship between the identified three practices scenarios, business case, and workshops and the success of requirements engineering.

Internal validity is concerned with the causal relationship between treatment and outcome. The survey does not tell us anything about such causal relationships. We have no evidence that it is the scenarios, the business case, or the workshops that caused success, but just know that their frequency of use is different significantly between successful and failing projects. Further research is needed to understand what the right causal relationship is.

Construct validity is concerned with the relation between theory and observation. Potential problems may be misunderstanding of questions and answers and inadequate operationalization of the concepts we evaluated. We used survey pretests with experts and with selected respondents, thus have reduced the likelihood of misunderstanding the questionnaire. Also, we filtered responses that were incomplete or unreasonable based on the free-text answers that were given. The potential problem of inadequate operationalization was addressed by basing our definition on prior research of requirements engineering success and by adding to the original success measurement the impact of requirements engineering: whether the specified system achieved its goals. The study thus reasonably reflects the constructs were intended to evaluate.

An important threat to validity of this survey concerns external validity. Alike other surveys in requirements and software engineering, we used nonprobability sampling to reach respondents. Hence, the frequencies we presented are valid for populations of projects that have a profile similar to the one presented in Fig. 2.1. As requirements engineering practice varies a lot across projects, other populations may have different frequencies and other conclusions about practice use may need to be drawn. Also availability and knowledge of techniques evolves over time and affect the frequency distribution of practice use. For example, 30 years ago Structured Analysis would have been much more frequent than Object-Oriented Analysis. We conjecture, however, that change in the frequency of technique use does not affect the effectiveness of the techniques. The causes that make business cases, scenarios, and workshops effective are hardly affected by such changes. Thus we expect the results about practice effectiveness to be replicable also in populations other than the studied one.

2.5.3 Need for Research

The large variations of the requirements engineering techniques used by the software projects indicate that technique use may depend on context. Such context dependency was shown in other related domains as well [80]. For software built for digital health, the context dependency may imply shifts in the frequency of practice use. Also, the regulated nature of the health care industry may imply that additional techniques, such as document analysis and reuse of requirements may correlate with requirements engineering success. The former may help in the identification of compliance requirements [81], the latter in how to specify a system that is compliant.

Another venue of research is the construction of models that explain how requirements engineering success can be achieved. For example, control theory of goal-oriented systems was used to explain how stakeholder needs and development intentions can be aligned in a one-to-one situation between a product manager and an architect [82] and successfully validated [13]. However, other approaches may be needed to achieve socio-technical alignment of a software solutions and technologies in large-scale. Once validated in large-scale, these models help us to develop and justify causes and effects behind the correlations that are observed in surveys such as the one presented here. They are also the basis to design techniques that help practitioners to be successful.

2.6 Summary and Conclusions

This chapter has presented the results of a large-scale survey of requirements engineering practice. The results were obtained by analyzing the answers of 419 projects. Many of the answering projects developed of information systems in a bespoke manner with known stakeholders. The projects implemented agile, waterfall, and hybrid development processes. A wide variety of industries were addressed by the developed software products. Two hundred twenty-one projects did requirements engineering successfully, 189 not.

Almost all projects elicited, planned, analyzed, specified, checked, and managed requirements. The most common techniques were stakeholder workshops and the specification of functional requirements with natural language. For most of the remaining techniques can be concluded that requirements engineering practice varies across the software projects. Formal techniques were extremely rare, even if they were researched intensively.

Only three techniques correlated with requirements engineering success: scenarios of system use, business cases, and stakeholder workshops. We recommend that all projects implement these practices. In addition we observed that projects with successful requirements engineering used more requirements engineering techniques and specified more types of requirements than unsuccessful ones. We thus recommend the use of experienced requirements engineers that are able to identify and apply the right technique for the many situations that may be encountered in a real-world project.

The obtained results extend previous surveys that were substantially smaller with updated frequencies of requirements engineering technique use and with the really new insights into what practices are correlate with success. Further research should look at specific project constellations, for example at projects that target digital health, and at building theories for what can be done to achieve requirements engineering success.

References

1. Standish Group International (1995) The CHAOS report. Standish Group International, Inc.
2. Hassenzahl M, Beu A, Burmester M (2001) Engineering Joy. IEEE Software 18(1):70–76
3. Gorschek T, Wohlin C (2006) Requirements abstraction model. Requirements Eng 11(1): 79–101
4. Glinz M, Fricker S (2013) On shared understanding in software engineering, Software engineering 2012. Aachen, Germany
5. Eveleens L, Verhoef C (2010) The rise and fall of the chaos report figures. IEEE Software 27(1):30–36
6. Davis A, Zowghi D (2006) Good requirements practices are neither necessary nor sufficient. Requirements Eng 11(1):1–3
7. Neill C, Laplante P (2003) Requirements engineering: the state of the practice. IEEE Software 20(6):40–45
8. Paech B, Koenig T, Borner L, Aurum A (2005) An analysis of empirical requirements engineering survey data. In: Aurum A, Wohlin C (eds) Engineering and managing software requirements. Springer, New York, pp 427–452
9. Rouibah K, Al-Rafee S (2009) Requirements engineering elicitation methods: a Kuwaiti empirical study about familiarity, usage and perceived value. Inform Manag Comput Security 17(3):192–217
10. Potts C, Takahashi K, Antón AI (1994) Inquiry-based requirements analysis. IEEE Software 11(2):21–32
11. Cheng B, Atlee J (2007) Research directions in requirements engineering. Future of software engineering (FOSE'07). Washington, DC, USA
12. Pohl K, Rupp C (2011) requirements engineering fundamentals: a study guide for the certified professional for requirements engineering exam—foundation level—IREB compliant. Rocky Nook Computing
13. Fricker S, Glinz M (2010) Comparison of requirements hand-off, analysis, and negotiation: case study. 18th IEEE international requirements engineering conference (RE'10). Sydney, Australia
14. Glinz M, Fricker S (2014) On shared understanding in software engineering: an essay. Computer Science - Research and Development. doi: 10.1007/s00450-014-0256-x. See also: http://link.springer.com/article/10.1007/s00450-014-0256-x
15. Hickey A, Davis A (2004) A unified model of requirements elicitation. J Manag Inform Syst 20(4):65–84
16. Zowghi D, Coulin C (2005) Requirements elicitation: a survey of techniques, approaches, and tools. In: Aurum A, Wohlin C (eds) Engineering and managing software requirements. Springer, Berlin
17. Hickey A, Davis A (2003) Elicitation technique selection: how do experts do it? 11th IEEE international requirements engineering conference. Monterey Beach, CA, USA

18. Davis A, Dieste O, Hickey A, Juristo N, Moreno A (2006) Effectiveness of requirements elicitation techniques: empirical results derived from a systematic review. 14th IEEE international requirements engineering conference (RE'06). Minneapolis, MN, USA
19. Dieste O, Juristo N, Shull F (2008) Understanding the customer: what do we know about requirements elicitation? IEEE Software 25(2):11–13
20. Pérez-Castillo R, Garciía-Rodríguez de Guzmán I, Piattini M (2011) Business process archeology using MARBLE. Inform Software Technol 53(10):1023–1044
21. Maiden N, Gizikis A, Robertson S (2004) provoking creativity: imagine what your requirements could be like. IEEE Software 21(5):68–75
22. Gorschek T, Fricker S, Palm K (2010) A lightweight innovation process for software-intensive product development. IEEE Software 27(1):37–45
23. Cleland-Huang J, Mobasher B (2008). Using data mining and recommender systems to scale up the requirements process. 16th IEEE international requirements engineering conference (RE'08). Barcelona, Spain
24. Alvarez R, Urla J (2002) Tell me a good story: using narrative analysis to examine information requirements interviews during an ERP implementation. Data Base Adv Inform Syst 33(1):38–52
25. Vermersch P (2009) Describing the practice of introspection. J Conscious Stud 16(10–12):20–57
26. Beyer H, Holtzblatt K (1995) Apprenticing with the customer. Commun ACM 38(5):45–52
27. Ng L, Barfield W, Mannering F (1995) A survey-based methodology to determine information requirements for advanced traveler information systems. Transport Res C Emerg Technol 2:113–127
28. Lam W, McDermid J, Vickers A (1997) Ten steps towards systematic requirements reuse. Requirements Eng 2(2):102–113
29. Gottesdiener E (2002) Requirements by collaboration: workshops for defining needs. Addison-Wesley Professional
30. Mylopoulos J, Chung L, Yu E (1999) From object-oriented to goal-oriented requirements analysis. Commun ACM 42(1):31–37
31. van de Weerd I, Brinkkemper S, Nieuwenhuis R, Versendaal J, Bijlsma L (2006) Towards a reference framework for software product management. 14th IEEE international requirements engineering conference (RE'06). Minneapolis, MN, USA
32. Martin RC, Meinik G (2008) Tests and requirements, requirements and tests: a möbius strip. IEEE Software 25(1):54–59
33. Danevas P, Garva G (2012) Domain driven development and feature driven development for development of decision support systems. 18th international conference on information and software technologies (ICIST 2012). Kaunas, Lithuania
34. Holtmann J, Meyer J, von Detten M (2011). Automatic validation and correction of formalized, textual requirements. IEEE fourth international conference on software testing, verification and validation workshops (ICSTW 2011). Berlin, Germany
35. Glinz M (2010) Very lightweight requirements modeling. 18th IEEE international requirements engineering conference (RE'10). Sydney, Australia
36. Arlow J, Neustadt I (2005) UML 2 and the unified process: practical object-oriented analysis and design. Addison-Wesley Pearson Education, NJ, USA See also: http://www.google.com/books?hl=en&lr=&id=Fme5TXzP0VgC&oi=fnd&pg=PT2&dq=UML+2+and+the+unified+process:+practical+object-oriented+analysis+and+design&ots=QnSaJAvKYu&sig=U_9uW2ctUpo2T13NBOcxWDt5BkA
37. Rettig M (1994) Prototyping for tiny fingers. Commun ACM 37(4):21–27
38. Chung L, Nixon B, Yu E, Mylopoulos J (2000) Non-functional requirements in software engineering. Kluwer Academic Publishers, Boston
39. Ross D (1977) Structured analysis (SA): a language for communicating ideas. IEEE Trans Software Eng 3(1):16–34
40. DeMarco, T. (1979). Structured Analysis and System Specification, Yourdon Press.
41. Schmidt M (2002) The business case guide. Solution Matrix, Boston

42. Achimugu P, Selamat A, Ibrahim R, Mahrin MNR (2014) A systematic literature review of software requirements prioritization research. Inform Software Technol 56(6):568–585
43. Svahnberg M, Gorschek T, Feldt R, Torkar R, Bin Saleem S, Shafique MU (2010) A systematic review on strategic release planning models. Inform Software Technol 3:237–248
44. Phaal R, Farrukh C, Probert D (2003) Technology roadmapping—a planning framework for evolution and revolution. Technol Forecast Soc Change 71:5–26
45. Fricker S, Schumacher S (2012) Release planning with feature trees: industrial case. Requirements engineering: foundations for software quality (RefsQ 2012). Essen, Germany
46. Davis A (2005) Just enough requirements management. Dorset House Publishing, New York
47. McGrath ME (2001) Product strategy for high technology companies: accelerating your business to web speed. McGraw-Hill, New York
48. Whittle J, Schumann J (2000) Generating statechart designs from scenarios. IEEE international conference on software engineering (ICSE 2000). Limerick, Ireland
49. Berard B, Bidoit M, Finkel A, Laroussinie F, Petit A, Petrucci L, Schnoebelen P (2010) Systems and software verification: model-checking techniques and tools. Springer, Berlin
50. IEEE (1990) IEEE standard glossary of software engineering terminology 610.12-1990
51. Myers B (1989) User-interface tools: introduction and survey. IEEE Software 6(1):15–23
52. Chung J-Y, Lin K-J, Mathieu R (2003) Web services computing: advancing software interoperability. IEEE Comput 36(10):35–37
53. Melão N, Pidd M (2000) A conceptual framework for understanding business processes and business process modelling. Inform Syst J 10(2):105–129
54. ISO/IEC (2010) Systems and software quality requirements and evaluation, ISO/IEC. ISO/IEC FDIS 25010
55. Alexander I, Maiden N (2005) Scenarios, stories, use cases: through the systems development life-cycle. Wiley, Hoboken
56. Alexander I, Robertson S (2004) Understanding project sociology by modeling stakeholders. IEEE Software 21(1):23–27
57. van Lamsweerde A (2001) Goal-oriented requirements engineering: a guided tour. 5th IEEE international symposium on requirements engineering (RE'01). Toronto, Canada
58. Denger C, Berry D, Kamsties E (2003) Higher quality requirements specifications through natural language patterns. IEEE international conference on software: science, technology and engineering (SwSTE'03). Herzelia, Israel
59. Dwarakanath A, Ramnani R, Sengupta S (2013) Automatic extraction of glossary terms from natural language requirements. 21st IEEE international requirements engineering conference (RE'13). Rio de Janeiro, Brazil
60. Bajec M, Krisper M (2005) A methodology and tool support for managing business rules in organisations. Inform Syst 30(6):423–443
61. Easterbrook S, Lutz R, Covington R, Kelly J, Ampo Y, Hamilton D (1998) Experiences using lightweight formal methods for requirements modeling. IEEE Trans Software Eng 24(1):1–11
62. Porter A, Votta L, Basili V (1995) Comparing detection methods for software requirements inspections—replicated experiment. IEEE Trans Software Eng 21(6):563–575
63. Glinz M, Seybold C, Meier S (2007) Simulation-driven creation, validation and evolution of behavioral requirements models. Dagstuhl-workshop MBEES: Modellbasierte Entwiclung eingebetteter Systeme III (MBEES 2007). Braunschweig, Germany
64. Fricker S (2009) Pragmatic requirements communication: the handshaking approach. Shaker, Germany
65. Fricker S, Gorschek T, Byman C, Schmidle A (2010) Handshaking with implementation proposals: negotiating requirements understanding. IEEE Software 27(2):72–80
66. Raiffa H (2007) Negotiation analysis: the science and art of collaborative decision making. Harvard University Press, Cambridge
67. Milne A, Maiden N (2012) Power and politics in requirements engineering: embracing the dark side? Requirements Eng 17(2):83–98
68. Schobbens P-Y, Heymans P, Trigaux J-C, Bontemps Y (2007) Generic semantics of feature diagrams. Comput Networks 51(2):456–479

69. Boehm B, Grünbacher P, Briggs R (2001) Developing groupware for requirements negotiation: lessons learned. IEEE Software 18(3):46–55
70. Conradi R, Westfechtel B (1998) Version models for software configuration management. ACM Comput Surv 30(2):232–282
71. Kobayashi A, Maekawa M (2001) Need-based requirements change management. 8th annual IEEE international conference and workshop on the engineering of computer based systems (ECBS 2001). Washington, DC, USA
72. Petersen K, Wohlin C (2010) Measuring the flow in lean software development. Software Pract Experience 41(9):975–996
73. Kniberg H, Skarin M (2010) Kanban and scrum—making the most of both. lulu.com
74. Cleland-Huang J, Settimi R, Romanova E, Berenbach B, Clark S (2007) Best practices for automated traceability. Computer 40(6):27–35
75. El Emam K, Madhavji N (1985) A field study of requirements engineering practices in information systems development. 2nd IEEE international symposium on requirements engineering (RE'95). York, England
76. Rea L, Parker R (2005) Designing and conducting survey research: a comprehensive guide. Jossey-Bass, San Francisco
77. Holm S (1979) A simple sequential rejective multiple test procedure. Scand J Stat 6(2):65–70
78. Cockburn A (2001) Writing effective use cases. Addison-Wesley Professional, Boston
79. Wohlin C, Runeson P, Host M, Ohlsson C, Regnell B, Wesslén A (2000) Experimentation in software engineering: an introduction. Springer, Berlin
80. Khurum M, Fricker S, Gorschek T (2014) The contextual nature of innovation—an empirical investigation of three software intensive products. Inform Software Technol. doi:10.1016/j.infsof.2014.06.010. See also: http://www.sciencedirect.com/science/article/pii/S0950584914001499
81. Thuemmler C, Fricker S, Mival O, Benyon D, Buchanan W, Paulin A, Fiedler M, Koops B-J, Kosta E, Grottland A, Schneider A, Jell T, Gavras A, Barros M, Magedanz T, Cousin P, Ispas I, Petrakis E (2013) Norms and standards in modular medical architectures. IEEE 15th international conference on e-health networking, applications and services (Healthcom 2013). Lisbon, Portugal
82. Fricker S, Gorschek T, Glinz M (2008). Goal-oriented requirements communication in new product development. International workshop on software product management (IWSPM 2008). Barcelona, Spain

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 11 111/4, 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

Chapter 4
Ethical Issues in Digital Health

Ai Keow Lim Jumelle and Ioana Ispas

Abstract With advancement in technology and breakthrough in Internet connectivity, digital health technologies have penetrated all aspects of our lives. Hospital information systems (HIS), electronic health records (EHR), ePrescriptions, eReferrals, personal digital assistant (PDA), wearable devices, telemedicine and telemonitoring are some of the growing number of digital health technologies that help to facilitate the storage, transmission and retrieval of medical data; improve communication between patients and healthcare professionals; monitor biological and physiological parameters, and provide remote health and social care services. However, technology-centred health and social care services also raise a number questions involving what sort of ethical conduct should be expected by developers of the digital health technologies. Issues such as privacy, security, equality, accessibility and data protection are some ethical concerns posed by new technologies in the health and social care sector. One challenge for those involved in the design, development and deployment of digital health technologies and applications will be to determine what constitutes ethics and what codes of ethics to adhere to. There are many frameworks and guidelines established to deal with the impact of digital technologies on our societies. Requirement engineers need to adhere to the relevant codes of ethics to address important engineering ethics-related software requirements.

4.1 Introduction

With advancement in technology and breakthrough in Internet connectivity, digital health technologies have penetrated all aspects of our lives. Hospital information systems (HIS), electronic health records (EHR), ePrescriptions, eReferrals, personal digital assistant (PDA), wearable devices, telemedicine and telemonitoring

A.K.L. Jumelle (✉)
Institute for Informatics & Digital Innovation,
Edinburgh Napier University, Edinburgh, UK
e-mail: a.limjumelle@napier.ac.uk

I. Ispas
Ministry of National Education, Bucharest, Romania
e-mail: ioana.ispas@ancs.ro

S.A. Fricker et al. (eds.), *Requirements Engineering for Digital Health*,
DOI 10.1007/978-3-319-09798-5_4

are some of the growing number of digital health technologies that help to facilitate the storage, transmission and retrieval of medical data; improve communication between patients and healthcare professionals; monitor biological and physiological parameters, and provide remote health and social care services. However, technology-centred health and social care services also raise a number questions involving what sort of ethical conduct should be expected by developers of the digital health technologies. Issues such as privacy, security, equality, accessibility and data protection are some ethical concerns posed by new technologies in the health and social care sector. One challenge for those involved in the design, development and deployment of digital health technologies and applications will be to determine what constitutes ethics and what codes of ethics to adhere to. There are many frameworks and guidelines established to deal with the impact of digital technologies on our societies. Requirement engineers need to adhere to the relevant codes of ethics to address important engineering ethics-related software requirements.

This chapter sought to discuss some ethical issues and their implications, including identifying ethical frameworks that could be used in assessing ethical challenges in the design, development and deployment of digital health technologies. This chapter classifies the frameworks and guidelines according to different purposes. This chapter also draws upon an example to explain the application of one of the recognised ethical frameworks in the real world in order to help developers and engineers understand and address the ethical issues and the fundamental of ethical principles pertaining to the field of digital health. An ethical matrix is used as a tool to illuminate the diverse requirement of a use case, part of the seven early trials in the healthcare domain of the Future Internet Social Technological Alignment Research [1] project.

The second section of this chapter provides a brief overview of digital health. The third section describes the ethical implications of digital health technologies. The fourth section reviews the ethical framework and guidelines relating to the field of digital health. The fifth section discusses the ethical matrix. The sixth section presents a step-by-step approach to understanding and adhering to the codes of ethics in digital health. The final section summarises and concludes by suggesting that while codes of ethics should keep pace with evolving technologies, requirements engineer should also adhere to the ethical guidelines for engineering ethics-related software requirements.

4.2 Overview of Digital Health

Paul Sonnier, a social entrepreneur and founder of the digital health group on LinkedIn, defines digital health as

> …… the convergence of the digital and genetics revolutions with health and healthcare – is empowering us to better track, manage, and improve our own and our family's health. It's also helping to reduce inefficiencies in healthcare delivery, improve access, reduce costs, increase quality, and make medicine more personalized and precise. [2]

There are many drivers of change within the health and social care services sector. The population of elderly people aged 65 and above is growing due to improved medical science. The increased number of chronic diseases among the elderly population has resulted in greater consumption of health and social care services [3–5]. With the growing numbers of elderly having multi-morbidities and needing integrated long-term health and social care, there is a shift from reactive to proactive personalised and predictive health management focusing on behavioural changes and prevention of illness and disease. Multi-morbidity is defined as the coexistence of two or more chronic diseases in an individual [6, 7]. The declining fertility rates have also resulted in a change in family structure and labour force participation rate. It is becoming more common for the elderly population to receive informal care from family and relatives. Some elderly, on the other hand, do not live in the same household as their children. These elderly self-manage everyday minor ailments such as coughs and colds and long-term conditions themselves or receive assistance from healthcare workers. The declining workforce participation may cause a shortfall in the health professionals and informal workforce [8, 9].

Over the next decades, digital health technologies will increasingly replace the traditional face-to-face interactions between patients and physicians [10]. In the new era of digital health, the patient's role is changing from compliance with healthcare professional's advice to active self-management of health, wellness and disease. Patients and their carers set health goals and take active role and responsibility in the self-management of health and disease such as tracking weight, diet and exercise and self-monitoring of blood pressure. As patient groups are demanding a more significant role in the self-management of health, wellness and disease, the EHR is regarded as an important instrument to enhance patient empowerment and improving quality of care [11]. The ability to gain access and manage their personal health data provides patients better insight into their medical history and health conditions.

Health interventions can be personalised and tailored to reach people at home and in rural areas in real time. Web-based patient treatment can bring convenience as it reduces the time and cost to travel to the physician's office. Patients do not have to wait for an appointment to ask questions. Patients can make online appointments, renew prescriptions and receive test results. Patients can also get information delivered to their email inbox. Research has shown that paediatric palliative care communication can be improved using digital health technologies [12]. A meta-analysis review also supports the use of behavioural digital health interventions in the treatment or prevention of paediatric physical health problems that involve health behaviours such as obesity and smoking [13].

Thousands of websites disseminate health and medical information. Patients can find and compare health and wellness information such as the costs of non-emergency surgical procedures at different hospitals. Based on a survey conducted by Pew Research Centre [14], 72 % of Internet users in the USA searched online for health information and about 3–4 % of Internet users have posted their experiences with healthcare service providers or treatments within the past year. Well-informed patients can become expert patients who are capable of facilitating and enriching the interactions with their physicians [15]. Online peer-to-peer support forums enable patients to communicate and share their experiences, health concerns and information with other patients in real time anonymously.

In light of the rising demand for health and social care from the aging population, the changing demographics, the effectiveness of digital healthcare interventions in the paediatric population and the escalating healthcare expenditure, many believe that digital health technologies have the potential to meet the increasing demand for and the changing nature of health and social care services and improve health outcomes and quality of life. Nevertheless, there are significant ethical implications emerging from the use of digital health technologies.

4.3 Ethical Implications of Digital Health Technologies

Before discussing the ethical implications, we first need to define what "ethics" and "medical internet ethics" are. Ethics refers to "norms of conduct that distinguish between acceptable and unacceptable behaviour" [16].

> Medical Internet Ethics is an emerging interdisciplinary field that considers the implications of medical knowledge utilized via the Internet, and attempts to determine the ethical guidelines under which ethical participants will practice online medicine or therapy, conduct online research, engage in medical e-commerce, and contribute to medical websites. [17]

Even though most societies use law to enforce widely accepted moral standards and ethical and legal rules use similar concepts, ethics and law are not the same [16]. Ethical norms tend to be broader and more informal than law [16].

While digital health technologies and applications have the potential to address health problems, improve health outcomes and lower healthcare costs, the increased access to health and social care services and information also brings new concerns. These concerns include privacy, confidentiality and security of personal healthcare data, equality of access to healthcare services, accountability, effectiveness of patient empowerment and quality of healthcare information. The following sections provide a brief description of each ethical concern.

4.3.1 Privacy, Confidentiality and Security of Personal Healthcare Data

Privacy, confidentiality and security are the primary concern regarding the high volume of personal healthcare data flowing between different devices and different healthcare information systems. The type of media that flow between devices and systems is also expanding. Patients' records may include diagnostic images, video, audio and email. While anonymising data such as removing names and addresses offers a certain degree of protection, EHR pose the risks of security and the potential of re-identifying patients through unauthorised methods. Therefore, not all patients are ready to accept blanket consent to automatically share their personal healthcare information in the EHR [11]. Personal healthcare information may also be collected indirectly without prior knowledge and consent using online survey and embedded cookies and web beacons [18]. It is important that organisations apply the same criteria that govern the storage, use and transfer of paper healthcare records to electronic records. Healthcare providers and developers have the responsibility to gather data meticulously and to keep personal health records with appropriate levels of privacy protections and to seek patients' consent regarding what data will be collected, who has access to which information in the EHR, and releasing information to a third party.

4.3.2 Equality of Access to Healthcare Services

Another ethical issue related to digital health technologies and applications is equality of access to healthcare services among economically disadvantaged and vulnerable populations [19]. Those economically disadvantaged may have low levels of education, have low health literacy, may reside in rural area, may be from racial and ethnic minority groups or may be immigrants. Vulnerable patients include those who have complex and/or multiple chronic diseases, disabled, mentally ill and very young children. Some people do not have the financial means, technical knowledge or desire to use the Internet, communication devices and digital health technologies and applications. Digital health technologies and applications should be included as part of the universal healthcare services to improve the health of the population.

4.3.3 Accountability

As healthcare organisations increase their reliance on digital health technologies, the importance of accountability cannot be ignored. Digital health has altered the traditional relationship between patients and physicians in terms of distance and time of communication and how medical care is delivered. When physicians communicate with their patients in a technologically mediated manner, there is a danger of lack of understanding between them [11]. Moreover, when basic diagnostic skills such as observation cannot be performed accurately online, physicians may miss important information to provide the right diagnosis [15]. There is a need to address the questions of whether virtual physicians need to apply for licence to practice medicine online and will they be held accountable to provide the same standard of care as in-person medical office visit. Informed consent, privacy, security, equity and protection of vulnerable populations are some challenges and ethical issues that have emerged as a result of the new form of patient-physician relationship. Forming a genuine patient-physician relationship will require knowledge and skills [20].

4.3.4 Effectiveness of Patient Empowerment

Even though empowerment may be a major benefit of digital health, an overemphasis may be harmful to patients [21]. Underachievement of health outcomes may lead to dissatisfaction, insecurity and depression. Dedding et al. [15] highlight how the shifting of task and responsibilities to patients as consumers can become an added responsibilities and burden in daily life. Some patients may resist their new role, not have the resources or may lack support in developing empowerment [20]. The risk of non-adherence and likelihood of patients modifying their treatment plans should not be ignored. Patients should be placed at the centre of the empowering process when encouraging patients to take more active responsibility in the self-management of their health with support from digital health technologies [21].

While assistive technologies such as tracking devices offer empowerment and other potential benefits to elderly people and their carers such as increased independence, it raises important ethical issues such as loss of privacy and liberty. Many elderly in need of care suffer from multi-morbidity and some may have significant physical dependency and mental impairment. This raises the question as to what extent can we balance benefits and risks when assessing the suitability, quality and effectiveness of digital health technologies. The appropriateness of digital health technologies depends on whether the technology replaces more restrictive measures, becomes a restriction on autonomy and erodes the privacy and confidentiality of health information [22].

4.3.5 Quality of Healthcare Information

Some major obstacles of online health and medical information include the overwhelming quantity of information and the poor quality of online health information [23]. A website that is accessed through a domain name using an international intergovernmental organisation's name such as WHO may not necessarily lead users to the official website of the organisation. Moreover, many people do not have the knowledge and skills to assess the trustworthiness and credentials of the information. Some people do not have the medical knowledge to assess whether information about therapies and interventions is scientifically proven. Many digital health applications provide social connections. Even though social connections allow patients to feel supported, there is an increased risk of invasion of patient privacy. Patients are reluctant or unwilling to share information and their feelings with others online due to the lack of reasonable and appropriate security measures. Another potential problem with online forums is the quality and trustworthiness of information shared [20]. In addition, the increasing complexity and variety of digital health technologies and applications can be overwhelming for people. People can become increasingly confused of who and which digital health technologies to trust for advice and support.

Although the health sector is highly regulated at the national level, enforcing national laws governing online behaviour is difficult [24]. While law constitutes a minimum standard for conduct and reflects a society's unique perspective, ethics embodies more than the law [11, 25]. National laws that stipulate that a code of ethics should respect the relevant laws would commit the fallacy of nationality [25]. It is dangerous if it is ethically acceptable to avoid specific and onerous ethical injunctions solely by moving medical research to another state where such injunctions are not in force because there are no similar laws [25]. Establishing ethical codes, standards and guidelines may help to overcome some of the difficulties and challenges posed by these digital health technologies and online health information.

4.4 Ethical Frameworks and Guidelines in Digital Health

Recent trends in machine-to-machine (M2M) technology and communication have been deployed across a wide variety of health and social care services. However, there has been no comprehensive ethical regulatory framework to address all aspects of digital health relationships, behaviours, interactions and communications, including people to people (P2P), machine to people (M2P) and machine to machine (M2M). Ethicists and researchers as well as some international and non-profit organisations such as the World Health Organisation (WHO), the European Union (EU) and the Health on the Net Foundation have taken the initiative to develop and promote digital health ethical standards, codes of conduct, accreditation systems and quality criteria. The objectives of these ethical frameworks and guidelines are to establish a code of conduct for websites, educate consumer and content providers, establish some form of accountability and self-regulation and ensure that content provider comply with the codes of ethics established in the field of digital health. Table 4.1 displays these ethical frameworks and guidelines, which will be further discussed in the sections below. Requirement engineers can use Table 4.1 as a checklist to review requirement specifications for digital health systems.

4.4.1 The Four Principles of Biomedical Ethics [26]

The Four Principles approach developed by Beauchamp and Childress [26] is one of the widely used frameworks for medical ethics issues and clinical setting to govern the delivery of care. Even though the Four Principles are not specifically designed for digital health [35], its guiding principles are considered to be universal and can be used to assess the ethical impact of digital health technologies and applications. The Four Principles are as follows:

(a) Respect for autonomy: Respecting the decision-making capacities of patients and research subjects and enable them to make independent, informed choices.

(b) Non-maleficence: A duty to protect patients to avoid inflicting and imposing harm.

Table 4.1 Ethical frameworks and guidelines for digital health

Framework and guideline	Description	Professional codes of ethics	Personal healthcare information/database	Content	Certification	Domain names
Four principles of biomedical ethics [26]	Clinical setting and moral action guides in medical ethics	✓	✓	✓		
Code of informatics ethics [27]	Ethical guidelines for health informatics professionals	✓	✓	✓		
Ethics for eHealth [18]	Management of ethics for digital health		✓			
eHealth standardisation and Internet domain names [24]	eHealth standardisation, interoperability and Internet domain					✓
WMA declaration on ethical considerations regarding health databases [28]	Ethical guidelines for health databases		✓			
EU Directive 2002/58/EC on the processing of personal data and the protection of privacy in the electronic communications sector [29]	Core set of quality criteria for health-related websites			✓		
eHealth code of ethics [30]	Ethical codes for online health information about health products and services			✓		
HoNcode [23]	Guide for medical and health websites			✓	✓	
The Information Standard [31]	Certification of electronic health and social care information			✓	✓	
DISCERN Genetics Tool [32]	An appraisal tool that enables information providers, patients and their carers to judge the quality of online information available to the public regarding genetic tests			✓		
Khresmoi Medical Information Analysis and Retrieval [33]	Project aims at improving access of health information for the general public, medical doctors and radiologists			✓		
Medline Plus [34]	Guide to health web surfing			✓		

(c) Beneficence: Balancing benefits of treatment against the risks and costs and act in a way that benefits the patient.
(d) Justice: Distribution of a fair share of benefits, risks and costs. This principle addresses between other aspects also the issue of inequalities in access to healthcare.

4.4.2 Code of Informatics Ethics [27]

Kluge [27] proposes a code of informatics ethics that focuses on health informatics professional. They include the principle of information-privacy and disposition, principle of openness, principle of access, principle of legitimate infringement, principle of least intrusive alternative, principle of accountability and principle of security. The duties consist of subject-centred duties, duties towards the healthcare professionals, duties towards society and duties towards health informatics professionals and the profession [27]. Kluge [25] argues that the protection of electronic healthcare data must focus solely on fundamental ethical principles because these are applied to the types of situations in which electronic healthcare data are generated, used and disposed of.

4.4.3 Ethics for eHealth [18]

Maddox [18] discusses four approaches in managing ethics for eHealth. The first approach is based on permission with regard to the release of information. This approach recognises the individual as the agent to grant or deny access to personal health information. The second approach is paternalistic whereby the decision of what constitutes reasonable access and best interest of patients lies with the healthcare professionals or information system managers. The third approach is an umbrella release to access of personal health information on a strict need-to-know basis. The final approach is establishing common rules to protect confidential information and facilitate sharing of information.

4.4.4 eHealth Standardisation and Internet Domain Names [24]

Given the increased potential for the unauthorised and misleading registration and use by third parties of intergovernmental names and acronyms, delegates attending the World Health Assembly resolution on eHealth standardisation and Internet domain names approved a resolution on eHealth standardisation and interoperability in 2013 [24]. Under this resolution, health-related, global, top-level domain names, including ".health", should be operated in a way that protects public health and is consistent with global health objectives. Names and acronyms of intergovernmental organisations, including WHO, should also be protected from abusive registrations in the Internet Domain Name System [24].

4.4.5 WMA Declaration on Ethical Considerations Regarding Health Databases [28]

In 2002, the declaration on ethical considerations regarding health databases was adopted by the World Medical Association (WMA) General Assembly. The declaration specifies that the right to privacy entitles an individual to exercise control over the use and disclosure of personal physical and mental health information. All physicians are responsible and accountable for the collection, storage, transfer and use of personal health information [28]. Patients should be informed of what information is held on health databases and the purposes of which their information may be used. Patients' consent should be obtained if their information on a database may be disclosed to third party [28]. In exceptional cases where personal health information is included in a database to comply with national law or ethical approval has been given by a specially appointed ethical review committee, patients do not have the right to object but should be informed about the potential uses of their health information [28].

4.4.6 EU Directive 2002/58/EC on the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector [29]

After widespread consultation with representatives from the industry, medical and patient interest groups, member states' governments, the field of health information ethics, international organisation and non-governmental organisation, the European Commission published a communication outlining a core set of quality criteria for health-related websites in 2002. The six quality criteria are as follows:

(a) Transparency and honesty: clear communication of the name, physical address and electronic address of the website site managers, the purpose and objective of the site, its target audience and transparency of all sources of funding.
(b) Authority: a clear statement of sources for information, the date of publication and the name and credentials of human/institutional providers of information.
(c) Privacy and data protection: privacy and data protection policy for processing personal data in accordance with EU community data protection legislation (Directives 95/46/EC and 2002/58/EC, refer to Chap. 3 on Laws and Regulations for Digital Health).
(d) Updating of information: clear and regular updating of the site, with the details of updates clearly displayed on the relevant page, regular checking of relevance of information.

(e) Accountability: a method for obtaining customer feedback, and appropriate oversight responsibility such as a named quality compliance officer, responsible partnering with trustworthy individuals and organisation, a clearly defined editorial policy.
(f) Accessibility: attention to guidelines on physical accessibility as well as general findability, searchability, readability and usability.

4.4.7 eHealth Code of Ethics [30]

During the summit organised by the Internet Healthcare Coalition and hosted by the World Health Organisation/Pan-American Health Organisation (WHO/PAHO) in 2000, a panel of experts from all over the world produced an eHealth code of ethics to ensure that people realise the potential and understand the risks of using the Internet in self-managing their own health as well as those under their care. This eHealth code of ethics focuses mainly on health information about health products and health services (e.g. personal medical care or advice and management of medical records) provided by organisations and individuals via the Internet.

There are eight guiding principles of the eHealth code of ethics:

(a) Candour: Information and services provided should be credible and trustworthy. Any conflict of interest (such as financial gain) should be declared.
(b) Honesty: All content should be truthfully presented.
(c) Quality: Health information should be accurate, up to date, easy to understand and in language appropriate for intended users. Personalised medical care or advice should be given by qualified practitioner.
(d) Informed consent: Users have the right to be informed when, what and how personal data may be collected, used or shared.
(e) Privacy: Users' privacy should be protected by removing any personal identifiers.
(f) Professionalism in online healthcare: Doctors, nurses, pharmacists, therapists and other healthcare professionals should abide the ethical codes that govern their professionals
(g) Responsible partnering: Sponsors, partners and other affiliates should abide by applicable law and uphold the same ethical standards
(h) Accountability: Users have the opportunity and confidence to raise any concerns and provide feedback with the content provider.

4.4.8 HoNcode [23]

The Health on the Net Foundation [23] is a non-governmental organisation set up in 1995 and is internationally known for the establishment of its code of ethical conduct, the HoNcode. The HoNcode provides a guide for medical and health websites to engage in responsible dissemination of objective, relevant and trustworthy health information for patients, professionals and the general public. The eight principles of

HoNcode are authority, complementarity, confidentiality, attribution, justifiability, transparency, financial disclosure and advertising [23]. Medical and health websites who are certified under the HoNcode and found to respect all the eight ethical principles are allowed to display the accreditation label onto their websites. Regular monitoring is conducted to ensure compliance and detect violations of the HoNcode.

4.4.9 The Information Standard [31]

Another organisation that provides certification to support people using health and social care information is the Information Standard, an independent certification programme commissioned by the National Health Service (NHS) England, the UK. Organisations are allowed to display the Information Standard accreditation label on their information material if they meet the stringent requirements of producing good-quality printed, electronic and scripted health and social care information and that those pieces of information are from reliable and trustworthy source [31].

4.4.10 DISCERN Genetics Tool [32]

DISCERN Genetics Project was funded by the British Library and the National Health Service Executive Anglia and Oxford Research and Development Programme and run jointly by the University of Oxford Division of Public Health and Primary Health Care, the Help for Health Trust and Buckinghamshire Health Authority [32]. The aim of the project is to develop an appraisal tool that enables information providers, patients and their carers to judge the quality of written information available to the public on genetic tests [36]. Users do not need specialist knowledge to use DISCERN Genetics to judge the quality of a publication in print and on the Internet and verbal communication such as consultations and telephone advice [36].

4.4.11 Khresmoi Medical Information Analysis and Retrieval [33]

Khresmoi Medical Information Analysis and Retrieval [33] is an ongoing European Seventh Framework Programme (FP7) research project aimed at improving access of health information for members of the general public, medical doctors and radiologists. Khresmoi will create a multilingual multimodal search and access system for biomedical information and documents by combining data and knowledge from multiple sources, including text (online journals and books, trusted websites) and image (images from journals and Picture Archiving and Communication Systems (PACS) in hospital radiology departments).

4.4.12 Medline Plus [34]

Medline Plus, the USA's National Institute of Health's Web, proposes a guide to healthy web surfing. When evaluating the quality of health information on websites, users should consider the source, focus on quality, get a second opinion if site makes false and unsubstantiated health claims, rely on medical research evidence and not opinion, look for the latest information, check the sources of funding for the sites and ensure that site has a privacy policy [34].

It is important to highlight that codes of ethics and professional guides are voluntary standards. There is a need to establish a universally accepted medical information standards for the nomenclature, coding and structure to achieve uniformity of definition and meaning of terminology [37]. Nonetheless, requirement engineer should adhere to the frameworks and guidelines to fulfil engineering ethics-related software requirements.

4.5 Ethical Tools: An Example of the Ethical Matrix

Ethical tools can be used to explore the types of ethical challenges in digital health, identify different interpretations of ethics relating to digital health and resolve conflicts in a multidisciplinary team. Ethical tools are required to be "comprehensive, transparent and democratic procedures" such as an expert workshop that enables relevant ethical issues to be addressed during public consultation and decisions to be reflected upon systematically [35]. An ethical matrix can be used during the workshop to reach sound consensus regarding various aspects of ethical acceptability of new digital health technologies. In this section, we review the ethical matrix and discuss a real-life example to understand how the ethical matrix is being applied in the context of digital health.

4.5.1 Ethical Matrix

The ethical matrix based on Beauchamp and Childress' [26] three principles, namely autonomy, well-being (beneficence) and justice, was developed by Professor Ben Mepham, Director of the Centre for Applied Bioethics at the University of Nottingham and a member of the Food Ethics Council in 1994 [38]. The ethical matrix acts as a framework to help individuals and groups to work through differences in perspectives and weigh each concern against the others. Although the ethical matrix was initially designed to facilitate ethical discussion among those who are interested in novel biotechnologies, the matrix may be used by researchers in the field of digital health to assess ethical and cultural understanding in multidisciplinary and cross-cultural research, assess the potential ethical implications of development of individual technologies, investigate different legal norms and discuss and reach consensus on contradictory aspects.

4.5.2 Future Internet Social and Technological Alignment Research (FI-STAR)

The Future Internet Social Technological Alignment Research project (FI-STAR) is a FP7 project and is concerned with the validation of future Internet technology developed under earlier FI-PPP projects and involves seven early trials in the healthcare domain. The FI-STAR consortium attended an experimental ethical matrix workshop to review ethical dimensions of the use cases' technologies involved. The purpose of this workshop which took place in Crete in September 2013 was to assess differences in ethical perceptions of the stakeholders and use case participants, the impact of national and European regulations and cross-cultural implications and the outcomes of the applied technology.

Table 4.2 presents the ethical matrix for the Basque Country Use Case [40]. The Basque Country Use Case looks at providing telecare for mental disorders and it targets specifically bipolar disorder, a chronic disorder with an aggregate lifetime prevalence of 0.4–2.4 % [39]. The proposed FI-STAR eHealth solution focuses on patients' empowerment by providing specific telecare capabilities and multi-channel interactions between the patients and the public regional health service provider in Spain (OSAKIDETZA), using their preferred available end-user devices and communication channels. The use case aims to provide a new service based on advanced communication channels to treat, monitor and support people with mental disorders and their caregivers. The main actors involved in this use case are (1) treatment participants: patients aged 18–50 years and their caregivers/relatives, and (2) professionals: psychiatric personnel (i.e. psychiatrics, psychologists and psychiatric nurses) and call centre nurses. In order to evaluate the impact of the proposed solution in the provision of telecare services, OSAKIDETZA will set up the validation phase as a single-blind, randomised clinical trial. While telecare has the potential to improve the confidence of patients with mental disorders and free up time for carers, there is a need to ensure that patients' rights and privacy are respected. The use of telecare service should not restrict a patient's autonomy. There is also a need to balance between patient's safety and privacy.

4.6 Key Steps for Understanding the Codes of Ethics in Digital Health

As discussed above, the ethical matrix can be used to easily identify ethical concerns that appear to be common among a heterogeneous group of collaborators and that might influence the design and eventual implementation of the technologies. Here we propose a series of steps that requirement engineers can use to enhance their understanding and adherence to the codes of ethics in digital health.

Step 1. Learn what the relevant codes of ethics in digital health are using Table 4.1 as a guide.

Table 4.2 Ethical matrix for FI-STAR's Basque country use case

	Beneficence	Non-maleficence	Autonomy	Justice
Hospital	• Efficient use of the health system resources (by reducing hospitalisation relapses, emergency admissions and visits to primary and secondary care). • Prevent emergency overuse. • Reduce the waiting list.	• FI-STAR eHealth solution can help to audit access to patients' health information. • Verify a patient's identity.	• Personalised treatment for patients according to the disease, functionality and social habits of the patients. • Scalability of systems (the performance of the system is independent on the number of patients).	• This use case facilitates the implementation of the data protection law. • With correct treatments, complaints from patients or their relatives can be reduced.
IT specialists	• Expertise in the implementation of scalability systems. • Improve monitoring and traceability of systems. • Flexibility in future application development.	• FI-STAR eHealth solution can help to audit access to patients' health information. • Confirm a patient's identity. • Protection against massive cyber attacks.	• Allow system planning implementation based on periodic data monitoring.	• Quicker answer to possible requirement about traceability of information.
Medical doctors	• Fewer face-to-face appointments. • More contacts with the patients. • More and quick information about the clinical state of patients. • Automatic alarms about the clinical state of the patients. • A systematic program of psychological treatment.	• More details about health measurements on a daily basis. • Conduct treatments in a friendly environment. Patients can use the telecare system to initiate a response in case of emergency. • This system reduces loss of information that might result from a change in the clinical team or other treatment elements.	• Less time is spent in each treatment because explanations of the illness are recorded in videos. • The cognitive therapy task can be analysed at a convenient time and during subsequent consultation with the patients. • This system allows easier graphical study of the evolution of the symptomatology of the patients.	• FI-STAR eHealth solution improves security to meet justice requirements (all records of treatment and mails are stored in secured system). • If the treatment provided for these patients is effective, it can be extended to the target population that might benefit from the treatment.
Industry	• An aim of the psychoeducation modules is to improve the medication adherence.	• Standardisation of the biometrical devices.	• Guidelines for defining and establishing interoperability requirements.	

(continued)

Table 4.2 (continued)

	Beneficence	Non-maleficence	Autonomy	Justice
Patients	● Improvement in treatment. ● Improvement of patients' knowledge of their illness. ● Prevention of manic or depressive relapse. ● Improvement of functionality. ● Better management of anxiety and problem solving. ● Knowledge about the pharmacological treatment and the possible side effects.	● Help to empower patients in their disease treatment through active participation.	● Patients can access their clinical information and know who and when their records have been accessed. ● Patient can access the psychoeducation modules at their own convenience. ● Patients can complete and send the task, at their own convenience, to the clinician. ● Patients have an off-line possibility to contact the clinician.	
Families and relatives	● Reduce family burden. ● Accurate information about the disease is being sent to patient's relatives so that they can participate in some psychoeducational sessions about the bipolar disorder.	● Help to ease worries about the disease and the situation of patient's family. ● Learn how to manage some situations or problems that could occur.	● Relatives can contact the clinician by internal email. ● Improvement in patient's condition.	
Scientific community	● Develop a digital protocol repository for several diseases. ● Possibility of analysing the effectiveness of the system.			

(© IEEE 2014)

Step 2. Conduct a workshop to consult and find out the kinds of ethical principles and values held by different key stakeholders. Understand the desired outcomes they would want from the new technology.

Step 3. Decide which ethical frameworks and guidelines are relevant to the situation. If there is a need to modify existing or formulate new codes of ethics, assess the possible harmful consequences.

Step 4. Resolve any differences in ethical dilemmas (for example, tension between different codes of ethics and reach a consensus).

It is important to note that these steps are not exhaustive and may not apply in all situations. Requirement engineers should use ethical judgement to act in a manner which is most consistent with the spirit of their codes of ethics and professional practices, given the circumstances [41].

4.7 Conclusion

People are increasingly using digital health technologies to proactively manage their health, wellness and disease. Digital health technologies present the potential to revolutionise health and social care experience and improve quality and health outcomes. However, ethical concerns such as privacy, confidentiality and security of personal healthcare data, equality of access to healthcare services, accountability, effectiveness of patient empowerment and quantity and quality of online health information should be recognised and properly addressed. Initiatives have been taken by ethicists, researchers, international and non-profit organisations such as WHO, WMA and Health on the Net Foundation to establish frameworks and guidelines as a basis for educating content providers and users and as guidelines for resolving ethical dilemmas.

This chapter has explained some ethical principles and described how they may be addressed with a software system. The chapter has contributed with an overview of typical requirements that a digital health system should fulfil and has shown with an example how they may be implemented. The results provide the requirements engineer with a guideline for engineering ethics-related software requirements and represent a checklist to review requirements specifications for digital health systems.

References

1. FI-STAR (2013) Future internet social technological alignment in healthcare. https://www.fi-star.eu/home.html. Accessed on 15 June, 2014
2. Sonnier P (2014) Story of digital health. http://storyofdigitalhealth.com/. Accessed on June 1, 2014
3. Rechel B, Doyle Y, Grundy E, McKee M (2009) How can health systems respond to population ageing? Policy brief 10. World Health Organisation. http://www.euro.who.int/__data/assets/pdf_file/0004/64966/E92560.pdf. Accessed on June 14, 2014
4. World Health Organisation (2005) Preventing chronic disease: a vital investment. http://www.who.int/chp/chronic_disease_report/contents/foreword.pdf?ua=1. Accessed on June 14, 2014

5. World Health Organisation (2011) Global health and aging. http://www.nia.nih.gov/sites/default/files/global_health_and_aging.pdf. Accessed on June 14, 2014
6. Boyd CM, Fortin M (2010) Future of multimorbidity research: how should understanding of multimorbidity inform health system design? Public Health Reviews 2010(32):451–74
7. Mercer SW, Smith SM, Wyke S, O'Dowd T, Watta GCM (2009) Multimorbidity in primary care: developing the research agenda. Family Practice 16(2):79–80. doi:10.1093/fampra/cmp020
8. Ambient Assisted Living (2014) Care for the future: an ageing society faces an increasing need for care, how will ICT contribute to sustainable solutions? Active and Assisted Living Programme. Challenge-led call for proposal 2014. http://www.aal-europe.eu/wp-content/uploads/2014/05/AAL-2014-call-text-20140526.pdf. Accessed on June 14, 2014
9. Stone RI, Wiener JM (2001) Who will care for us? Addressing the long-term care workforce crisis. U.S. Department of Health and Human Services. http://aspe.hhs.gov/daltcp/reports/ltcwf.htm. Accessed on June 14, 2014
10. Weiner JP (2012) Doctor-patient communication in the e-health era. Israel Journal of Health Policy Research 1:33. doi:10.1186/2045-4015-1-33
11. Reidl C, Wagner I, Rauhala M (2005) Examining ethical issues of IT in health care. Action for health. Institute of Technology Assessment & Design. Vienna University of Technology. http://www.sfu.ca/act4hlth/pub/working/Ethical-Issues.pdf. Accessed on June 6, 2014
12. Madhavan S, Sanders AE, Chou W-YS, Shuster A, Boone KW, Dente MA, Shad AT, Hesse BW (2011) Paediatric palliative care and eHealth: opportunities for patient-centred care. American Journal of Preventive Medicine 40(5 Suppl 2):S208–S216. doi:10.1016/j.amepre.2011.01.013
13. Cushing CC, Steele RG (2010) A meta-analytic review of eHealth interventions for paediatric health promotion and maintaining behaviours. Journal of Paediatric Psychology 35(9): 937–949
14. Pew Research Centre (2012) Health fact sheet. Pew research internet project. http://www.pewinternet.org/fact-sheets/health-fact-sheet/. Accessed on June 6, 2014
15. Dedding C, van Doorn R, Winkler L, Reis R (2011) How will e-health affect patient participation in the clinic? A review of e-health studies and the current evidence for changes in the relationship between medical professionals and patients. Social Science & Medicine 72(1): 49–53
16. Resnik DB (2011) What is ethics in research and why is it important? http://www.niehs.nih.gov/research/resources/bioethics/whatis/. Accessed on June 14, 2014
17. Dyer KA (2001) Ethical challenges of medicine and health on the Internet: a review. Journal of Medical Internet Research (JMIR) 3(2):e23. doi:10.2196/jmir.3.2.e23
18. Maddox P (November 21, 2002). Ethics column: ethics and the brave new world of e-health. Online Journal of Issues in Nursing 8(1): 6. www.nursingworld.org/MainMenuCategories/ANAMarketplace/ANAPeriodicals/OJIN/Columns/Ethics/Ethicsandehealth.aspx. Accessed on June 3, 2014
19. Oliver A, Mossialos E (2004) Equality of access to health care: outlining the foundations for action. Journal of Epidemiology Community Health 58:655–658. doi:10.1136/jech. 2003.017731
20. Townsend A, Adam P, Li LC, McDonald M, Backman CL (2013) Exploring eHealth ethics and multi-morbidity: protocol for an interview and focus group of patients and health care provider views and experiences of using digital media for health purposes. Journal of Medical Internet Research (JMIR) Research Protocol 2(2):e38
21. Alpay LL, Henkemans OB, Ottens W, Rövekamp TAJM, Dumay ACM (2010) E-health applications and services for patient empowerment: directions for best practices in the Netherlands. Telemedicine and e-Health 16(7):787–791
22. United Kingdom Alzheimer's Society (2014) Position statement on safer walking technology. http://www.alzheimers.org.uk/site/scripts/documents_info.php?documentID=579. Accessed on June 1, 2014
23. Health on the Net Foundation, HoNCode (2013) The commitment to reliable health and medical information on the internet. http://www.hon.ch/HONcode/Webmasters/Visitor/visitor.html. Accessed on June 2, 2014
24. World Health Organisation, WHO (2013) eHealth and health internet domain names. World Health Organisation Sixth-Sixth World Health Assembly, A66/26, Provision agenda item 17.5,

14 May 2013. http://apps.who.int/gb/ebwha/pdf_files/WHA66/A66_26-en.pdf?ua=1. Accessed on June 2, 2014

25. Kluge E-HW (2000) Professional codes for electronic HC record protection: ethical, legal and economic and structural issues. International Journal of Medical Informatics 60:85–96. doi:10.1016/S1386-5056(00)00107-6
26. Beauchamp TL, Childress JF (2001) Principles of biomedical ethics, 5th edn. Oxford University Press, New York, NY
27. Kluge E-HW (1998) Fostering a security culture: a model code of ethics for health information professionals. International Journal of Medical Informatics 49:105–110
28. World Medical Association, WMA (2002) WMA declaration on ethical considerations regarding health databases. The 53rd WMA General Assembly, Washington, DC, USA, October 2002. http://www.wma.net/en/30publications/10policies/d1/index.html. Accessed on June 2, 2014
29. European Commission (2002) Directive 2002/58/EC of the European parliament and of the council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications). http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002L0058&from=EN. Accessed on June 6, 2014
30. Internet Healthcare Coalition (2000) eHealth code of ethics. http://www.ihealthcoalition.org/ehealth-code-of-ethics/. Accessed on June 4, 2014
31. The Information Standard (2012) The information standard: frequently asked questions. http://www.theinformationstandard.org/about/faq?page=2&theme=highcontrast. Accessed on June 2, 2014
32. DISCERN (1999) DISCERN on the internet. http://www.discern.org.uk/hoti.php. Accessed on June 2, 2014
33. Khresmoi (2010) Khresmoi medical information analysis and retrieval. http://www.khresmoi.eu/. Accessed on June 2, 2014
34. Medline Plus (2012) MedlinePlus guide to healthy web surfing. U.S. National Library of Medicine and National Institute of Health. http://www.nlm.nih.gov/medlineplus/healthywebsurfing.html. Accessed on June 2, 2014
35. Wadhwa K, Wright D (2013) eHealth: frameworks for assessing ethical impacts. In: George C, Whitehouse D, Duquenoy P (eds) eHealth: legal, ethical and governance challenges. Springer, Berlin, pp 183–210
36. DISCERN Genetics (2005) Background: the DISCERN genetics tool. http://www.discern-genetics.org/quality_criteria_and_references.php. Accessed on June 2, 2014
37. Raghupathi W (1997) Health care information systems. Communications of the ACM 40(8):81–82
38. Food Ethics Council, United Kingdom (2013) Ethical matrix. http://www.foodethicscouncil.org/system/files/Ethical%20Matrix_1.pdf. Accessed on May 3, 2014
39. Merikangas KR, et al (2011) Prevalence and correlates of biopolar spectrum disorder in the World Mental Health Survey Initiative. Archives of General Psychiatry 68(3):241–251. doi:10.1001/archgenpsychiatry.2011.12
40. Lim Jumelle AK, Ispas I, Thuemmler C, Mival O, Kosta E, Casla P, Ruiz de Azúa S, González-Pinto A (2014) Ethical assessment in E-health. In: Proceedings of the IEEE HealthCom, Natal, 2014 (© IEEE 2014)
41. Association of Computing Machinery (2014) Software engineer code of ethics and professional practice. http://www.acm.org/about/se-code#full. Accessed on June 15, 2014

Chapter 5
Standards for Interoperability in Digital Health: Selection and Implementation in an eHealth Project

Karima Bourquard, Franck Le Gall, and Philippe Cousin

Abstract The complexity increase of healthcare processes together with wider adoption of eHealth systems imposes stringent consideration of interoperability across deployed services. Addressing this, standard organizations are proposing standards, sometime enforced through regulation, to develop interoperable eHealth services. Facing an increasingly important number of standards, industrial associations are building application-specific interoperability profiles identifying subset of standards relevant for the targeted applications. This chapter proposes an approach for eHealth service developers to efficiently capture interoperability requirements using these profiles and illustrate it through its application to a transnational project.

5.1 Introduction

The access to medical and social data is today one of the major challenges in eHealth and well-being areas. With the use of Internet by citizens including elderly people, the human behavior is starting to change and the expectation for better care and better access to medical data "at anytime and everywhere" is increasing very quickly. This expectation is also related to the empowerment and the awareness of the citizens and patients for their own illness. At the same time, healthcare processes are becoming more and more complex with the increase of the needs of medical and social skills and the decrease of such an expertise that can be found close to the patient. Within the four objectives defined by the European Commission in its 2012–2020 action plan for eHealth [1], the objective 2 is to "address issues currently impeding eHealth interoperability" by achieving wider interoperability in

K. Bourquard
IN-SYSTEM, Paris, France
e-mail: karima.bourquard@in-system.eu

F. Le Gall (✉) • P. Cousin
Easy Global Market, Nice, France
e-mail: franck.le-gall@eglobalmark.com; philippe.cousin@eglobalmark.com

S.A. Fricker et al. (eds.), *Requirements Engineering for Digital Health*,
DOI 10.1007/978-3-319-09798-5_5

eHealth services through an eHealth European Interoperability Framework (eEIF), looking at several interoperability layers.

Technical and syntactical interoperability as presented in the ETSI[1] four-layer interoperability model [2] is the prerequisite of the semantic interoperability. This layer ensures that appropriate protocols are in place to enable machine-to-machine communications (technical level) and that data can be exchanged (syntactical level). Definition of data structure, communication, and protocols is the condition for processing and exchanging data and is the basis of the standards and profiles. To ensure *organizational interoperability* in which healthcare providers are able to exchange clinical information within their business processes, the concepts and the activities shall be correctly interpreted and the meaning safeguarded. It means that at each level, semantic interoperability exists, providing the description of the concepts and ensuring their correct transformation using common "interpreters." *Semantic interoperability* is one of the challenges and the most difficult to achieve.

Semantic interoperability is used at all interoperability levels. At the technical level, semantic describes coding systems that are shared by two systems where the first one sends information that the second is able to accept, to understand and to further process. At the clinical level, *clinical terminologies* are used in order to describe clinical concepts related to the description of the diagnosis, the organs, the clinical activities, or any other clinical concepts that can be represented by a code and name or term.

Several standards organizations dedicated to eHealth have started to develop standards that answer the need of interoperability in order to enable seamless medical exchanges between healthcare systems. To operate between them, several levels of standards describing protocols, structured data, terminologies … are thus needed corresponding to different levels of interoperability, i.e., technical, semantic, and clinical levels.

To allow health solution providers to better deal with the large number of existing standards, the report of the Mandate M403:2007 [3] that was coordinated by the three European Standards Development Organisations (SDOs) CEN,[2] CENELEC,[3] and ETSI proposed the use case approach as the way to organize the process for eHealth interoperability standards taking up. The keystone of the proposed methodology is the definition of "intermediate level of interoperability building blocks" called *profiles* that maintain sufficient flexibility between projects and standards (Fig. 5.1). Profiles are based on a set of standards pieces such as DICOM, HL7, W3C, and security and provide precise specifications of how standards can be implemented to meet specific clinical needs or use cases. Use cases cover different domains such as radiology, pharmacy, laboratory, or EHR workflows. For example, the workflow of the order, schedule, imaging acquisition to the delivery of the radiology report, and the images from the prescriber to the radiologist in hospital is the

[1] European Telecommunications Standards Institute.

[2] European Committee of Normalisation.

[3] European Committee for Electrotechnical Standardization.

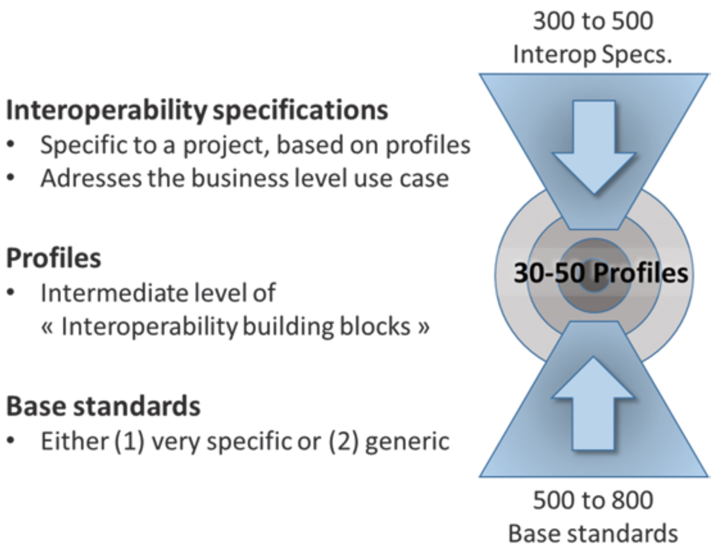

300 to 500
Interop Specs.
Interoperability specifications
• Specific to a project, based on profiles
• Adresses the business level use case
Profiles
• Intermediate level of
« Interoperability building blocks »
30-50 Profiles
Base standards
• Either (1) very specific or (2) generic
500 to 800
Base standards

Fig. 5.1 Importance to capitalize on profiles (source European Commission Mandate M403: 2007 [3])

workflow that the profile called IHE SWF (Scheduled Workflow) answers to this clinical needs.[4]

Section 5.3 presents a practical use of these profiles to identify standardization requirements when building a health-related application.

Industrial alliances, also called fora, have thus developed a methodology to optimize the selection of subsets of operational and robust standards, answering the specific business needs based on use case analysis. The relevance of the selected standards set (the profile) is validated through testing by the health solution providers in controlled environment before they are implemented by the healthcare solutions' providers (see Fig. 5.2).

Profiles are detailed implementation guides for developers and provide a common language for specifying integration needs expressed by clinicians and shared with vendors (use cases). They provide a clear understanding of how various sets of standards can be implemented altogether, merging for example part of HL7 for clinical needs together with DICOM for imaging, protocols, and security standards (see Sect. 5.2). Testing sessions organized by third parties such as IHE connectathons support implementers to test their own implementation with their peers before deployment in the real life. At each step, a validation process allows feedbacks from the community and increases the consensus.

The next section lists the main standardization and profiles bodies, their main domain of standardization, some of their standards, and the main area of use of them.

[4] http://wiki.ihe.net/index.php?title=Scheduled_Workflow

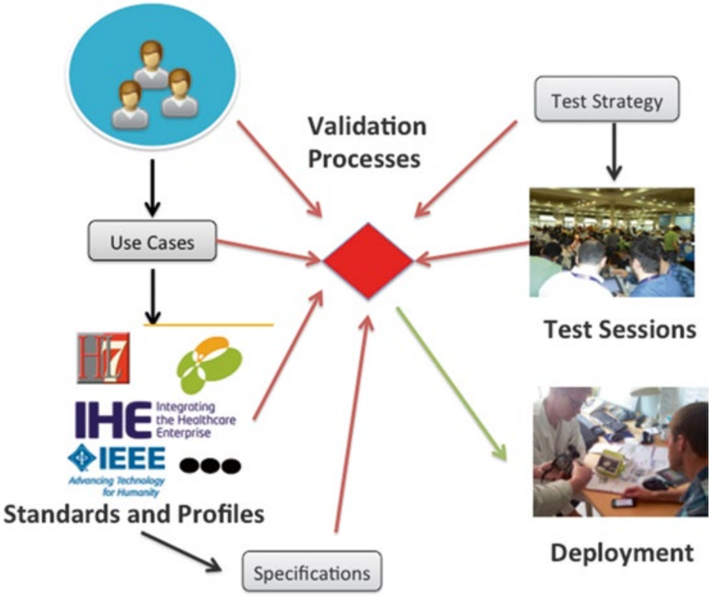


Fig. 5.2 Life cycle and validation processes

5.2 Standards Bodies and Fora in eHealth

The universe of standards used in eHealth is very large coming from Europe and worldwide. Some national standards also exist when used as a basis for national regulation. As underlined in Sect. 5.1, standards are clear guidelines for solution implementers to provide robust and interoperable solutions. The process to develop standards is based on a consensual approach, setting up a working group, publishing ballots for public comments, and providing trial specifications and stable versions. These approaches vary from one standard organization to another. More and more organizations publish their specifications free of charge and these are available directly on their websites.

In Tables 5.1, 5.2, and 5.3 the reader will find an overview of the standards bodies in eHealth, the most commonly used terminologies to support semantic interoperability as well as a list of consortia developing profiles. This listing is based on the experiences developed by the writers in the field of health interoperability developed during connectathon, the health interoperability events of the IHE alliance.[5]

It is important to note that security is one of the challenges of interoperability in eHealth. Developers will find several profiles and recommendations available in IHE technical frameworks and in Continua Alliance implementation guidelines.

[5] http://www.ihe.net/connectathon/

Table 5.1 List of main standard organizations relevant for the health sector

Standardization bodies	Standards	Usage
HL7 Inc. (Health Level 7): International nonprofit association founded in 1987 that develops framework and related standards for the "exchange integration, sharing, and retrieval of electronic health information that supports clinical practice and the management, delivery and evaluation of health services" www.HL7.org	HL7 v2.X messaging standards	Commonly used within healthcare enterprises such as hospitals.
	HL7 Reference Information Model (RIM)	Object model representing the clinical data.
	HL7 V3	Messaging used mostly in the patient domain and used in IHE PDQ (Patient Demographic Query) profile.
	HL7 CDA r2 or r3 (Clinical Document Architecture)	Structured clinical document description such as patient summary, ePrescription, discharge letter, or other shared medical documents used in several national or regional EHRs or PHR projects.
	Other standards: EHR systems functional model (EHR-S),[a] FHIR (Fast Health Interoperable Resources[b]), CCOW (Clinical Contect Object Workgroup), MLLP (Minimum Lower m Layer Protocol, …	EHRs functional model is used in some quality labeling programs over the world
		FHIR is a new standard for exchanging data for mHealth, cloud communications, actually in test. It combines the best features of HL7v2 and HL7 CDA and web standards (XML, JSON, HTTP, Atom, OAuth, …)
DICOM (Digital Imaging and Communication in Medicine): The DICOM is a committee led by the National Electrical Manufacturers Association (NEMA) since 1983. DICOM publishes the DICOM standards specifying "a network protocol utilizing TCP/IP and defining the operation of SOP Classes (Service-Object Pair) beyond the simple transfer of data and uniquely identifying Information objects."[c] http://medical.nema.org	DICOM	DICOM is widely used in several domains such as radiology, radiotherapy, ophthalmology, ultrasound, digital mammography, pathology, dentistry, dermatology, computed tomography, etc. Five services are proposed: transmission and persistence of complete objects, query and retrieve of objects, workflow management, quality and consistency of image appearance.

(continued)

Table 5.1 (continued)

Standardization bodies	Standards	Usage
IEEE (Institute of Electrical and Electronics Engineers): The Institute of Electrical and Electronics Engineers is an association that the mission is to foster technological innovation. IEEE has published the standards family ISO/IEEE 11073-X (Personal Health device Communication) for interoperable communication among devices and compute engines such as servers, boxes, or cellphones. https://standards.ieee.org/	IEEE 11073-10101™ "Health informatics—Point-of-care medical device communication—Part 10101: Nomenclature"	The devices communications that have been specified are the glucose meter, blood pressure monitor, insulin pump, ECG, body composition analyzer, International Normalized Ratio (INR) monitor, Independent living activity hub, cardiovascular fitness, etc. (see the list).
	IEEE 11073-10201™ "Health informatics—Point-of-care medical device communication—Domain information model"	
	IEEE 11073-20101™ "Health informatics—Point-of-care medical device communication—Application profile—Base standard"	
	IEEE 11073-20601™ "Health informatics—Personal health device communication—Part 20601: Application profile—Optimized exchange protocol"	
	Etc.	
CEN/TC 251: European Committee of normalization specifies eHealth standards in TC 251 (Technical Committee)	EN ISO DIS/13940, System of Concepts for Continuity of Care (ContSys) provides domain coherence to support interoperability in healthcare integration	The standard CEN/ISO 13606 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.
	EN ISO/TS 19218 specifies coding practices for describing adverse events relating to medical devices	
	EN ISO 15225 defines a medical device nomenclature data structure for exchange of data used by regulatory bodies	

[a] http://www.hl7.org/implement/standards/product_brief.cfm?product_id=269
[b] https://www.hl7.org/implement/standards/fhir/
[c] http://medical.nema.org/dicom/geninfo/Strategy.pdf

Table 5.2 Main system coding (terminologies) in the health sector

System	Description
LOINC (Logical Observation Identifiers Names and Codes)	LOINC[a] is an international coding system for clinical and laboratory observations generally used with the HL7 V2.X messages but also in the laboratory reports structured using HL7 CDA. The laboratory categories are chemistry, hematology, serology, microbiology, and toxicology as well as cell counts, antibiotic susceptibilities and other. Six dimensions of the test are described: component, property, time, system or specimen, scale, and method.
	LOINC is today used in several hospitals and national/regional projects in Europe for sharing information.
ICD-10 (International Classification of diseases)	This terminology is "*the standard diagnostic tool for epidemiology, health management and clinical purposes*"[b] and is developed by World Health Organization (WHO). This is the most common terminology used in countries worldwide. This terminology is available in 6 official languages and in 36 other languages. The ICD is a variable-axis classification. The structure presents five groups of diseases: epidemic diseases, constitutional or general diseases, local diseases arranged by site, developmental diseases, and injuries.
SNOMED/CT (Systematized Nomenclature of Medicine—Clinical Terms)	This terminology is today maintained by IHTSDO (International Health Terminology Standards Development Organisation), a nonprofit association in Denmark and it is "*the most comprehensive multilingual clinical healthcare terminology in the world*."[c] It has been developed by clinical experts and allows its use in EHR system. SNOMED/CT has a hierarchical architecture covering more than 18 concepts such as body structure, clinical finding, environment and geographical location event, organism, and pharmaceutical/biological product.
	A formal work under the WHO is in progress in order to develop and assure maps and linkages between SNOMED/CT and ICD-10.

[a] http://loinc.org

[b] http://www.who.int/classifications/icd/en/

[c] http://www.ihtsdo.org/snomed-ct/

Table 5.3 Main organizations developing health profiles

IHE (*Integrating the Healthcare Enterprise*): International association and initiative led by healthcare professionals and vendors to improve the integration between healthcare systems. IHE specifies profiles based on primary standards such as HL7 and DICOM and Internet standards. Several healthcare domains are covered: pathology, cardiology, dental, eye care, patient care coordination, patient care devices, laboratory, pharmacy, radiology, etc. http://www.ihe.net	Profiles in 13 domains such as infrastructure, radiology, laboratory, pharmacy, pathology, patient care devices, ….	IHE develops initiatives in countries and regions worldwide. Connectathon is a testing event carried out in a controlled environment in order to test profile implementation by systems and is yearly organized by the deployment committees in countries and regions such as North America, Europe, Australia, Korea, Japan, and China. A test bed platform called Gazelle Management tool[a] is used worldwide and provides a good quality and results homogeneity of the tests among connectathons.
	The list of IHE profiles used for the European use cases are available in the eEIF (eHealth European Interoperability Framework). http://ec.europa.eu/digital-agenda/en/news/ehealth-interoperability-framework-study-0.	
Continua Healthcare Alliance: Industry association that provides guidelines on interoperable communication for an ecosystem of connected devices used in the personal healthcare. http://www.continuaalliance.org	The guidelines are based on IEEE standards, IHE profiles, and communication protocols such as Bluetooth and USB	These guidelines are specifications based on connectivity standards and resolve gaps in standards in order to offer a complete solution of interoperability. The domains covered by Continua Healthcare Alliance are health and illness, chronic diseases, management, and aging. Continua Healthcare Alliance provides a certification program that ensures customers in their choice of products.

[a] http://gazelle.ihe.net

These are based on security standards used at the protocol levels (TLS 1.0), messaging (S/MIME v3.1), syslog Protocol (RFC5424), HTTPS, certificates (X509), WS-Security profiles 1.1,[6] etc.

5.3 Profile-Based Approach for Engineering Interoperability Requirements

5.3.1 Introduction

A healthcare IT system is a complex system that includes several components from healthcare application such as an electronic health record (EHR), specialized applications such as laboratory or radiology applications, modalities, robots, and medical devices and includes also mobile applications and homecare applications. Healthcare organizations are no longer the only point of care and will share with telemedicine and care delivered at home with the introduction of medical devices.

Communication between healthcare professionals, providers of the devices, and the patient will facilitate the extended development of healthcare processes in an interoperable and secured environment.

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 regard to health and safety reasons the necessity of standards and regulation is undisputed, regulations on the other hand make product development risky and costly, and hence discourages software and electronic companies to contribute to value creation and innovation.

Identifying standards relevant to the development of interoperable healthcare services requires a multi-step approach from the development teams.

1. *Mapping of relevant standards (elicitation), see Sect. 5.3.3.1*: 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.
2. *Identification of interoperability profiles (analysis), see Sect. 5.3.3.2*: 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, integration using healthcare profiles specifies how the products interact.

[6] https://www.oasis-open.org/committees/download.php/16790/wss-v1.1-spec-os-SOAPMessageSecurity.pdf and http://docs.oasis-open.org/wss/v1.1/

3. *Defining and implementing validation strategies (checking), see Sect. 5.3.3.3*: Besides usual test practices used in software development processes, specific test frameworks have been created to contribute to both standard compliance and interoperability of produced software. These frameworks need to be analyzed and included within the validation strategy.

5.3.2 Case Study: epSOS for Transnational Integration of EHR

This section describes the use of the profile-based approach illustrated with the case of a large European project named epSOS (Smart Open Services for European Patients), chosen for its adherence to the approach and its multinational dimension.

epSOS is a European project with the aim of exchanging medical data (patient summary and ePrescription) for a patient travelling to another European country. More specifically, epSOS aims to design, build, and evaluate a service infrastructure that demonstrates cross-border interoperability between electronic health record systems in Europe.

epSOS has the objective to increase the patient in safety by providing a quick access to medical information of a patient that will not be in a native language of the healthcare professionals and will allow the reduction of medical errors. In emergency situations, it provides a "quick access to documentation with life-saving information."[7]

epSOS allows a patient travelling abroad to access to his(her) patient summary or prescription when he(she) finds him(her) self in need of using healthcare services. epSOS specifies cross-border eHealth services that answer to these use cases.

Several services are today available:

- Patient summary access for patient treatment
- Cross-border use of ePrescription or eMedication
- Access of patients to their data and the medication-related overview (MRO)

The design of the EED (epSOS Evolving Document on Architecture and Design—Interoperability Specification) provides a blueprint for connecting existing eHealthcare services. This specification is based on the Enterprise Conformance and Compliance Framework (ECCF); see Sect. 5.3.1.

The design of the architecture is based on a national contact point (NCP) that is not intrusive in the country and it connects national eHealth infrastructures between them without changing their organizations. The advantages are that the country is neither obliged to update its own infrastructure nor its internal policies

[7] www.epsos.eu

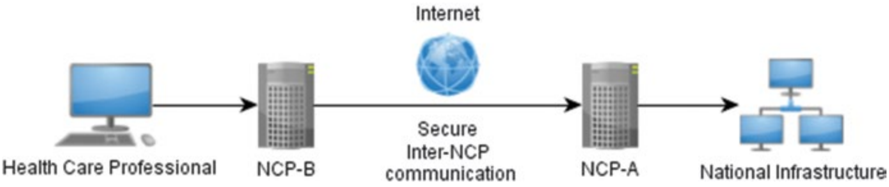


Fig. 5.3 Overview of NCP communication (D3.B.2 AppA1_OSS_NCP design v1.0)

and procedures. The security aspects are taken into account through the NCP and no connections can be established by by-passing it. The medical data can only leave or enter a national infrastructure through the national NCP (Fig. 5.3).

5.3.3 Applying the Profile-Based Approach for Engineering Interoperability Requirements

5.3.3.1 Mapping of Relevant Standards

When developing a healthcare product, four different areas of investigation have to be considered:

- Software development
- Usage of the product
- Resilience to protect from harm
- Security for data protection.

For each of them, a solution provider can have a look for standards in the mentioned areas in order to identify all requirements relevant for his or her endeavor. Indications of international standards existing in these areas are listed below and should be used as a starting point to build the list of potential standards of interest for the development team.

Software Development

IEC 62304 [4] 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[8] (Capability Maturity Model integration) and ITIL (Information Technology Infrastructure Library)[9] and development lifecycle models such as waterfall and agile. It constrains development, maintenance, risk

[8] http://whatis.cmmiinstitute.com

[9] http://www.itil-officialsite.com

Table 5.4 Dimensions and perspectives of the HL7 ECCF [8]

Dimensions	Relation with the four interoperability levels	Perspectives
– Enterprise view point (Why)	– Clinical	– Conceptual perspective
– Information dimension (What)	– Semantic	– Logical perspective
– Computational dimension (How)	– Syntactical	– Implementation perspective
– Engineering dimension (Where)	– Technical	
– Technical dimension (Where)	– Technical	

management, configuration management, and problem resolution practices based on an assessment of safety criticality of the software. IEC 62304 compliance contributes to FDA (Food and Drug Administration) compliance for medical devices.

ISO 9241-210 [5] specifies the processes of designing interactive systems from a usability perspective, and ISO/TR 16982 [6] specifies the use of usability engineering methods as part of such development processes. IEC 62366 [7] defines the corresponding process to be followed for engineering medical devices.

In eHealth systems can be designed on the Enterprise Conformance and Compliance Framework (ECCF) (derived from the SAIF—Services-Aware Interoperability Framework Canonical Definition—*HL7* [8]) where the characteristics of the system are analyzed through the matrix of the five dimensions (columns) and three perspectives (lines). Table 5.4 gives an overview of the ECCF dimensions and perspectives. In terms of interoperability, the dimensions of HL7 ECCF can be mapped with the previous ETSI model according to the second column of the table.

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.

Usage of the Products

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 [9] 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 [10] defines guidelines for multimedia interfaces that are used by the general public without any special previous training. ISO 15223 [11] 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 [12] 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 [13] 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. In particular:

- ISO/IEC 27001:2013 “Information technology—Security techniques—Information security management systems—Requirements”[10] contains information security requirements generic for all types of organizations. It contains “the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization,” as well as for “the assessment and treatment of information security risks.”
- ISO/IEC 27002:2013 is complementary to ISO/IEC 27001:2013 and contains guidelines for organizational information security standards and information security management practices, “taking into consideration the organization's information security risk environment(s).”
- Standard ISO 27799:2008 contains guidelines on best practices and indicators of health data security. It supports the interpretation and implementation in health informatics of ISO/IEC 27002 and is complementary to that standard.

Whereas the product supplier perspective is covered within IEC 80001, ISO 14971 [14] specifies the risk management practices to be followed by a medical

[10] http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=54534

device manufacturer. ISO 13485 [15] defines regulatory requirements for medical devices, including documentation, management, product realization, and quality assurance processes.

Data Security and Data Protection

Current data protection legislation in Europe does not contain mandatory requirements to comply with particular data security standards or of data security certification. However, using such standards contributes to establishing whether or not the data controller abides by the data security obligations under the European Data Protection Directive (DPD) [16]. These issues are described in greater details in Chap. 3.

epSOS is compliant with several directives and recommendations and one of the epSOS working groups worked deeply on the alignment of epSOS to regulation. Among them, the following were studied:

- European data Protection Directive 95/46/EC: This directive is actually under revision and the recommendations issued by epSOS are also under revision and discussed.
- Directive 2011/24/EU on the application of Patients' Rights in Cross-Border Healthcare in order to facilitate and promote the exercise of patient's choice to access healthcare services in other country: In article 48, it is stipulated that appropriate information is enabled to exercise the patient rights and one of the mechanisms for providing such information is to establish national contact points within each member state in Europe and can be provided to the patient in any of the official languages of the member states in which the NCP is situated.
- EC Article 29 working group recommendations on eID and trust services regulation for electronic transactions in the internal market.
- European Directive on Recognitions of Professional Qualifications (2005/35/EC).

Directives and regulation are going through a reform process. The sustainability of the epSOS assets is supported by member states involved and the eHN SG (eHealth Network) and will be examined in the new European project called EXPAND.[11]

5.3.3.2 Identification of Interoperability Profiles

The identification of the profiles needs some expertise. The evaluator should go through the three perspectives listed in Table 5.4.

- *Conceptual perspective*: To identify the business strategies and the use cases.

[11] The goal of EXPAND is to maintain and expand the already existing resources and assets and act as a catalyst for real operational use by member states.

- *Logical perspective*: To define the architecture of the IT solution using clearly defined, product agnostic, services, or components.
- *Implementation perspective*: To detail the profiles targeted, the process, as well as deployment models

During this process, the evaluator has to review the existing profiles provided by IHE and Continua Alliance and select the one answering the needs of the targeted use cases, workflow, and semantic assets. The selection of the profiles depends on criteria such as

- The ability to answer the needs: Descriptions of the use cases supported by the profiles are listed. These descriptions facilitate their selection.
- The ability to mix profiles for the chosen architecture: A solution or a project implements several profiles mixing the clinical needs, the complementary functionalities that support the infrastructure, and the security environment. For example, exchanging patient summary between two countries for a given patient has to implement profiles providing patient identification and patient consent. The security will be taken into consideration by adding profile and node authentication and audit trail.
- The ability to customize easily the profiles: Once the profiles are selected, they have to be analyzed in detail for their customization by adding specific implementation needs such as the choice of OID (Object Identifier), terminologies, ….

Profiles are thematically organized to ease the work of the evaluator. Taking the case of IHE, there is a first family of profiles[12] looking at the underlying "IT infrastructure" and then others are use case oriented (anatomic pathology, cardiology, eyecare, etc.).

In the case where a gap is found, i.e., there is no profile that answers the request, relevant standards shall be investigated to fill the gap. Preference to mature and operational standards shall be taken. If no standards are available, proprietary specifications will support an earlier development. It is recommended to contact the standard body for starting further standard development.

Some expertise is mandatory for leading this task. Standard bodies and fora deliver trainings and courses for the new comers in the eHealth sector.

In the example of epSOS, the services were specified with the experts and members of IHE. Most of the epSOS services described in the following list

1. Identification service
2. Patient service
3. Order service
4. Dispensation service
5. Consent service

[12] http://wiki.ihe.net/index.php?title=Profiles

are supported by IHE profiles (IHE XCA, IHE XCPD, IHE Fetch, IHE XDR, IHE BPPC). These profiles involve several underlying standards. For example, the profiles

- IHE XCA (Cross Community Access) embed
  - ebRIM OASIS/ebXML Registry Information Model v3.0
  - ebRS OASIS/ebXML Registry Services Specifications v3.0.
- IHE XCPD (Cross Community Patient Discovery)
  - HL7 Version 3 Edition 2008, Patient Administration DSTU, Patient Topic
  - HL7 V3 Data types 2008 Normative Edition.
- IHE XDR (Cross Enterprise Document Reliable Interchange)
  - ebRIM OASIS/ebXML Registry Information Model v3.0
  - ebRS OASIS/ebXML Registry Services Specifications v3.0.
  - MTOM: SOAP Message Transmission Optimization Mechanism [W3C MTOM]
  - XOP: XML-binary Optimized Packaging [W3C XOP].

This list of profiles was completed with other standards for specific needs. For example epSOS defines a user assertion based on SAML V2 standard.

5.3.3.3 Defining and Implementing Validation Strategies

The testing strategy is defined, following the know-how of the IHE testing team (accreditation ISO/IEC 17025) and the recommendations of the International Software Qualification Board (ISTQB).[13] This testing strategy could be identified as a label testing involving a third party which is IHE-Europe.

At the interaction level, the testing methodology includes three steps (see Fig. 5.4):

- Pre-Projectathon: Testing stand-alone the implementation test methods based on test scripts, validators and simulators, test data, and test methodologies defined by IHE-Europe.
- Projectathon when the Pre-Projectathon is passed, where countries and community test their own implementation in a face-to-face testing session which is a controlled testing environment using test methods.
- Pre-Pilot testing is a virtual testing session where countries test their real implementation with test data in their environment. When this Pre-Pilot testing session is passed, the countries are allowed to go to the pilot phase.

User interfaces are also tested by the healthcare professionals during the Projectathon and the Pre-Pilot testing session in order to verify that the medical data presented at the end user are the data sent by the country of origin according to their translation.

[13] www.istqb.org

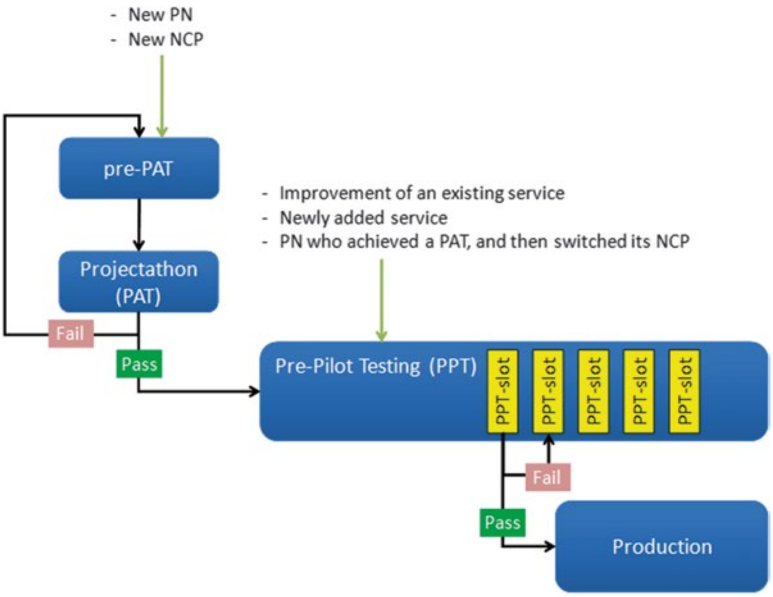


Fig. 5.4 epSOS testing strategy. *PN* participating nations, *PAT* projectathon, *NCP* national contact point

5.4 Discussion

This section presents the challenges encountered and lessons learned by the epSOS project. It covers how to guide thoughtful application of the profile-based approach for engineering interoperability requirements. Each lesson is concluded with a concrete recommendation of what research and practice can do to further ease interoperable digital health applications.

5.4.1 Software Development and Quality Management

The epSOS community had developed the open NCP components (national contact point) under a quality management process. The software development is based on the “V model” with four levels: component, system, integration, and acceptance. For each level specifications are provided and in mirror the test strategy is adapted.

The epSOS software development approach[14] was analyzed under the ISO/IEC 9126 standard by the epSOS team over which the evaluation should be performed. Their conclusions are the following:

- IQ V&V “Internal quality” is technical and verifies the internal functional and nonfunctional aspect of the system: This item is not within the scope of epSOS

[14] D3.C.1—Proof of Concept testing strategy v1.0

and restricted to the implementing bodies themselves such as participating nations and industry that develop the first implementation of the NCP.

- EQ V&V "External Quality" is mostly technical, verifying functional and nonfunctional aspects of a system with a view to its external interfaces: Some of relevant quality attributes were not tested in epSOS (suitability, accuracy, reliability compliance, usability compliance, performance ….) for several reasons and more specifically due to the complexity of the architecture that did not allow to create a complete testing environment that encompasses the NCP and their respective PN national infrastructures.
- QI V&V "Quality in use" gives a nontechnical, functional end-user perspective verifying business and end-to-end processes.

epSOS developed specifications implemented first by industry. It was assumed that the selected companies developed their own software under a controlled environment using guidelines for software development. After 2 years, epSOS decided to develop a new NCP (national contact point) which was developed by the open NCP community under the APACHE license 2.0.[15] "This open group of people orchestrated by an agile software development methodology conducts effort on designing, coding, testing and delivering openNCP software." Several member states are participating to the development of the open NCP software.

The quality label process is well defined with a transparent testing strategy, testing methods, and testing third party. Several industrial tools to follow the quality assurance process were selected (Jenkins, JIRA, MAVEN, etc.).

While profiles provide a pragmatic answer to the need for interoperability, they do not guarantee that software developments are following state-of-the-art quality practices. For that purpose, the use of software development standards is recommended. As for any standard, it is recommended to search for the latest version of the standard. As an example, the ISO/IEC 9126 standard used by the epSOS team is now obsolete, being replaced by the ISO/IEC 25010:2011 [17]. In addition specific standards for health application development exist and setting the software development processes should start with the analysis of the IEC 62304:2006 "Medical device software—Software life cycle processes."

5.4.2 *Identification of Existing Software Building Blocks*

To reduce the burden of software certification for the developers, a number of open-source initiatives are emerging, supported by the fora and the market. The purpose of these initiatives is to provide certified reference implementations of standards and profiles. The easiest to find recent information about these initiatives is through a web search from the IHE or Continua Alliance. IHE is maintaining a wiki page [18] of ongoing projects, one of the most active being the Open Health Tools Project Implementation of IHE Profiles. Client-side implementations of IHE profiles are

[15] https://openncp.atlassian.net/wiki/display/ncp/OpenNCP+Community+Home

supplied under the Eclipse Public Licence. At the time of writing, ten profiles were covered: ATNA (Audit Trail and Node Authentication), MPQ (Multi Patient Query), PAM (Patient Demographics Source), PIX (Patient Identifier Cross-Referencing), PDQ (Patient Demographics Query), SVS (Shared Value Sets) XCA (Cross Community Access), XDR (Cross-Enterprise Document Reliable Interchange), XDS (Cross-Enterprise Document Sharing), and XUA (Cross-Enterprise User Assertion) [19].

5.4.3 Usage of the Product

The NCP as proprietary or open software is implemented in pilot sites from more than 19 member states. The services that are exposed are the main specified services such as patient summary and ePescription services. No medical devices except medical applications displayed in terminal were tested during the pilot phases. The end-to-end model was considered as a human-centred process (see ISO 9241). Because of a process of translation (from the language of patient to the language of the healthcare professional in the hosting country) and transcodage of terminology (from the coding system used in the country of origin to the coding system of the targeted country) from one language to another, a particular attention of the requirements for the display of the documents (patient summary and ePrescription) and for the ergonomy of the application was highlighted during the project and the requirements were carefully tested with a transparent validation process in place.

The lessons learnt from the epSOS project reinforced the fact that eHealth services shall be delivering with high level of security, data protection, and liability in order to address patient safety in all the ny steps of the healthcare delivery processes. European and national/regional legislations shall be taken into account for any deployed cross-border eHealth services. A security policy was specified[16] to enhance user and patient to trust the epSOS environment. Security principles adapted to epSOS allows an effective acceptance of sharing information among member states and ensures that the respective national legislation on privacy and data protection are respected.

One of the objectives of this security policy is to establish the basic security provisions that shall be satisfied to ensure the data security and the system continuity and to prevent and minimize the impact of security incidents. Security rules describe requirements that apply to the medical data exchanges of the epSOS model. A security audit policy is also defined and covered several items compliant with ISO 27002 requirements.

The testing process with the different phases of testing phases contributes largely to the deployment of the solutions showing the feasibility of the project and helping the development team to solve technical and semantic issues. Using a mutualized test bed infrastructure with IHE accelerates the deployment of the national contact point (NCP) in member states.

[16] D3.7.2 Security policy v1.0

5.5 Summary and Conclusions

The proposed chapter provided an overview of the standardization landscape for eHealth and proposed a practical method to take it into account within the interoperability requirement engineering processes of eHealth applications. This approach relies on the use of IHE profiles which provide precise definitions of how standards can be implemented to meet specific clinical interoperability needs. The three-step approach is described and is presented to the case of the epSOS project. In this discussion, it is shown that the proposed approach has been a success. However expert knowledge and skills are needed both in the understanding of the IHE profiles and the targeted application architecture. Overall this chapter gives developers and practitioners a better understanding of standards development organizations, existing standards, terminologies, and interoperability profiles and of their relations. It provides guidelines to make an effective use of these to increase interoperability of developed eHealth systems.

References

1. European commission. eHealth Action Plan 2012–2020: innovative healthcare for the 21st century. https://ec.europa.eu/digital-agenda/en/news/ehealth-action-plan-2012-2020-innovative-healthcare-21st-century
2. Van der Veer H, Wiles A (2008) Achieving technical interoperability—the ETSI approach, ETSI White Paper No. 3. http://www.etsi.org/images/files/ETSIWhitePapers/IOP%20whitepaper%20Edition%203%20final.pdf
3. eHealth-INTEROP Report in response to eHealth Interoperability Standards Mandate, SA/CEN/ENTR/000/2007-20 eHealth Mandate M/403-Phase 1, 10 Feb 2009. http://www.ehealth-interop.eu
4. IEC 62304:2006—Medical device Software—Software life cycle processes. ISO Standards. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=38421
5. ISO 9241-210:2010—Ergonomics of human-system interaction—Part 210: Human-centred design for interactive systems. ISO standards. http://www.iso.org/iso/catalogue_detail.htm?csnumber=52075
6. ISO/TR 16982:2002—Ergonomics of human-system interaction—Usability methods supporting human-centred design. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31176
7. ISO 62366:2007—Medical devices—Application of usability engineering to medical devices. http://www.iso.org/iso/catalogue_detail.htm?csnumber=38594
8. HL7 Architecture Board (ArB). HL7 Services-Aware Enterprise Architecture Framework (SAEAF): Enterprise Conformance and Compliance Framework (ECCF), Dec 2009. http://wiki.hl7.org/images/9/96/ECCF_DECeditFINAL_clean_12228009.doc
9. ISO 14915 Software ergonomics for multimedia user interfaces (3 parts). ISO 14915-1:2003—Part 1: Design principles and framework. ISO 14915-2:2003—Part 2: Multimedia navigation and control. ISO 14915-3:2003—Part 3: Media selection and combination. http://www.iso.org/iso/catalogue_detail.htm?csnumber=25578
10. IEC/TR 61997 ed 1.0—Guidelines for the user interface in multimedia equipment for general purpose use. http://webstore.iec.ch/Webstore/webstore.nsf/ArtNum_PK/27914!opendocument&preview=1

11. ISO 15223:2012—Medical devices—Symbols to be used with medical device labels, labelling and information to be supplied (2 parts). ISO 15223:2012 Part 1: General requirements. http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=50335. ISO 15223:2010 Part 2: Symbol development, selection and validation. http://www.iso.org/iso/catalogue_detail?csnumber=42343
12. ISO/TR 16142:2006—Medical devices—Guidance on the selection of standards in support of recognized essential principles of safety and performance of medical devices. http://www.iso.org/iso/catalogue_detail.htm?csnumber=38401
13. IEC 80001:2010—Application of risk management for IT-networks incorporating medical devices (5 parts). IEC 80001:2010: Part 1: roles, responsibilities and activities. http://www.iso.org/iso/catalogue_detail.htm?csnumber=44863
14. ISO 14971:2000 Medical devices—Application of risk management to medical devices. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=31550
15. ISO 13485: 2003—Medical devices—Quality management systems—Requirements for regulatory purposes. http://www.iso.org/iso/catalogue_detail?csnumber=36786
16. Directive 1995/46/EC, Official Journal 1995, L281/31
17. ISO/IEC 25010:2011—Systems and software engineering—Systems and software Quality Requirements and Evaluation (SQuaRE)—System and software quality models. http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=35733
18. Implementation. IHE. http://wiki.ihe.net/index.php?title=Implementation
19. Open health tools. http://www.openhealthtools.org/index.htm

Chapter 6
User Experience (UX) Design for Medical Personnel and Patients

Oli Mival and David Benyon

Abstract UX design is concerned with all the issues that go into providing an engaging and enjoyable experience for people in both the short and longer term. This is more than mere functionality and includes aesthetics, pleasure, and emotional engagement in terms of both the product and the service provided. In particular it is important to consider experiences at a physical, behavioral, and social level and in terms of the meanings people derive from their experiences. In this chapter the authors explore the ideas of UX and methods for applying a user-centered design (UCD) approach to the design of interactive medical and healthcare applications and provide guidelines and recommendations for the delivery of high-quality user experiences within medical domains.

6.1 Introduction

6.1.1 What Is UX and Why Does It Matter?

In the twenty-first century the interaction between people and technologies cannot be merely functional. People are now used to websites, smartphone apps, and other forms of interactive experiences and have the expectation for things to function well and to be enjoyable to use. If an e-Health application—whether delivered through a website, mobile device, or PC—is not engaging, people will not use it or search for an alternative that is. If they are forced to use it (for example if it is the only alternative), then it is likely that they will make mistakes, or use it badly and hence its effectiveness will be compromised. For these reasons it is critical that the focus is on delivering a good user experience (UX) when developing interactive products, infrastructures, and services.

Contributions to an understanding of experience design come from many different areas. Nathan Shedroff published *Experience Design* [1] and John McCarthy and Peter Wright explore the wider issues of experiences through their book

O. Mival (✉) • D. Benyon
Centre for Interaction Design, Institute for Informatics & Digital Innovation,
Edinburgh Napier University, Edinburgh, UK
e-mail: o.mival@napier.ac.uk; d.benyon@napier.ac.uk

S.A. Fricker et al. (eds.), *Requirements Engineering for Digital Health*,
DOI 10.1007/978-3-319-09798-5_6

Technology as Experience [2], drawing on the philosophy of John Dewey. Patrick Jordan and Don Norman have both published books on the importance of designing for pleasure [3, 4] and others talk about "ludic" design, "hedonomics," and "funology." Work on aesthetics has a long history and has recently been applied to interactive systems design [5].

UX design is about recognizing that interactive products and services do not just exist in the world, they affect who we are. They influence our culture and identity. As the philosopher John Dewey said, "experience is the irreducible totality of people acting, sensing, thinking, feeling and meaning-making including their perception and sensation of the artifact in context" (quoted in [2]). UX is concerned with all the qualities of an experience that really pull people in—whether this is a sense of immersion that one feels when reading a good book, or a challenge one feels when playing a good game, or the fascinating unfolding of a drama. It is concerned with all the qualities of the interactive experience that make it memorable, satisfying, enjoyable, and rewarding.

In their treatment of technology and experience, McCarthy and Wright highlight the need to take a holistic and pragmatic approach. They argue that experiences have to be understood as a whole and cannot be broken down into their constituent parts, because experience lies in the relations between the parts. Interactivity involves the combination of people, technologies, activities, and the social and cultural contexts in which the interaction happens. Designers need to consider the combination of these elements and strive to achieve a harmonious combination.

Experiences, therefore, cannot really be designed. Designers can design *for* experience, but it is individuals and groups who *have* the experience. However, designers *can* be sensitive to the characteristics that create a good experience and can draw upon knowledge of designing for engagement, function, pleasure, and aesthetics. The most common method is the application of user-centered design, or UCD.

The terms "user experience design" (UX) and "user-centered design" (UCD) are often used interchangeably but there is an important distinction. UX design is the discipline or field; *what we* (as UX practitioners) *do*. Precise definition can be elusive, but most attempts focus on experience as an *explicit* design objective. User-centered design however is a process: *how we* (as UX practitioners) *do it*.

Put another way, *UCD* is a *method* (or *process*) to achieving good *user experience*.

In this chapter we explore the ideas of UX and methods of UCD, provide an example of a UCD approach to the design of interactive e-Health application, and give guidelines for the delivery of high-quality UX.

6.2 UX, UCD, and Medical Software Products: A Developer's Cookbook

UX and UCD can play significant roles in successful software and service development and deployment, but the question developer communities commonly have is "how." This section is intended to provide guidance to develop the right user experiences by introducing and discussing UCD methods in a simple, succinct, and practical manner to help facilitate their potential uptake and deployment in medical software product development.

6.2.1 Software Products in the Medical Domain

The domain of healthcare information technology, often called eHealth or digital health, is a large and expanding market estimated to be growing from $21.9 billion in 2013 to $31.3 billion in North America alone [6]. From massive national electronic health records to smartphone apps monitoring glucose levels for diabetics the software products and services vary greatly in size and scope and the proliferation of mobile devices including smartphones and tablets has increased the market opportunity for personal healthcare apps which avoid several of the pitfalls of the larger medical devices software whose challenges include FDA compliance and stringent quality requirements. A further challenge of large-scale medical software platforms and services is the length of time taken for deployment and upgrade, even more reason to ensure that the design phase is optimized.

Typically, in hospital scenarios medical software is used for diagnostic purposes via monitoring or analysis of sensor or physiologically derived test data [7]. Examples of software systems, services, and applications in medical use cases provide some interesting and challenging requirements and constraints specific to that particular domain of deployment. For example, in hospital environments such as operating theatres there is often the need for interactions with software whilst in a sterile environment. There has also been a significant shift in the past 30 years in areas such as radiology where there has been a decoupling of location and hardware requirements for data acquisition and data display (e.g., for MRI or similar radiological sensors where the monitor for reading the scans was located on the scanners themselves) plus the recent move to mobile reading (although not yet for primary diagnosis) via tablets [8]. This trend towards mobile medical applications, sometimes referred to as mHealth, is even more prevalent in consumer facing healthcare applications, many of which can be found within the various mobile platform's app stores [9]. As mHealth apps begin to raise consumer expectations with deeply considered and pleasurable user experiences, well-crafted, contextually appropriate UX should become the standard for all medical software, regardless of scale or location of deployment.

6.2.2 The UCD Approach

User-centered design (UCD) is a philosophy and set of methods focused on designing for and involving end users in application development to achieve high-quality user experiences and high-quality software products and services. The UCD process is based on proven, essential design processes and accountability across the entire design life cycle. A UCD approach results in more usable and satisfying systems [10], making software more effective, efficient, easy to learn, pleasant to use, and predictable thus delivering a high-quality UX which contributes to high-quality products. Furthermore, Jakob Neilson's analysis of the ROI (return on investment) of usability derived from UCD concludes an average KPI improvement of +83 % in projects based on usability engineering [11]. This is less than the +135 % he determined in 2002, but still a clear indicator of the impact a UCD approach can have.

UCD practice is based on four fundamental principles:

1. Focus on *real* end users.
2. *Validate* requirements and designs.
3. Design, prototype, and develop *iteratively*.
4. Understand and design for the *holistic* user experience.

The UCD process embraces these principles through three pre-development phases:

1. Understanding users
2. Defining interactions
3. Designing user interface(s)

The foundational principles and pre-development phases of UCD are applicable to all software development domains of use and platforms of deployment, from traditional PC-based applications and services to websites and mobile apps. The activities are organized around understanding end users' needs, scoping and defining interactions based on that understanding, and designing user interfaces (UIs) from the interaction definitions. Each is discussed in the following sections.

6.2.3 A User-Centered Design Methodological Overview

Figure 6.1 provides an overview of a typical software product design and development life cycle incorporating a UCD philosophy in which can be seen the three pre-development phase activities.

6.2.4 First Phase: Understanding Users

Product development typically begins with a vision of a product, which includes a vision of the *users* for that product [12]. A vision, however, is not enough to start design. Every product has different users and some products have many different types of users. Even new versions of old products have a changing user population. The users of medical products can be wide ranging depending on the functionality and context of use including not just medical personnel but also administrative and technical support staff, plus at times of course the patients themselves.

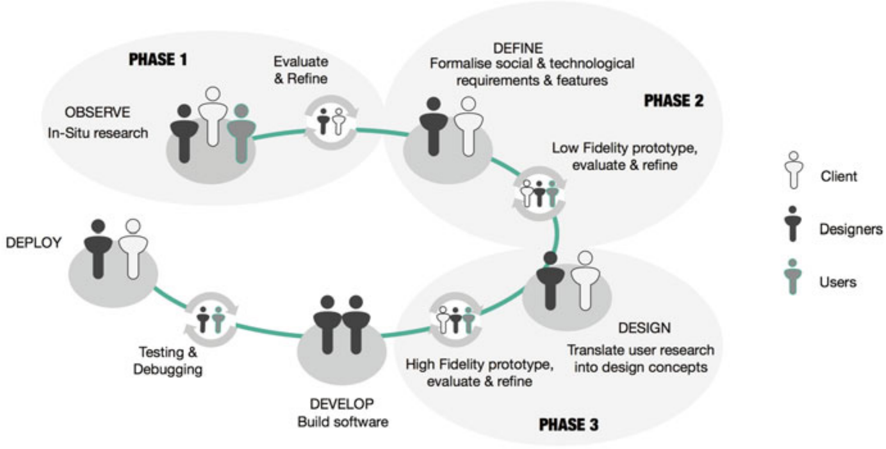

PHASE 1
OBSERVE
In-Situ research
Evaluate
& Refine
DEFINE
Formalise social & technological requirements & features
PHASE 2
Low Fidelity prototype, evaluate & refine
DESIGN
Translate user research into design concepts
PHASE 3
High Fidelity prototype, evaluate & refine
DEVELOP
Build software
Testing & Debugging
DEPLOY
Client
Designers
Users

Fig. 6.1 Overview of a model three-phase UCD approach for software design and development

The UCD process relies on iterative user-focused research to understand users and their needs. Existing user knowledge database can be a good start but it is important to involve potential end users at the onset of UCD. Ethnographically informed methodological tools such as focus groups, interviews, and field research form the basis of the first two phases of UCD (the OBSERVE and Evaluate-Refine parts of Fig. 6.1). To ensure that end users and their needs are sufficiently understood, the first phase examines the user population, their work, and their needs. All the user research conducted is then organized and summarized in a user research synthesis, leading to user profiles, work activities, and requirements for the intended user populations from which the user interfaces will be determined and designed.

6.2.5 Second Phase: Defining the Interaction(s)

One of the problems in UCD can be when attempting to transfer the understanding of users (research) to the actual user interface (UI) design [13]. Even simple products struggle without a clear definition. The key is to *define* interactions first, without necessarily "designing" them in the process.

The summarized user research information feeds directly into use cases, which define a products use, i.e., interaction. To start use cases, a subset of work activities are identified and organized into a coherent product with a high-level overview on how information will flow throughout the application. In medical scenarios this often involves connections between multiple pieces of hardware, for example biometric measurement sensors monitoring a patient's vital signs or other physiological factors, and thus the interaction flow with and between these devices must be considered holistically. Then the specified work activities are captured in further detail with goal-based use cases. The use cases show steps to accomplish task goals and the data needed to perform interactions. The data definitions are the only elements of an "interface" that need to be determined in this phase; therefore, dialogs, buttons, tabs, labels, and all other interface elements are not mentioned.

Completed use cases are then evaluated and refined with the intended user population. This is a checkpoint to see if the vision is being achieved and the value is clear to users.

6.2.6 Third Phase: Design the UI

The third phase of UCD is to design the UI, evolving directly from the interaction definition. Product scope and interface organization are clear from the high-level information organization, and UI components are clear from use case steps and data.

A software product's UI is its means of communication and interaction with users who have, on the whole, little to no interest in the technical underpinnings of software systems. The UI "look and feel" can directly impact perceived (and actual) usability [14] and hence aesthetics is a large area of study concerned with human appreciation of beauty and how things are sensed, felt, and judged.

Lavie and Tractinsky [15] see the aesthetics of interactive systems in terms of classical aesthetics (clean, clear, pleasant, aesthetic, symmetrical) and expressive aesthetics (original, sophisticated, fascinating, special effects, creative). They assert that "what is beautiful is useable." Certainly, there is more than traditional usability at work in people's judgments of quality of interactive systems, but at times people will rate usability as most important. Content, services, and brand are also factors to be taken into consideration.

Gillian Crampton-Smith [16] has argued, "The job of the designer is now not just to design the device, the software, and the way you interact with it, but to design the whole experience of the service so it is coherent and satisfying" (p. 3). Dan Saffer [12] defines a service as "a chain of activities that form a process and have value" (p. 175). The key thing about service design is that there are multiple "touch points" where people encounter a service and the interactions with services happen over time. To be well designed these touch points need to demonstrate a *consistent* look and feel, and present consistent values.

In service design, designers are concerned with providing resources to enable people-to-provider interactions. Services are more intangible and flexible than products. People do not walk away carrying a service, they take away the *results* of a service. Services are co-created to a large extent, negotiated between consumer and provider.

A consistent and engaging service must fit in with people's lifestyles. Interactivity in the next generation is distributed in time and place, the touch points. Saffer highlights the importance of service moments that these touch points provide and the need to design for these moments [12]. Moments come together as service strings, as short paths of an overall process description. To achieve this the interface and the history of interactions have to be transmitted between touch points, carried by the individual so that quality of service, security, privacy, and quality of interactive experience are all maintained across places and across time. There are both short-term and long-term interactions and the service needs to know what is mine, what I (as the user) am interested in, who I am willing to share what with, and how this changes depending on how I am feeling.

6.2.7 Prototyping the Design

A primary concern with design work is to avoid being locked into a single solution too early. To help prevent design traps, this phase is explicitly broken into two stages: low-fidelity prototyping and high-fidelity prototyping. Low-fidelity prototypes allow experimentation and rapid evaluation. High-fidelity prototypes provide exacting design and behavior previews of the final product that specifies what is to be coded.

Low-fidelity prototypes should be quick, inexpensive, and flexible sketches or mockups of tasks or flows, not the full product. Using pen and paper or post-it notes allows the focus to remain on concepts, navigational flow, metaphors, and alternatives rather than being distracted by look and feel or iconography. The goal is to improve design by rapidly iterating. Using low-fidelity designs ensures that iteration is built into the UCD process, which is the surest path to achieving high-quality user interfaces [12].

High-fidelity prototypes on the other hand are intended as stand-alone imitations of real applications and should mimic the full design look and feel plus interactive behavior as closely as possible. They will typically be authored using full featured tools (e.g., HTML editors, Adobe Creative Suite, or similar) and encompass the full interaction definition where possible (information architecture, use cases, and data flows) and incorporate the low-fidelity design decisions.

Iterative user evaluations at both stages should be fast and effective in improving UI through design feedback, rapid iterative evaluations, and usability evaluations. The purpose is less about testing or benchmarking usability and more about improving the UI design and hence user experience.

6.2.8 Documenting the Three Phases of UCD

Below in Table 6.1 is an example UCD report template that has been developed by the authors as a means of capturing and formalizing the critical outputs from the three UCD phases outlined above. It is intended to enable succinct communication between clients, designers/developers, and users for clarification and review of activities, insights, and designs thus far in the product development cycle outlined in Fig. 6.1.

Table 6.1 A UCD report template

Section 1—UI Overview		
List the User Interfaces (graphical or other) that exist within your product.		
Name	UI_ID	Description
For each UI identified, provide a succinct response to the questions in section 2. If you have multiple UIs, complete sections 2, 3, and 4 below and answer for each UI (label each part of section 2 with the UI_ID used above with the format UseCaseNameUI_name)		
Section 2—UI Detail		
1. What is the *user problem* the user interface is there to solve? (*i.e., what can they not do without it, refer to the goals to be achieved for each feature that is covered in the feature specification in the vision document)*		
2. Provide a *functional* overview of the User Interface. *(NB: If there are multiple functions, please list them in order of importance to the user. Please refer to the list of functionalities that were covered in the feature specification in the vision document)*		
3. Provide a *profile* of the user group(s), include relevant demographic and other details. *(e.g., age, occupation, technical experience)*		
4. What is the *location* of use? Be specific. *(e.g., if at a user's home, where within the home?)*		
5. How is it anticipated that the demographics and locations identified in points 3 and 4 impact the User Interface requirements (if at all)?		
6. What *hardware and software platform(s)* are involved in the User Interface and how do they impact user interface requirement? *For example physical dimensions, sensors, input devices (gesture, touch, etc.) provide boundaries, what are the impact they impose?*		
7. Who from the user groups identified above have you talked to? If you have additional/alternative insight into the users please provide details.		
8. How do you plan to evaluate the quality of your User Interface with your users? *For example interviews, focus groups, user trainings (how many), mockup testing.*		
Section 3—User Interface Navigation Architecture		
Include wireframes of application UI architecture. The wireframes should show the architecture and the navigation around the application.		
Section 4—Graphical User Interface Screenshots		
Include screenshots of application GUI.		
Section 5—Software Use Case Specification		
IEC 62304 Process Requirements has implications for user interaction design as there must be consideration of: – Input/output behavior of the application – Alarms/warnings/operator messages – Traceability features <-> User Interaction		
Section 5.1		
Feature Name and Description		
Feature Overview		
Addressed stakeholder interests and expectations	Goals to be achieved: External interfaces: Use cases:	
Comments		
Software Use Case Specifications of this feature		
For each use case identified, provide a succinct description of goals to be achieved, external actors (users and third-party systems), input devices, output devices, pre-conditions, flow of events, post-conditions, and alternatives and exceptions.		

6.2.9 Development Validation

Before development commences, the UI design should be reviewed for both quality and compliance with UI ISO standards (a discussion of the ISO standards related to this process is beyond the scope of the chapter; however information on the relevant standards can be found at www.iso.org). These steps are part of an ongoing UCD checks and measures process to facilitate the progress towards a high-quality user experience. End-user consideration (focus groups), iterative design, and some user evaluation of designs into any development project should be incorporated as early as possible into the validation process. Completed products should also undergo formal usability testing which helps monitor benchmark ongoing improvement over time against prior versions as well as competing products.

6.3 UCD in Action: Designing an Example Medical Application

This section introduces the application of a UCD methodology to a real-world project that developed software for addressing an important issue that can arise in surgical scenarios.

During surgery, to clean the surgical field or to remove blood from the surgical side, typically surgical towels are used. Additionally because of their size and the used materials, they are ideally to be placed under organs to get a better exposition or to remove organs from the area of interest. According to the surgical guidelines these towels have to be counted before and after operation to ensure that all material is removed out of the abdominal cavity before closing the incision. However, the problem of retained foreign body continues to be relevant. The incidence of retained foreign bodies is reported with every 1/3,000 to 1/5,000 cases still very high [17], and therefore has to be reduced by novel techniques.

As part of the FI-STAR: Future Internet—Social and Technological Alignment Research project one of the seven use cases within the project has focussed on the problem of tracking surgical towels and the potential of RFID technology to connect towels (and potentially any other surgical devices) that are being used and let them communicate and share information fits into our solution. Thus if the system can identify abdominal towels, track them, and share their location to other systems, it would help in reducing the number of cases where towels are forgotten. Multiple RFID antennas are installed in the operating room. By installing these antennas, it is possible to track the towels across three locations and be sure that no towels are missing or forgotten in the abdominal cavity.

These locations are the mayo stand (a sterile tray on which surgical tools and towels are laid out for the surgical team), the operating table (i.e., where the patient is) and the trashcan (where used towels and other surgical paraphernalia are placed

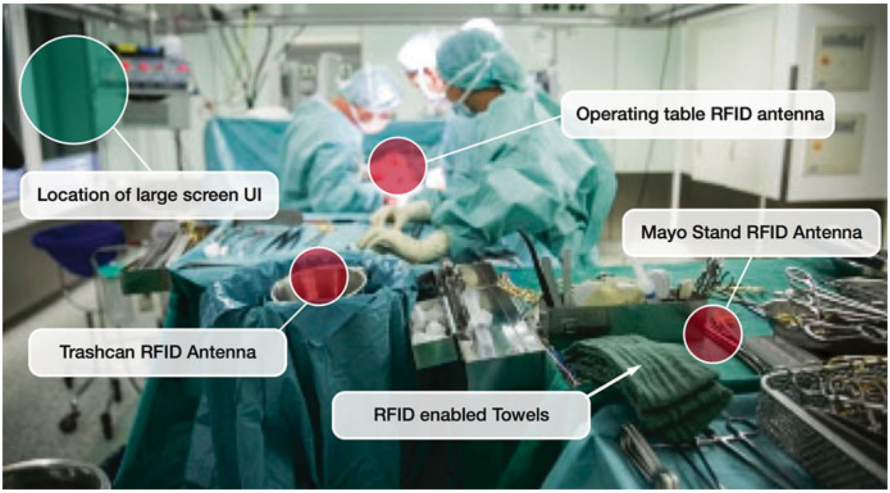


Fig. 6.2 Overview of RFID antenna locations for tracking towels in operating theatre

when finished with); see Fig. 6.2. The solution helps nurses and surgeons by providing intuitive way to visualize the position of towels on a central display in the operating room and also tablets used by nurses. The intention is for users of the solution to easily detect if there are missing towels by one glance at the display or the tablet.

The three-phase UCD method was deployed in the design of this solution and a completed UCD report template is shown in Table 6.2 below. Please note that due to limited space only one UI is outlined (the RFID towel tracker shown on the tablet and in theatre large screen) although the solution has three in total.

1. The total number of towels within operation "view" as understood by the system.
2. If the sum of towels in the three locations does not = total towels, then an alert indicated here with the number of missing towels and color change.
3. The UI is designed to enable simple "glancable" verification of the operations towel status via a large screen mirror of the iPad UI.
4. If no towels are detected, representation is grey; NB: if no antenna is detected (or associated to location) color and icon are greyed out and "OFFLINE" message shown (see Fig. 6.3).
5. When a towel is detected, location representation changes color with a numeric representation.
6. The key purpose of the RFID tracker is to prevent towels from being left in the patient; hence, whenever a towel is detected in the patient the representation turns red with a numeric representation.

The UI of the RFID tracker as shown in Fig. 6.3 is foremost a visualization of the underlying sensor data generated by the RFIDs embedded within the surgical towels

Table 6.2 A completed UCD template outlining the RFID tracker use-case UI

Section 1—UI Overview		
List the User Interfaces that exist within your product.		
Name	UI_ID	Description
RFID Tracker	RFID_Tracker_UI	In Operating Theatre UI to track and represent location (mayo stand, in patient or in rubbish) of RFID-enabled towels during operation.
Section 2—UI Detail		
1. What is the *user problem* the user interface is there to solve?		
The user problem is the challenge of keeping track of how many towels are in use at any one time (and their specific location, i.e., on a mayo stand, in the patient, disposed of) so to ensure no towels are left within the patient on completion of the operation.		
2. Provide a *functional* overview of the user interface.		
• Track and represent location of towels as in one of three locations: On Mayo Stand, In Patient, In Rubbish. • Highlight the number of towels in the patient. • Highlight if any towels are considered in "missing" state (i.e., the number of total towels in the system is more than the sum of numbers at the three locations) • Track and represent total number of towels in system. • Edit antenna location details and frequency • Reset system		
3. Provide a *profile* of the user group(s), include relevant demographic and other details.		
Operating theatre staff (doctors (sterile), sterile nurse, non-sterile nurse). Mixed ages from approx. 22 to 65 with range of technical experience.		
4. What is the *location* of use?		
In Operating Theatre on iPad for interaction by non-sterile nurse. In Operating Theatre on large format display (e.g., large screen on wall), non-touch interactive visualization for sterile staff.		
5. How is it anticipated that the demographics and locations identified in points 3 and 4 impact the user interface requirements (if at all)?		
Being in the location Operating Theatre, interaction may be at a distance from user therefore requiring a large format "glanceable" UI where the information visualization is more important than the interaction capability. Plus there will be sterile requirements which would impact (and likely prohibit) how sterile staff could directly interact with the UI.		
6. What *hardware and software platform(s)* are involved in the user interface and how do they impact user interface requirement? *For example physical dimensions, sensors, input devices (gesture, touch, etc.) provide boundaries, what are the impact they impose?*		
Large-format display is needed for visualization although direct interaction with the UI will be through a secondary display and keyboard/mouse and/or an iPad app (where the UI on the large format screen is mirrored).		
7. Who from the user groups identified above have you talked to? If you have additional/alternative insight into the users please provide details.		
Operating theatre staff including surgeons and nurses have been interviewed. Observations of current practice as to how towels (and other surgical equipment) are tracked throughout an operation have been undertaken.		
8. How do you plan to evaluate the quality of your user interface with your users? *For example interviews, focus groups, user trainings (how many), mockup testing.*		
Mockup testing and user training will be undertaken with appropriate medical staff to evaluate the UI components.		
Section 3—User Interface Navigation Architecture		
See Fig. 6.4.		
Section 4—Graphical User Interface Screenshots		
See Fig. 6.3.		

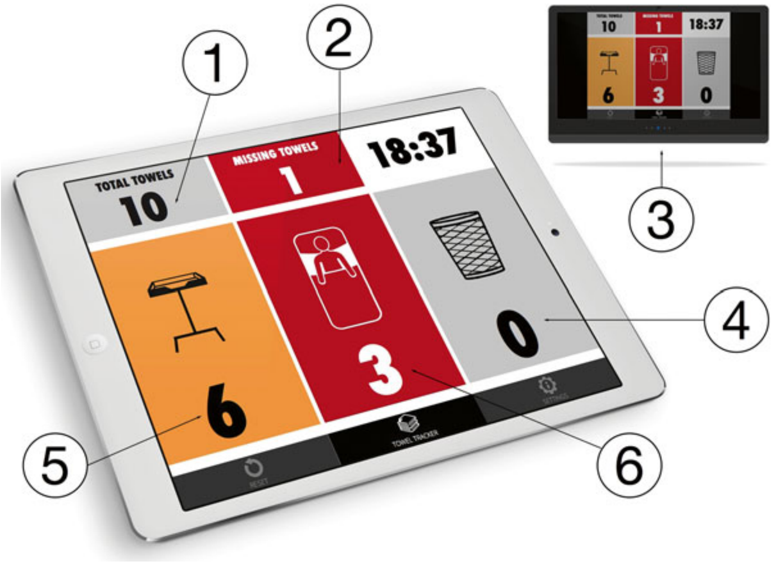


Fig. 6.3 iPad and large-screen UI for RFID-enabled towel tracker application

as they move through their operational life cycle from package to mayo stand to patient to trash. The central purpose is to answer one primary question: "Are there any towels in the patient?" A secondary question to be answered being "do we know where all the towels are." Resolving these key user problems led to the simple but clear UI design which allows operating theatre staff to know at all times the answers to those questions with a simple glance. The architecture and navigational flow of the application (shown in Fig. 6.4) also follows this simplicity in presentation whilst maintaining the functional requirements of resetting the tracker alongside adding/editing antenna settings.

Using the UCD report template with screenshots and navigational wireframe proved a great success for communicating the UCD findings, requirements, and design rationales within the design and development team of the application. It also helped communicate the functional and UX benefits to medical personnel involved in the trials and other external stakeholders within the hospital infrastructure.

6.4 Summary

UX design is concerned with all the issues that go into providing an engaging and enjoyable experience for people in both the short and longer term. This includes aesthetics, pleasure, and emotional engagement in terms of both the product and the service provided. In particular it is important to consider experiences at a physical, behavioral, and social level and in terms of the meanings people derive from their

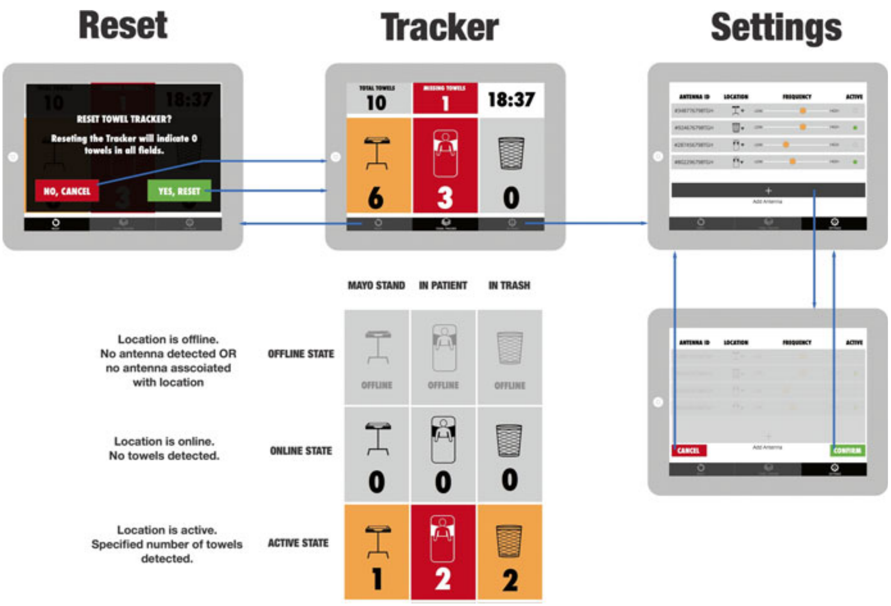


Fig. 6.4 Wireframe overview of UI for RFID-enabled towel tracker application architecture and navigation

experiences. To achieve a great UX we recommend integrating user-centered design methods into development practice in order to:

1. Focus on *real* end users
2. *Validate* requirements and designs
3. Design, prototype, and develop *iteratively*
4. Understand and design for the *holistic* user experience

This can be achieved by following these steps:

Understand the User (Phase 1):

- Observe and understand the users and their needs through focus groups, interviews, and field studies.

Define the Interaction(s) (Phase 2):

- Evaluate and refine into user profiles, work activities, and user requirements.
- Define the interactions by translating user work activities associated with user requirements into goal-driven, interactive, step-by-step use cases.
- Validate with end users.

Design the User Interface (Phase 3):

- Create low-fidelity design prototypes to translate user requirements into design concepts.

- Undertake iterative user evaluation and design refinement.
- Create high-fidelity design prototypes that mimic complete design functionality as closely as possible.
- Undertake iterative user evaluation and design refinement.
- Review UI design for both quality and compliance with UI standards.

Develop and Deploy:

- Develop, incorporating early end-user consideration as much as possible.
- Test and debug.
- Deploy.

As Neilson and others have stated many times, the application of a UCD approach increases the likelihood of a high-quality UX as well as saving money during the development process [10, 12]. More than that, UCD enables and actively encourages insight into user needs and requirements from which the next generation of products, services, and devices will be derived; as such there is arguably no area in which this process is more important than the medical domain.

References

1. Shedroff N (2001) Experience design. New Riders, Indianapolis
2. McCarthy J, Wright P (2004) Technology as experience. MIT Press, Cambridge, MA
3. Jordan P (2000) Designing pleasurable products: an introduction to the new human factors. Taylor and Francis, London
4. Norman DA (2004) Emotional Design: Why We Love (or Hate) Everyday Things. New York: Basic Books
5. Hassenzahl M (2007) Aesthetics in interactive products. In: Schiffersteign H, Hekkert P (eds) Produce experience. Elsevier, Amsterdam
6. Research and Markets (2013) North American Healthcare IT Market by Application Delivery Mode & Component—Forecasts to 2017. Available online at http://www.researchandmarkets.com/research/hzq965/north_american
7. Bond R, Finlay D, Nugent C, Moore G, Guldenring D (2014) A usability evaluation of medical software at an expert conference setting. J Comput Methods Programs Biomed 113(1): 383–395
8. Esfandiari N, Babavalian M, Moghadam A, Tabar V (2014) Review: knowledge discovery in medicine: current issue and future trend. Expert Syst Appl 41(9):4434–4463
9. Martínez-Pérez B, Torre-Díez I, Candelas-Plasencia S, López-Coronado M (2013) Development and evaluation of tools for measuring the quality of experience (QoE) in mHealth applications. J Med Syst 37(5):1–8
10. Macaulay C, Sloan D, Jiang X, Forbes P, Loynton S, Swedlow JR, Gregor P (2009) Usability and user-centered design in scientific software development. IEEE Softw 26(1):96–102
11. Nielsen J (2008) Return on Investment (ROI) for Usability, 4th Edition, Nielsen Norman Group
12. Saffer D (2009) Designing for interaction, 2nd edn. New Riders, Indianapolis
13. Benyon D, Mival O (2008) Human-centered design of interactive services. In: Proceedings HCI 2008, Manchester, Sep 2008
14. Norman DA (2002) Emotion and design: attractive things work better. Interact Mag ix(4): 36–42

15. Lavie T, Tractinsky N (2004) Assessing dimensions of perceived visual aesthetics of web sites. Int J Hum Comput Stud 60(3):269–298
16. Crampton-Smith, G. (2004) Transferring Design Research to the Marketplace‘ in Bridging Concepts: Developing the Interface between Design, Education and Industry, EDF, Glasgow
17. Gayer G, Petrovitch I, Jeffrey RB (2011) Foreign objects encountered in the abdominal cavity at CT. Radiographics 31(2):409–428

Chapter 7
Identifying Security Requirements and Privacy Concerns in Digital Health Applications

Gerd Stefan Brost and Mario Hoffmann

Abstract Security and privacy by design are important paradigms for establishing high protection levels in the eHealth domain. This means that security requirements and privacy concerns are considered and analyzed from the very beginning of any system design. For a reliable and robust system architecture and specification we recommend a four-step approach: (1) Decompose the system and identify the assets on the basis of the multilateral security concept, i.e., taking all participants of an eHealth scenario as potential attackers into account; (2) evaluate threats based on STRIDE for a holistic and systematic modelling of threats; (3) define use case-specific security requirements and privacy concerns as well as their relevance; and (4) mitigate threats by deciding what countermeasures should be implemented. After the introduction of each step this chapter illustrates the practical use in a step-by-step walkthrough with a real-world eHealth scenario and discusses advantages of security and privacy by design as well as its limitations.

7.1 Introduction

The healthcare sector has entered the digital age. Users of mobile healthcare devices and services no longer only monitor and analyze stress level, heartbeat, and blood glucose but also maintain detailed health diaries in the Cloud and share experiences with social communities—in March 2013 a study counted 97,000 mHealth applications [1]. Biosensors communicate with your watch, your watch with your smartphone, and your smartphone with healthcare services or communities [2]. Health cards have been introduced for storing individual diagnoses and medication and supporting not only administrative processes between patients, doctors, hospitals, pharmacies, and insurances but also emergency cases if allergies have been indicated on the card. Telemedicine and the exchange of large genome data sets take advantage of broadband connections and Cloud infrastructures. Healthcare has become an

G.S. Brost • M. Hoffmann (✉)
Fraunhofer AISEC, Munich, Germany
e-mail: gerd.brost@aisec.fraunhofer.de; mario.hoffmann@aisec.fraunhofer.de

S.A. Fricker et al. (eds.), *Requirements Engineering for Digital Health*,
DOI 10.1007/978-3-319-09798-5_7

important application domain of the Internet of Things and Services with a growing demand for research and development for example to support patient's self-management or provide Cloud-enabled platforms for individualized personal healthcare services.[1]

Information systems that are operated in a digital health context, however, have an intrinsically strong need for information security, since patient data is considered to be very sensitive in many contexts. This affects in total seven application categories according to [3] (1) education and awareness, (2) helpline, (3) diagnostic and treatment support, (4) communication and training for healthcare workers, (5) disease and epidemic outbreak tracking, (6) remote monitoring, and (7) remote data collection. For a detailed security evaluation in one of such application categories the parties involved as well as the assets to be protected have to be identified. Then typical threats, such as misuse, spy out, deny, misinform, divert, and tamper, can be applied and provide the common starting point to a detailed security evaluation.

User trust in an eHealth system is one of the central aspects [4]. Without sufficient trust, only few users are willing to enter their personal data into a system or use it for transmission and processing of their patient data. The effects of user's perception of system security and privacy concerns have been studied in [5] and have proven to be measurable. Security and privacy considerations must go hand in hand with the overall design. Only adequate security and privacy-enhancing technologies integrated in the design phase and implemented in systems can help establishing a certain level of trust.

Trust can be ephemeral and one security incident can cause the whole user base to mistrust a system. Once lost, it can be hard or impossible to gain it back.

Regarding this, security engineering has direct impact onto system design, since good security engineering is mandatory to create a trustworthy system. The security engineering process accompanies the system design and starts with defining security requirements. This can even affect the overall system functionality and user experience if strict security requirements have to be enforced. A late change in this kind of requirements can have an impact as hard as a late change in fundamental functional requirements.

Security experts, on the one hand, complain the fact that the analysis of implications to security and privacy still only follows—if any—the functional realization of eHealth solutions. For most parties in the healthcare ecosystem security requirements, protection goals, and threats remain abstract and risks of security incidents are not taken seriously into account. The investment in a security and privacy by design approach [6], on the other hand, can save money if properly implemented. Typically, in case of an incident reputation loss, recovering a compromised system, and integrating security mechanisms afterwards lead to much higher invests.

[1] In order to get an overview about EU-funded projects in FP6 and FP7 visit the EU PHS Foresight project (http://www.phsforesight.eu/). A good starting point for further search is the EC's website "eHealth and Ageing" (https://ec.europa.eu/digital-agenda/en/living-online/ehealth-and-ageing). Future European funding opportunities can be found at http://ec.europa.eu/research/participants/portal/desktop/en/home.html; example: H2020-PHC-2014-2015.

This chapter aims at providing a guideline for designers and practical security engineers of eHealth ecosystems as Sect. 7.2 explicates in detail. This includes how to conduct a threat analysis, define protection goals, and analyze your specific risks. Section 7.3 elaborates a concrete example of security engineering for a real-world digital health application. The discussion in Sect. 7.4 illustrates the limitations, costs, and benefits of a security engineering process, i.e., what can be achieved and what not. Finally, we conclude the key findings of this book chapter in Sect. 7.5 in order to highlight the arguments for security and privacy by design.

7.2 A Guideline for Practical Security Engineering

In order to structure the security engineering process we follow the holistic concept "multilateral security." Here, multilateral security means taking into consideration the security requirements and privacy concerns of all parties involved in the eHealth scenario that needs to be analyzed. It also means considering all involved parties as potential attackers. Not all parties are in favor of this approach but it includes the case that security incidents can be caused unintended as well as the case of malicious insiders. This is especially important for open communication systems, such as complex health ecosystems, as one cannot expect the various parties to trust each other [7].

In order to follow the multilateral security concept robust security design requires that the protection goals are made explicit [8]. They serve to protect assets and shape the security engineering process. So, in security engineering for a specific system it is a good starting point to get a thorough understanding of what protection goals are relevant for system design and which aspects need to be covered. They could be interpreted as a set of requirements for the security engineering process itself.

7.2.1 Security and Privacy Protection Goals

While designing an information system, it is useful to bear certain security goals in mind. As general building blocks of information security, three concepts are popular and serve as security goals when designing or evaluating information systems [9]:

Confidentiality: Confidentiality is the assurance that access controls are enforced and information is not disclosed to entities that they are not meant for. It is one of the core goals when dealing with sensitive information. Achieving confidentiality requires defining what information is to be considered as confidential, then to secure all exposed communication channels, and to store information in a secure way as well as other means to avoid leakage of this data. Without it, sensitive data would spread around.

Integrity: The concern when dealing with integrity is to make sure that data is protected from unauthorized modification or deletion. This can be expanded to an undo-functionality to revert illicit changes. It is important to achieve integrity to avoid these changes. Loosing integrity means making information in a system not to be trusted.

Availability: This goal aims to achieve continuous accessibility of relevant data and operation of the system. A system without sufficient availability will be neglected by users. Disrupting availability is a popular method to break system functionality (e.g., with denial-of-service attacks).

This core model is simple, robust, and served for many years. However, limitations became apparent. Ongoing discussion is concerned if and how to extend this model. Other properties or goals that are often used are [10]:

Authenticity: The property that information is authentic and coming from a person that is guaranteed to be the one it claims to be. Without authenticity, it is possible to have secret data transmissions, but it is not sure who that information comes from.

Non-repudiation: This is a property motivated by legal considerations. It implies one intention to fulfill their obligations to a contract. Not having non-repudiation makes it hard to fulfill certain legal standards. Users, e.g., could repudiate statements of will.

Another set of properties comes from recent discussion of privacy and is called privacy protection goals. Considering we are dealing with eHealth systems, privacy appears to be one of the most important goals. Important privacy goals are [11]:

Unlinkability: Unlinkability ensures that privacy-relevant data cannot be linked across privacy domains or be used for a different purpose than originally intended. This can be achieved by, e.g., early erasure, anonymization, or pseudonymization. Anonymization means removing identifying properties from data (e.g., removing the name of a person). Pseudonymization means the replacement of these properties with something less identifying, but reversible (e.g., replacing the name with a number).

Transparency: Transparency is one of the cornerstones of every modern privacy-oriented system and has found its way in some legislation. To achieve this, an adequate level of clarity of processes is necessary and brought to the user. This has also an important impact in user trust, since trust will hardly be achievable with a non-transparent system.

Intervenability: To achieve intervenability, data subjects and operators must be able to interfere with planned or ongoing privacy-related data processing.

The privacy goals are an important aspect of generating trust into a system, both on the technical and legal layer.

Protection goals in general are a direct reaction to threats. In order to understand and model these threats we recommend following the STRIDE[2] model. It has been

[2] http://msdn.microsoft.com/en-us/magazine/cc163519.aspx

defined by Microsoft in 2005 and has been established in many application domains already. The key aspects of STRIDE are:

S—Spoofing: "An example of identity spoofing is illegally accessing and then using another user's authentication information, such as username and password."

T—Tampering: "Data tampering involves the malicious modification of data. Examples include unauthorized changes made to persistent data, such as that held in a database, and the alteration of data as it flows between two computers over an open network, such as the Internet."

R—Repudiation: "Repudiation threats are associated with users who deny performing an action without other parties having any way to prove otherwise—for example, a user performs an illegal operation in a system that lacks the ability to trace the prohibited operations."

I—Information disclosure: "Information disclosure threats involve the exposure of information to individuals who are not supposed to have access to it—for example, the ability of users to read a file that they were not granted access to, or the ability of an intruder to read data in transit between two computers."

D—Denial of service: "Denial of service (DoS) attacks deny service to valid users—for example, by making a Web server temporarily unavailable or unusable. You must protect against certain types of DoS threats simply to improve system availability and reliability."

E—Elevation of privilege: "In this type of threat, an unprivileged user gains privileged access and thereby has sufficient access to compromise or destroy the entire system. Elevation of privilege threats includes those situations in which an attacker has effectively penetrated all system defenses and become part of the trusted system itself, a dangerous situation indeed."

In order to illustrate STRIDE in the following subsections we decompose a simplified health care system into relevant components, analyze each component for susceptibility to the threats, and try to mitigate the threats. According to the STRIDE model, then, you need to repeat the process until you are comfortable with any remaining threats. Alternatively, a cost and risk analysis can help to quantify and qualify the remaining threats in order to take a decision whether all threats have to be mitigated. Note: There is no 100 % security.

7.2.2 Security Engineering Process

In order to deal with possible threats concerning a system and its assets, the following steps are taken:

Figure 7.1 gives an overview of the security engineering process. In step 1, the application that is analyzed is decomposed. Based on this decomposition, relevant assets for the threat evaluation are determined. In step 2, threats are determined that can affect the assets. Misuse cases can help to see the "other side" by changing the perspective to that of an attacker. Misuse cases can be used to gain a better

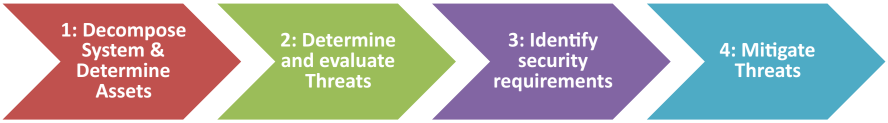

1: Decompose System & Determine Assets
2: Determine and evaluate Threats
3: Identify security requirements
4: Mitigate Threats

Fig. 7.1 Security engineering process

understanding of attack scenarios. In step 3, starting with the selection of security goals, appropriate security requirements are identified and described. The security requirements are the baseline for threat mitigation decisions in step 4. We will take a brief look on these steps, before demonstrating them on a real-world example in the next section.

7.2.2.1 Decompose System and Determine Assets

Since we deal with security engineering that accompanies the development process, we have access to software design documents like architecture diagrams (e.g., UML Component Diagrams and Collaboration Diagrams) or use case descriptions. These are then used to gain an understanding of the outer and inner workings of the system and help to identify assets and data flow patterns. Assets and data flow patterns are important for identifying protection mechanisms later on.

Assets are objects with direct and indirect value. A direct value, e.g., would be the monetary value of a server machine. An indirect value, e.g., would be the money that could be gained by selling patient data.

These assets can be furthermore divided into tangible assets (like Smart Cards, Desktop Computers or Servers) and intangible assets (like patient data or a PIN code). Tangible assets may be physically stolen or destroyed. Intangible assets may also be stolen by copying them or deleting them from disk.

Many risk assessment models require the quantification of an asset's value. This is often hard to measure. While the loss of a server machine is easy to quantify, the financial impact of losing reputation and user trust due to leaked personal information is quite difficult to put into numbers. When dealing with intangible assets, e.g., data, it is often more practical to identify channels and data sinks where sensitive data are transmitted and stored and secure those with adequate means.

7.2.2.2 Determine Threats

To determine treats do the identified assets; it helps to define misuse cases that accompany the system's relevant use cases.

Abuse/misuse cases [12,13] help to change the perspective by accompanying every use case of the system with appropriate misuse cases. So when a user is signing in at the system to access his data, an attacker might try to feign authentication

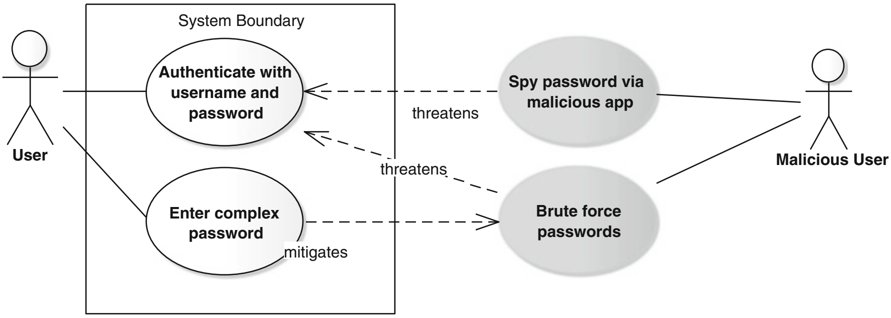


Fig. 7.2 Authentication misuse case diagram (*white*: use case, *grey*: misuse case)

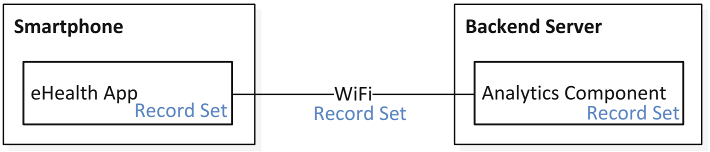


Fig. 7.3 Simplified system diagram

and access the data without proper rights to do so. It is helpful to reduce the usage to central misuse cases that do not descend into unnecessary design and architectural constraints. Figure 7.2 depicts a very simple misuse case diagram, where a malicious user attempts to brute force the user's password. This could be mitigated by choosing a complex password.

After getting a better understanding of the system (and the use cases and misuse cases), a threat analysis is performed to cover as many attack angles as possible so that a complete set of security requirements can be derived. To define threats for a system, it is necessary to choose an attacker model.

In formal protocol verification, the first step would be to choose an attacker model. The most prominent would be the Dolev-Yao attacker model [14]. The properties of these models are often a problem and have always been a point of discussion [15]. Choosing an attacker model is still a necessary prerequisite for threat analysis. This includes which channel the attacker can read and what tools he has. In practical work, choosing a powerful but realistic attacker produces the most benefit. To narrow the scope of the analysis, it often makes sense to exclude components that are not part of the current project. For example, the hospital backend already deals with highly sensitive information and might be excluded. This changes, however, when the usage of such a system is altered. An example would be if a closed data storage component is attached to the Internet and used for external communication.

As stated before, modeling data sinks and communication channels grounds on system decomposition and is the baseline for threat analysis.

Figure 7.3 shows a highly simplified overview of an eHealth App with a connection to the backend. It is a simplified version of a deployment diagram enriched with

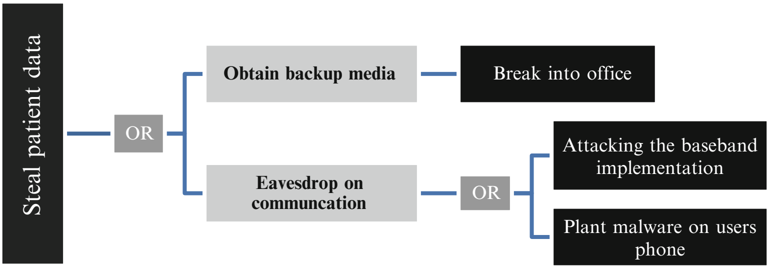

Steal patient data
OR
Obtain backup media
Break into office
Eavesdrop on communcation
OR
Attacking the baseband implementation
Plant malware on users phone

Fig. 7.4 Sample attack tree (*black*: root or leaf leading to sub-tree, *light grey*: node)

data that is stored and transmitted. Analyzing such architecture instantly makes clear that patient data is stored in the backend and on the user's smartphone as well as transmitted between those two. From this it is possible to derive attacks on the components and communication channels that aim to block, read out, or even modify communication.

To gain a better understanding of possible attacks on these assets and to avoid missing relevant attacks, the creation of attack trees is a common practice. Let us take a look at the example that an attacker wants to steal patient data. The root of each tree is the attack goal (e.g., steal patient data), where the nodes lead down to specific attacks (e.g., breaking a weak WLAN encryption to sniff user data).

In Fig. 7.4 we show an exemplary attack tree with possible sub-threats related to the outcome of stolen patient data. These attack trees can be broken into sub-trees. In this example, all three sub-threats need further detailing, resulting in a sub-tree for each. More detailed information about attack trees can be found in [16].

It is common practice to use formulae to calculate values for risks. This is a quantitative approach with a certain justifiable charm. Formulae to evaluate threats are mostly designed in a way similar as it is depicted in the following formulae:

$$\text{Risk} = \text{Likelihood} \times \text{Damage}$$

$$\text{Likelihood} = \frac{\text{Sophistication Level} + \text{Difficulty of Implementation}}{2}$$

$$\text{Damage} = \frac{\text{Financial Severity} + \text{Casual Severity} + \text{Privacy Loss}}{3}$$

Depending on the scenario, these formulae can get very complex and tend to produce rankings that are hard to verify or to understand.

Advantages and disadvantages for quantitative and qualitative approaches are shown in [17]. We will present a hands-on, qualitative approach (Table 7.1).

Table 7.1 Advantages and disadvantages of risk analysis methods

Quantitative methods	Qualitative methods
Advantages	
Applicability to all assets	Simple risk calculation
Mathematical foundation	Usefulness when asset value is irrelevant or unknowable
Using a management specific language (support cost benefit decision)	Less time consuming
Accuracy tends to increase over time as the organization builds historic record of data while gaining experience	Easier to involve people who are not experts on security or computers
Disadvantages	
Inappropriateness of monetary asset value	Coarse granularity
Inappropriateness of general statistics	Inability of cost benefit decision
Time consuming, requires much preliminary work	Subjective results, depend on quality of risk management team

Table 7.2 Threat evaluation matrix example

Attack 1: Steal user data by bruteforcing or spying on weak password			
Vulnerabilities exploited	Weak password chosen by user	Safety relevant?	No
		Component/system	Smartphone
		Attack type	Information disclosure
		Financial severity	Low
		Loss of privacy	Yes
Risk	6.00	Sophistication level	Low
Likelihood	3 (High)	Difficulty of implementation	Low
Resources required	Access to smartphone		
Attack scenario	Attacker either steals smartphone or accesses it while unattended. Weak passwords are tested or a simple pin that has been eavesdropped before is tried.		
Outcome	The attacker gains knowledge of user data.		

In a practical scenario, the security evaluation team must judge if it seems more sensible to evaluate each of the threats on its own and judge if this threat is going to be mitigated and how, or a more formal method is required using adapted formulae and threat matrixes. This choice, however, must always be made regarding the project and organizational situation.

To document the values and the qualitative aspects of an attack, such as technical details or setup requirements, threat evaluation matrixes can be used. Table 7.2 shows the evaluation of a threat resulting from a specific attack.

From this highly simplified example, we can learn that it is easy to gain access to the data a user has on his smartphone and a simple PIN protection might not be sufficient. Later on, a conclusion could be that we will need to implement mechanisms to keep user data safe.

7.2.2.3 Identify Security Requirements

The security goals we discussed are taken as a baseline for specific security requirements. It must be evaluated which of these security goals are suitable for the current system. Then requirements can be derived, by analyzing the goals and requirement categories. These requirements might be several or all of the following [18]:

- Identification requirements
- Authentication requirements
- Authorization requirements
- Immunity requirements
- Integrity requirements
- Intrusion detection requirements
- Non-repudiation requirements
- Privacy requirements
- Security auditing requirements
- Physical protection requirements
- System maintenance security requirements

We will briefly describe each requirement category. Identification means identification of entities (e.g., users or devices), whereas authentication is the process to confirm that identity. Authorization defines how a system specifies and grants access rights to resources. Immunity specifies the extent to which a system or component should protect itself from infections, e.g., from viruses. Intrusion detection covers means for a system to detect access or modifications by unauthorized entities (e.g., programs). Integrity, non-repudiation, and privacy directly relate to the security goals specified before. Security auditing means auditing status and use of security mechanisms. Physical protection defines protection against physical access, where system maintenance (in the security context) is concerned about avoiding maintenance operations colliding with security mechanisms.

To illustrate the identification of security requirements with an example: Confidentiality is the baseline for a privacy-related requirement that all patient data transmitted to the backend must be encrypted with a specific cypher (an algorithm to encrypt data).

7.2.2.4 Threat Mitigation

When the system is being designed in a way to mitigate a threat, it needs to be decided what countermeasures should be installed. Here, financial impact (cost), impact on usability, impact on performance, and threat severity need to be weighed against each other to make a choice. Security, usability, and performance are factors that influence each other. Many highly secure authentication mechanisms reduce usability (e.g., always carrying a smart cart and presenting it to the smartphone with a user password) or performance (e.g., a highly secure, but bandwidth consuming transfer protocol).

Documents with recommendations on what cryptographic methods, algorithms, and key lengths to use like [19], [20], or [21] are valuable tools for this task. These guidelines help decide about technical or organizational security means without having to be too familiar with all elements and the most recent attacks.

If the effort to mitigate a threat exceeds the possible budget or the usability decrease in doing so would be reduced as much to make the system unusable, it might be necessary to recommend alternative system designs that avoid that threat.

7.2.2.5 Summary

We discussed necessary steps for the security engineering process. The steps for verifying the security design like penetration testing are not part of this description. In the next section we will apply it on a realistic use case and discuss short examples of how these steps can be performed.

7.3 Example of Security Engineering for a Real-World Digital Health Application

To illustrate the security engineering process, we picked a real-world example for an eHealth system. We are discussing the diabetes share system, which has been designed as part of the FI-STAR project.

> The Diabetes Share System (DSS) is intended for patients, next-of-kin (e.g. relatives), physicians, and nurses who train, monitor, and consult an empowered Diabetes patient. DSS is a FI-STAR cloud solution that enables mobile recording of health and biometrical parameters, remote counselling, and comparison with other patients' anonymous observations. Unlike in-clinic treatment based upon manually recorded or lacking health parameters, DSS increases evidence to support treatments, increases the patient's knowledge base, assists in maintaining a healthy lifestyle, reduces the number of in-person appointments, and improves the patient's diabetes condition, wellbeing, and health. [22]

We will illustrate the security engineering process step by step with details taken from this example, following the steps briefly explained in the section before.

7.3.1 Decompose System and Determine Assets

In this step, we take design documents and architect input for the software design phase and try to decompose the system in a way that we can get an understanding of the assets and data flow in the system.

Figure 7.5 shows a component diagram from the DSS example. Patient data is transmitted over component boundaries and processed in remote locations. Diagrams

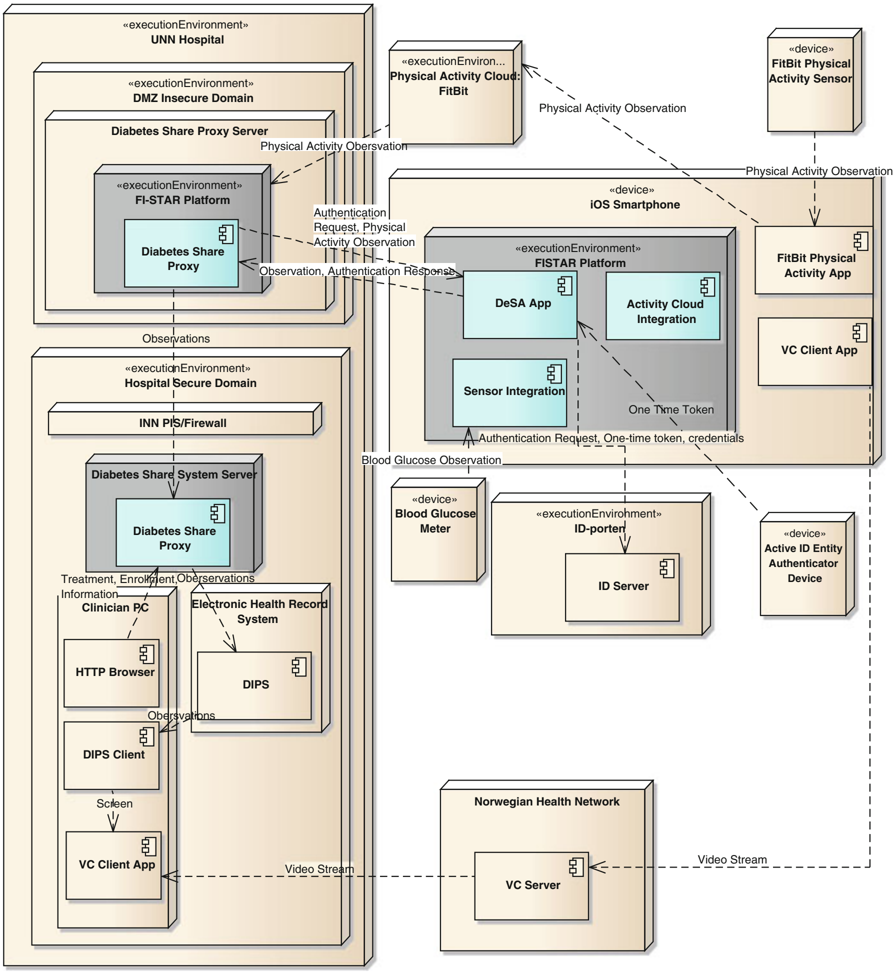


Fig. 7.5 Real-world example component diagram

like this one, coming from the design team, are very useful for determining potential assets and communication channels.

Several communication channels can be identified in the figure and the most relevant ones are listed in Table 7.3.

This list of communication channels and transmitted information is an important factor to gain knowledge about assets and potential threats. However, it is necessary to not only rely on certain views on the system design. This component overview, for example, does not reveal all information about the technical realization of the system since it is just a logical view.

Table 7.3 Communication channels

	Channel between	Assets
C01	Smartphone, FitBit Cloud	Physical activity observations
C02	FitBit Cloud, Diabetes Share Proxy Server	Physical activity observations
C03	Diabetes Share Proxy Server, Smartphone	Physical activity observations
C04	Smartphone, Diabetes Share Proxy Server	Observations, authentication data
C05	Smartphone, VC Server	Video stream data
C06	VC Server, Clinician PC	Video stream data
C07	Smartphone, ID-Porten-Server	Credentials
C08	Blood Glucose Meter, Smartphone	Blood glucose observations
C09	Physical Activity Sensor, Smartphone	Physical activity observations
C10	Diabetes Share Proxy Server, Diabetes Share System Server	Observations
C11	Clinician PC, Diabetes Share System Server	Treatments, enrollment information
C12	DSS Server, Electronic Health Record System	Observations
C13	Electronic Health Record System, Clinician PC	Observations

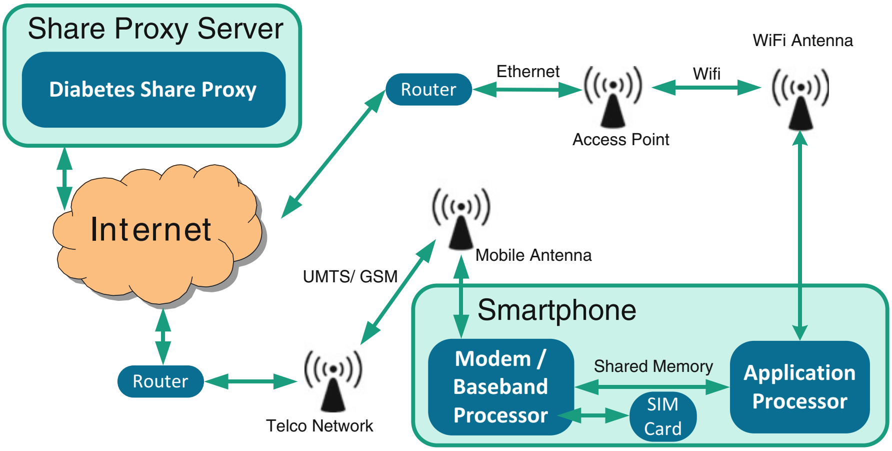


Fig. 7.6 Detailed communication scenario

Figure 7.6 is a refinement of Fig. 7.5 according to the dimension of communication network topology.

If we take a look on the communication over a smartphone, we can see that communication can be achieved over different channels and different networks. When we rely on the encryption of point-to-point-connections, it is hard to achieve overall security.

Figure 7.6 shows a more technical view on the smartphone's communication channels. Perspective is changed from a logical component or deployment diagram to a real technical decomposition. Depending on how the smartphone transmits its data (WiFi or mobile network data connections), several networks are involved.

Table 7.4 Assets

	Asset	Locations	Sensitive?
A01	Observations	Smartphone, DSS Proxy Server, DSS Server, Electronic Health Record System, Clinician PC	Yes
A02	Authentication data	Smartphone, Diabetes Share Proxy Server	Yes
A03	Video stream data	Smartphone, VC Server, Clinician PC	Yes
A04	Credentials	ID-Porten Server, Smartphone	Yes
A05	Blood glucose observations	Blood Glucose Meter, Smartphone	Yes
A06	Physical activity observations	Physical Activity Sensor, Smartphone	Yes
A07	Treatment plan	Clinician PC, DSS Server	Yes

Data leaves the phone, passes into wireless or mobile networks, and is routed into the Internet, and delivered to the hospital infrastructure. The smartphone itself is not a single component but a system of components, which can be manipulated and internal communication channels that could be eavesdropped on. It is hardly possible to take all of these details into account, but it is important to be aware of the complexity and take reasonable decisions what areas to cover. In this case it would be reasonable to care for the security of the application and its data flows, but not drilling down into securing the smartphone itself. If a project relies on components and systems that are considered to be secure, these decisions must be documented to make the rationale traceable for others.

The same is true for certain communication flows embedded in protocols. A typical example is authentication protocols. When a standard authentication protocol is used and the used protocol is considered to be secure, we can exclude transmitted data (e.g., credentials) from our asset and channel list. This decision, however, also needs to be documented.

Determining assets and analyzing data flows over the communication channels in Table 7.3 can be helpful, but is not sufficient. Data is often at rest or not transmitted at all, but still represents an asset that needs to be protected. So user data that resides on the smartphone and is not transmitted must also be protected by adequate means (e.g., by a password policy).

To identify and evaluate threats to assets, the value of those assets must be determined. A quantitative approach is often difficult, since exact amounts of damage done by data leakage and the damage resulting from bad system reputation and lost user trust are hard to measure or define. A qualitative approach can help to ease the decision what assets to protect and what level of security is needed. For this simplified example, we will just define what assets are to be considered sensitive. We will only take into account intangible assets and indirect values here, since tangible assets are either in the responsibility of the patient (smartphone) or form a component in an existing server infrastructure which is not part of this example. In this example, we consider all assets in “Table 7.4: Assets” as sensitive.

7.3.2 Determine and Evaluate Threats

Since we know what assets are present in our system and need to be protected, we can get an understanding of what approaches could be interesting for a malicious user (attacker) to use the system inappropriately.

In Fig. 7.7, use cases from the system design documents are taken and matched with misuse cases to help threat determination.

Building on misuse cases and the evaluated communication channels and assets, we can perform a classical threat evaluation, starting with attack trees. These trees provide the means for an effective and systematic approach to cover as many relevant attacks as possible. Figure 7.8 depicts a high-level attack tree, where the leaves define sub-trees. An example for that can be seen in Fig. 7.9. The attacks can be broken down until the desired granularity level is reached.

This breakdown of attacks can be performed to a level as detailed as a certain known attack, e.g., on a cryptographic algorithm. In most projects, this might not be necessary. It is sufficient in most cases that certain transmission type cannot be fully trusted. As in this example it becomes clear that there are attacks on wireless data transmission which would be a valuable input for security requirements engineering and later system design, e.g., advocating the need for end-to-end encryption of data later on.

When all relevant attacks are covered, they can be evaluated with a threat matrix. When using such a matrix, it is important to adapt it to the specific project's needs.

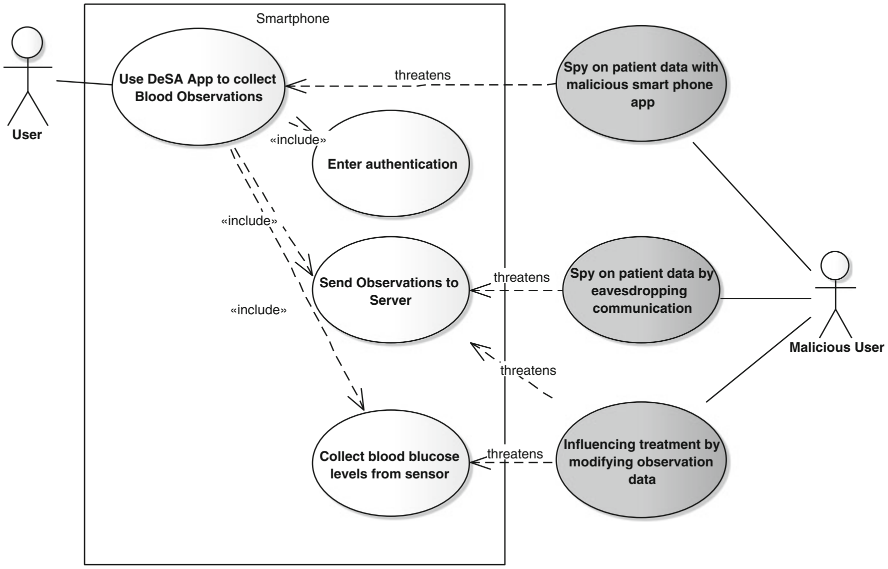
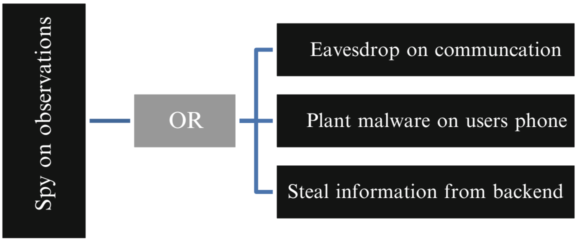

Smartphone
User
Use DeSA App to collect Blood Observations
Enter authentication
Send Observations to Server
Collect blood blucose levels from sensor
«include»
«include»
«include»
threatens
threatens
threatens
threatens
Spy on patient data with malicious smart phone app
Spy on patient data by eavesdropping communication
Influencing treatment by modifying observation data
Malicious User

Fig. 7.7 Sample misuse case diagram without mitigation

Fig. 7.8 Sample high-level attack tree


Spy on observations
OR
Eavesdrop on communcation
Plant malware on users phone
Steal information from backend

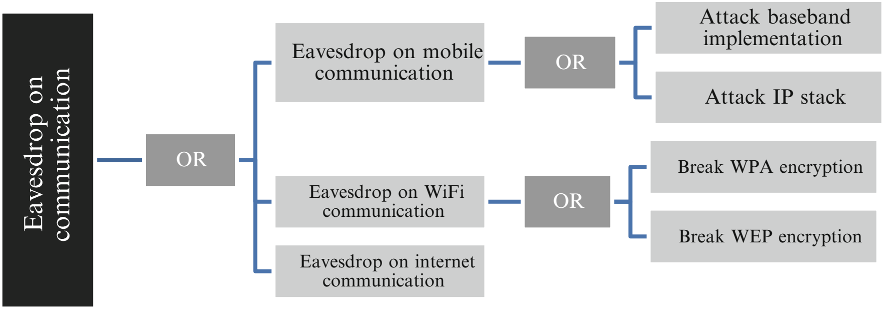

Eavesdrop on communication
OR
Eavesdrop on mobile communication
Eavesdrop on WiFi communication
Eavesdrop on internet communication
OR
OR
Attack baseband implementation
Attack IP stack
Break WPA encryption
Break WEP encryption

Fig. 7.9 Attack sub-tree

As discussed in the section before, if the formulae to calculate the risk are getting too complex, the value of the assessment becomes questionable.

Table 7.5 shows the threat evaluation for an attack on the baseband implementation of a mobile handset to eavesdrop on transmitted data.

7.3.3 Identify Security Requirements

Since we now have a good understanding of possible attacks and of the assets that are worthy of protection, we can identify relevant security requirements for our system. It is helpful to keep in mind that security requirements do not include architectural decisions for the software system. Although it is useful to state a certain level of protection for system access, the concrete type of access mechanisms is supposed to be left open for further investigations. This should be delegated to the architect and the decisions should be negotiated together. Such a negotiation process is described in [23].

As discussed before in the security engineering process description, there are a number of categories for security requirements like identification, authentication, and privacy requirements. Let us specify a few requirements that are an outcome of the threat evaluation. In this threat evaluation we realized that data could be read out by an attacker. This leads to the following privacy requirements for the DeSA application:

Table 7.5 Attack example: Eavesdropping on communication

Attack 1: Steal patient data by eavesdropping on wireless communication by attacking the baseband implementation			
Vulnerabilities exploited	Most encryption algorithms used in GSM and GPRS have weaknesses. Only the recent A5/3 algorithm can be considered as relatively secure. Regardless of the encryption algorithm GSM does not have mutual authentication and an attacker can launch a rogue base station attack.	Safety relevant?	No
		Component/system	Smartphone
		Attack type	Information Disclosure
		Financial severity	Medium
		Loss of privacy	Yes
Risk	2.67	Sophistication level	Medium
Likelihood	2 (Medium)	Difficulty of Implementation	Medium
Resources required	Standard Laptop, GSM/GPRS Base Station (Hardware and Software), frequency jammer		
Attack scenario	It is possible to eavesdrop on communication via GSM/GPRS or UMTS/LTE. Since GSM/GPRS does not have mutual authentication a rogue base station can be employed in order to attack the ATM. Either the traffic is captured directly or encryption can disabled for this GSM/GPRS communication channel. Alternatively the attacker can try to break the encryption of a GSM or GPRS channel set up by his victim and another operator. In the UMTS scenario, jamming is required to force a fallback to GSM and use the approach described above. Additionally, there are the following attack vectors: • The RRC protocols of UMTS and LTE is spoken before authentication • The attacker could try to break into a femtocell supplied by a provider		
Outcome	The attacker gains knowledge of any additional unprotected communication.		

Since we are facing communication flows over several technological domains and media, we need end-to-end security, as stated in R2. Security requirements are seldom independent from each other. When securing connections to transmit data in private, other requirements, as for identification, can be derived as in R3. Identification requirements are often not sufficient for themselves, since authentication bases on identification, as derived in R4. Also authentication requirements are most often not sufficient for themselves but need to be accompanied by authorization requirements as in R5 or R6.

When the security requirements are derived for every component, this is the baseline for the security design of the overall system. Keep in mind that until now no decisions have been made how the technical realization will look like. These decisions can now be made by the architect in consultation with the requirements engineer to shape the solution.

7.3.4 Threat Mitigation

After the security requirements have been defined, a security concept for the overall system can be created. This concept will map requirements to specific means like authentication tokens, encryption algorithms, and access control methods. We give a short outlook on how threat mitigation could be realized by countering relevant threats with technical means.

Since the evaluation of threats led to the definition of security requirements, we need to realize the system in a way that the requirements from Table 7.6 are fulfilled.

R1 and R2 can be fulfilled by not relying on inherent security mechanisms of the underlying technology (e.g., UMTS or WiFi encryption), but to provide our own end-to-end security. This could be achieved by choosing TLS (recommended is version 1.2) and proper authentication and key exchange methods. This, however, is more complicated than it seems. The selection and configuration of cipher suites is a complex topic that should only be taken care of by experienced experts in that field. Slight misconfigurations could result in a complete loss of confidentiality. For example, AES is a very-well-known symmetric encryption algorithm.[3] By choosing the wrong mode of operation or a weak generation of random numbers for the key, AES can be made totally insecure. So, experience in the field of cryptography and its application is needed to construct a secure system.

R3 requires authentication of communication partners. This could be realized by issuing soft tokens that are compliant with PKCS#11[4] (Public Key Cryptographic Standard). This, however, requires the presence of a Public Key Infrastructure (PKI). In the scenario we discussed in Fig. 7.5 id-porten is used. This is a Norwegian

Table 7.6 Derived security requirements

Requirement ID	Short description
R1	The DeSA application shall not allow unauthorized individuals or programs access to transmitted data that flows between components.
R2	Communication that flows over several technological barriers or components must be secured end to end.
R3	The DeSA application must identify other valid communication partners before transmitting data.
R4	The DeSA application must verify the identity of each communication partner before transmitting data.
R5	The DeSA application shall allow the successfully authenticated Diabetes Share Proxy access to Observations the user authorized for transmission.
R6	The DeSA application shall not allow any other entity to access Observations.

[3] http://www.ijcset.net/docs/Volumes/volume1issue3/ijcset2011010306.pdf

[4] http://www.emc.com/emc-plus/rsa-labs/standards-initiatives/pkcs-11-cryptographic-token-interface-standard.htm

identification portal[5] with different authentication levels. R4 mandates that these identification tokens are not only available but also actually verified in the software. R5 and R6 require the selection of an access control model (e.g., mandatory access control) and a definition of access rights. This could be realized by choosing RBAC (role-based access control).

These decisions are complex and entail many details that need to be defined. Fortunately these tasks are similar in many different projects and a lot of guidelines and standards are available as, e.g., [20] or [21].

Some technological solutions are highly secure, but would ruin user acceptance. The use of smart cards is well understood and could be realized with modern smartphones that could connect to the smart card wirelessly over NFC (near-field communication). The usability drops dramatically, though. This is where user acceptance and usability engineering come into play to determine a realistic solution. One example would be the design of a mechanism that requires the presentation of the smart card only for specific operations. If accessed normally, the user is only required to enter a PIN.

For other components, it is not possible to actively influence the security levels. For user smartphones, for example, certain risks will always remain (e.g., malware) and maybe made worse through rooting the phone through the user. In this case, all we can do is to inform the user (relating to transparency) as best as possible. The same is true for the identification service. We can only decide if we want to trust id-porten or not. We can base our decision on security evaluation reports and certifications to make it justifiable, however.

7.4 Discussion

We gave an overview of a security engineering process to define and elicit security requirements.

Another important component to achieve security of a system is a security evaluation of the system and the verification of security requirements. Where other nonfunctional requirements as performance can be verified by load tests, it is possible to implement security tests to verify security requirements. This should be accompanied by specific penetration testing efforts. Penetration testing reverses the role of an engineer to that of an attacker. This is comparable to the design of misuse cases, where the user role is converted into a misuser or attacker role. Security must also be a part of managing change requests, since modifications of the source code without a specific focus on security can break security mechanisms easily.

We presented a comprehensive process for security engineering in a software system with distributed components, which is hands-on and inspired by practical experiences.

[5] http://eid.difi.no/nb/id-porten

However in reality, the security engineering process is not as linear as depicted. It is more an iterative approach where some requirements are detailed early in the project and some other relate to technical or organizational framework conditions that come up later in the project. So every process step has feedback loops with the other steps and the requirements need some time to stabilize. Some aspects of the process steps need to be customized for each project.

One huge driver of project effort can come from threat evaluation. The methodology to evaluate threats and represent these with hard numbers or at least qualitative values can grow very complex, making it hard to maintain and to verify. Complex formulae tend to have an esoterical touch for other project participants and make traceability hard, as well as the justification for technological measures, which directly increase cost. Reducing the complexity to a purely qualitative evaluation can make it also harder to justify decisions since for external readers, the results may appear less founded. Documentation is a key aspect to not loose important information on the way.

This evaluation, as well as the threat assessment matrices, needs to be customized to the project needs. There might be different needs for safety or financial losses and this should be reflected in the evaluation. Also the level of complexity for the threat evaluation formulae needs to be adjusted, where some regulatory or legislative requirements can demand a certain level of detail.

Another aspect that needs to be defined is the definition of protection levels. It would be possible to define certain levels and attach them to technological and organizational means. In simpler projects, it might be sufficient to define one level for the whole system.

An issue that is still not solved in a satisfactory manner is how to find the right trade-offs between security, usability, and performance. Each goal can be achieved on its own. Balanced combinations are subject for further research.

Regarding threat evaluations, there are multiple models and numerous variations of the exact process (e.g., remember the discussion of quantitative and qualitative approaches). It would be very helpful to evolve towards a framework where such decisions are covered and are made easier for security engineers.

7.5 Conclusion

This chapter has introduced security and privacy by design as a driving paradigm to realize reliable and trustworthy eHealth systems. In order to break down this paradigm to concrete security methods and technologies for use cases in eHealth a comprehensive requirements engineering process has been illustrated and applied. The conceptual basis is called "multilateral security" where all participants of a specific use case, e.g., patients, physicians, and third-party service providers, are considered as potential attackers. This is important for taking any kind of possible attack vector into account—no matter an attack is intended or by accident. Single attack vectors can then be reflected according to use case-depending protection goals. Typical security goals are confidentiality, availability, and integrity; we recommend, however, to consider additional privacy goals such as unlinkability, transparency, and intervenability in order to specify a well-balanced system design.

The threat analysis that we have proposed supports designers and developers of eHealth systems to meet all of their protection goals. Following the STRIDE model we illustrated four important phases: (1) decompose system and determine assets, (2) determine and evaluate threats, (3) identify security requirements, and (4) mitigate threats. How these phases should be applied from our point of view is described step by step in a concrete example of a diabetes share system, which has been designed as part of the FI-STAR project.

From the discussion we, finally, derived that the engineering of security requirements is not a job for an isolated team, but requires constant communication between system architects and security engineers. The security engineering process accompanies the whole system development. Analyzing the security requirements and privacy concerns in the design phase, thus, is just one but important step in the complete security development life cycle.

References

1. Research2Guidance (2013). Accessed on 1 May, 2014, from http://research2guidance.com/the-market-for-mhealth-app-services-will-reach-26-billion-by-2017/
2. Lymberis A, De Rossi DE (2004) Wearable eHealth systems for personalised health management: state of the art and future challenges. Ios Press, Amsterdam
3. Vital Wave Consulting (2009) mHealth for development: the opportunity of mobile technology for healthcare in the developing world. United Nations Foundation, Washington, DC
4. Ruotsalainen P, Blobel B, Seppälä A (2012) A conceptual framework and principles for trusted pervasive health. J Med Internet Res 14:e52
5. Hsu C-L, Lee M-RS-H (2013) The role of privacy protection in healthcare informatipn systems adoption. J Med Syst 37(5):1–12
6. Cavoukian A, Chanliau M (2013) Privacy and security by design: a convergence of paradigms
7. Müller G, Rannenberg K (2004) Multilateral security in communications. Addison-Wesley, Reading, MA
8. Anderson RJ (2008) Security engineering: a guide to building dependable distributed systems. Wiley, New York, NY
9. McCumber J (1991) Information systems security: a comprehensive model. Proceedings of the 14th national computer security conference, Washington, DC, 1–4 October 1991
10. Zhou J, Gollmann D (1996) Observations on non-repudiation. In: Advances in cryptology. Springer, New York, NY
11. Hansen M, Probst T (2012). www.datenschutzzentrum.de. Accessed on May 2014, from https://www.datenschutzzentrum.de/guetesiegel/Privacy_Protection_Goals_in_privacy_and_data_protection_evaluations_V05_20120713.pdf
12. McDermott J, Fox C (1999) Using abuse case models for security requirements analysis. 15th Annual computer security applications conference. Phoenix, Arizona
13. Sindre G, Opdahl A (2005) Eliciting security requirements with misuse cases. Requir Eng 10:34–44
14. Dolev D, Yao A (1983) On the security of public key protocols. In: Information theory. IEEE, Washington, DC, pp 198–208

15. Roscoe, B. (2003). The attacker in ubiquitous computing environments: formalising the threat model. Proc. of the 1st Intl workshop on formal aspects in security and trust, Italy
16. Schneier B (1999) Attack trees. Dobb J 24:21–29
17. Tatat Ü, Karabacak B (2012) An hierarchical asset valuation method for information security risk analysis. International conference on information society, 25–28 June 2012, London, pp 286–291.
18. Firesmith DG (2003) Engineering security requirements. J Obj Tech 2:53–68
19. BSI (2014) Kryptographische Verfahren: Empfehlungen und Schlüssellängen.
20. ENISA (2013) Algorithms, key size and parameters report
21. Barker E, Roginsky A (2011) Transitions: recommendation for the use of cryptographic algorithms and key lenghts. NIST, Gaithersburg, MD
22. Fricker S, Thümmler C (2014) Technical requirements and architecture report including open call requirements. Technical Report. Accessed on 1 May, 2014, from https://bscw.fi-star.eu/pub/bscw.cgi/d42532/D1.1_R1.pdf
23. Fricker S, Gorschek T, Byman C, Schmidle A (2010) Handshaking with implementation proposals: Negotiating requirements understanding. *IEEE Software* 27(2):72–80

Chapter 8
How to Elicit, Analyse and Validate Requirements for a Digital Health Solution

Mojca Volk, Niklas Falk-Andersson, and Urban Sedlar

Abstract This chapter outlines the challenges and the requirements engineering practices we used to address these challenges in the form of a cookbook. The material is intended for RE practitioners, researchers as well as digital health stakeholders, and is prepared as a set of practical guidelines and recommendations, further explained through a specific real-world case of a digital health application developed in cooperation between industry partners and health providers. It covers an overview of the requirements engineering background and the stakeholders specific to digital health, identifying in particular patients, medical personnel and regulators as the crucial actors in digital health RE; and it explains the concrete steps needed to bridge the gaps and engage them throughout the entire process. Next, it provides to the reader pragmatic guidelines for bringing the solution to market through an agile and flexible, digital health-flavoured and oftentimes creative RE process and explains lessons learned during one such attempt, dealing with a system for managing diabetes, which was deployed in the University Hospital of North Norway. Tips for selecting the most suitable RE techniques are given, along with insights into key challenges that should be expected in digital health, including crucial needs for establishing tacit knowledge, security and data handling considerations, engaging patients and medical personnel to increase chances for high adoption of the resulting system, focus on regulatory requirements and acquisition of ethical approvals to conduct the project. Finally, practical experience is shared with the reader based on the real-world diabetes healthcare system case, providing an insight into how such a custom digital health RE process was applied in practice.

M. Volk (✉) • U. Sedlar
Laboratory for Telecommunications, University of Ljubljana, Ljubljana, Slovenia
e-mail: mojca.volk@ltfe.org; urban.sedlar@ltfe.org

N. Falk-Andersson
Norwegian Centre for Integrated Care and Telemedicine, Tromsø, Norway
e-mail: niklas.andersson@telemed.no

S.A. Fricker et al. (eds.), *Requirements Engineering for Digital Health*,
DOI 10.1007/978-3-319-09798-5_8

8.1 Introduction

When confronted with a real-world challenge, a manager quickly tries to zoom out to comprehend the bigger picture: who are the stakeholders, what are their needs, who will be the end users and what are the project constraints. This provides the foundation for everything that needs to be developed and serves as guidance for finding the right balance in the project management triangle, where a trade-off has to be made between the required time, quality and the cost of the project.

However, in the case of a digital health solution, the dynamics between the stakeholders is not one of a simple two-sided market, and the stakes are much higher than in typical consumer-facing projects. Indeed, a poorly designed, developed and deployed digital health solution can not only cause financial losses, wasted time and inconvenience, but also endanger lives and cause physical, as well as psychological damage (e.g. through leaked data due to inappropriate data security). This presents significant challenges and forces the project into the time-tested "slow development" paradigm, which tries to tread lightly through the project realisation, learning about and adapting to the development, regulatory, legal, ethical, data privacy and other challenges as the project progresses. The problem is further exacerbated by the fact that not many people possess the big picture of the digital health domain; thus, doctors are typically oblivious to developmental or regulatory issues and an analogous statement can be made about engineers. Several studies have shown that even certified medical equipment and devices can be easily reverse engineered and compromised, leading to severe consequences for patient privacy and safety.

The goal of this chapter is to outline the challenges in requirements engineering that are specific to digital health solutions and address them in the form of a guideline. The material is presented in the form of a recipe, further explained through a specific real-world case of a digital health application developed in cooperation between industry partners and health providers, which is currently being deployed in the University Hospital of North Norway.

Thus, this chapter tries to guide the reader through this multi-sided domain, through lessons we have learned the hard way and through months of time stuck in red tape. The remainder of the introduction gives a brief overview of the requirements engineering (henceforth RE) specifics in digital health and the digital health stakeholder landscape that can serve as a basis for the RE process. Section 8.2 provides a cookbook for the RE process, describing concrete steps for elicitation, analysis and requirements validation in more detail. Section 8.3 provides the lessons learned in a real-world implementation of a digital health solution and Sect. 8.4 reflects on how the implemented use case benefited from the recipes provided in Sect. 8.2. Section 8.5 provides the final summary and conclusions.

8.1.1 Defining the Domain

Digital health is an emerging field that brings together healthcare, medicine and modern information and communication technologies (ICT) to help patients manage illness and address their health-related problems, as well as enable medical personnel to help patients more efficiently. By relying on a plethora of digital technologies and solutions, most notably wireless sensors and devices, mobile connectivity and the Internet, social networking, genomics, medical imaging, big data processing techniques and use of health information systems [11], it helps eliminate the inefficiencies in the healthcare system and medical processes. In addition, it serves as the underlying enabler for increasing the general well-being of the population, prolonging life expectancy and enhancing the quality of life.

8.1.1.1 Requirements Engineering Perspective

In essence, the RE process tries to bridge the gap between the stakeholders and the project team through the steps of gathering (eliciting), analysing (documenting) and validating the requirements [2]. For each of those phases, a variety of methods can be used; typical methods of requirement elicitation include workshops, interviews, surveys, document analysis, reusing requirements of similar projects, system archaeology (i.e. study of poorly documented or undocumented legacy systems), data mining (inferring requirements from large datasets), observation, introspection and using the creative thinking process to arrive to a set of requirements. Once requirements are elicited, the analysis can be performed by modelling or prototyping the system, or using structured, object-oriented, problem domain-oriented or viewpoint-oriented techniques. Finally, the requirements and assumptions should be agreed upon, confirmed and validated. This is usually done through walkthroughs, simulations and reviews.

However, as illustrated, the RE practice is a very varied discipline in itself and when it comes to applying selected methods, a customised approach is needed for each individual domain. In this respect, digital health is fundamentally different in subtle ways from most mainstream domains, and has the following specialities [2–4]:

1. The context of use and the technology to be used are often poorly matched and balanced.
2. The stakeholder list is long and includes many possibly conflicting relations. This amounts to a lot of work with requirements elicitation, analysis and checking, and can introduce significant delays. Also, there is a high possibility of stakeholder resistance, which is usual in slow-changing and heavily regulated fields. For example, doctors are not always willing to invest the time and work necessary to adopt the solution that would in the long run benefit all stakeholders.
3. Since doctors and nurses, as well as the patients, together represent two of the most prominent user groups for the digital health application, their specific

use cases need to be given a strong emphasis. Patients typically encompass the entire population with significantly diverse requirements; for example the elderly that may have little experience with digital technology have oftentimes poor eyesight and hearing, and can come into contact with the solution in different settings (in the hospital, in the office, at home, etc.). Meanwhile, the caregivers already have a workflow that may encompass clinic hours in their office, performing examinations or direct supervision, domiciliary visits, etc. Using observation as a requirements elicitation technique may prove especially valuable in such varied environments, and using modern tools to capture stills, audio or video of the process can be of great help in later requirements analysis phase.

4. Business case is typically a complicated one reaching beyond regular provider-consumer relationship in the fact that typically digital health services are offered free of charge to individuals as part of a greater care concept by a not-for-profit medical organisation, but involving also for-profit providers such as insurance companies and technology providers.
5. It is therefore vital for successful requirements development and delivery of an acceptable and useful solution to have good understanding of digital health specifics and contexts, as well as to understand social and emotional implications associated with the required socio-technological alignment.

To successfully cope with the digital health challenges, requirements should be developed by a multidisciplinary team that together possesses good understanding of the technology and the context and can cooperatively apply human-centred requirements development in a well-organised but flexible and creative process.

8.1.1.2 Stakeholder Landscape

Digital health is a truly multi-disciplinary domain that involves many stakeholders with different backgrounds, ranging from medical and healthcare to engineering, legal and social sciences. Before the requirements investigation phase it is crucial that the stakeholders and any possible conflicts among them be identified. Involving the stakeholders in the process of designing a solution is important regardless of the domain. This is to ensure that the end result is both usable and useful. However, due to the fact that medicine and, by extension, healthcare are heavily regulated, it is even more important that the stakeholder list also includes regulatory bodies, security, legal and ethics experts, as well as manufacturers and supply chain specialists. This can ensure that the final solution is also secure, safe to use, economically viable as well as legally and ethically sound.

Many stakeholder classification approaches exist in the literature, however [5] providing a nice basis for understanding the healthcare ecosystem by dividing the stakeholders into the following four groups:

- Entities accepting care—Members of this group are the single most important reason for existence of the healthcare system; therefore they must be given special attention to ensure that the solution benefits them (directly or indirectly). In digital health, the group is represented by:

  - Patients: Not only hospital patients and outpatients, but also anyone that could require medical assistance in the future; the latter group is especially relevant in non-clinical, preventive and well-being use cases.
  - Next-of-kin: In most cases next-of-kin represents a secondary stakeholder group, except where they take on additional roles, such as being payers or caregivers.

- Entities providing care—Providers are at the heart of medical decision-making. In particular, clinicians are expected to provide accurate diagnosis, choose appropriate therapy and monitor the resulting health outcome while maintaining good doctor-patient relationship and bedside manner. Providers can be further broken down into individuals and institutions. Individuals include medical personnel: clinicians (doctors, nurses, medical students), outpatient care providers and medical researchers. However, in the case of a digital health solution, this group also extends to the non-medical personnel, such as IT administrators and IT operation managers.
- Supporting entities—They enable the health care system to function smoothly. The payers group does that by financing the providers (most commonly this means insurance companies and employers that pay for health insurance). Manufacturers group does it by designing and developing the solutions and the technology to enable new, better and more efficient processes, while the distributors take care of the delivery of goods and services to the users (either clinicians, their institutions, or the patients). This includes manufacturers of tangible products: pharmaceutical companies, biotechnology, medical devices and infrastructure, as well as manufacturers of intangible products (software): developers, designers and solutions architects.
- Controlling entities—This group regulates the ecosystem in multiple ways to ensure that the standard of health care is high, and that the safety of the patients, as well as their security and privacy, is not compromised. Best practices are established based on the available scientific evidence that serve as guidelines for other stakeholder groups.

During the RE process, identified stakeholders are prioritised. Key stakeholders are the ones with significant influence and impact on the project, required resources or other stakeholders (e.g. a diabetology department that is setting up a digital health solution for their patients). Also, they are typically categorised as primary or secondary, depending on the way they are affected by the process and the solution: the primary group is directly affected (for example diabetes patients using the application), while the secondary group only feels the consequences of the actions and decisions indirectly (for example, next-of-kin). The digital health stakeholder landscape is presented in the diagram in Fig. 8.1.

Key challenges of each of the identified stakeholder groups are presented in Table 8.1, together with their expectations with regard to digital health solutions.

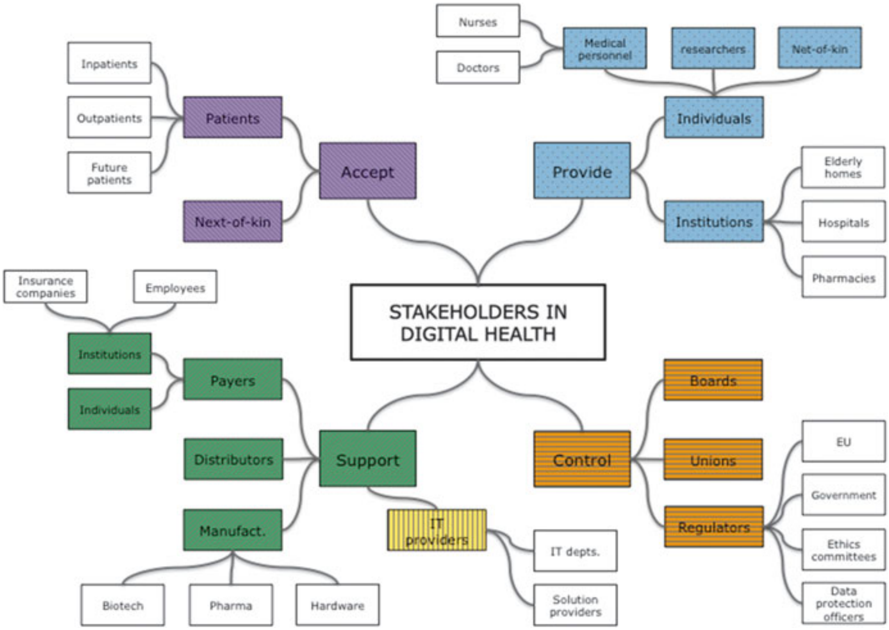


Fig. 8.1 Digital health stakeholder landscape breakdown

8.1.1.3 Promising Digital Health Technologies

Recent technological trends in digital health consumer end indicate increasing adoption of self-care and health monitoring solutions that combine smart sensing devices (such as glucometers, pedometers, smart scales, and pulse-oximeters, with Bluetooth or other similar standard interfaces), cloud computing, smartphone and tablet-based applications based on Android and iOS platforms, as well as powerful web-based technologies (such as HTML5). In healthcare provider domain, electronic health record (EHR) systems, centralised web-based patient management and communication portals as well as intelligent healthcare ambient (such as sensor-supported operation theatre, digitised pharmacy) are gaining momentum. The importance and increasing strength of this technological field are in part driven by advancements and increasing availability of the latest commercial off-the-shelf technologies, and vice versa.

8.2 Requirements Inquiry in a Clinical Environment

In this chapter, we provide a balanced set of guidelines for implementation of the RE process in a project that has the following characteristics:

- The targeted solution is one in the digital health domain, where the quality implications of poor requirements handling are particularly serious.

Table 8.1 Key digital health stakeholder groups, and their challenges and expectations with regard to digital health solutions

General problems/challenges faced	Digital health solution should aim to
Entities accepting care	
Quality of care/inadequate care. High cost of care. Inability to understand the condition/treatment.	Increase quality, lower cost, shorten waiting times, increase convenience, etc. Provide ease of use and ensure responsiveness. Present information to the patient in the most suitable and accessible way, and provide primary, secondary or tertiary prevention benefits. Respect user privacy, ensure and maintain data security and have well-defined data ownership model.
Care providers	
Harm done to the patient due to poor judgment. Misdiagnosis due to lack of information (e.g., missing context data). Low efficiency due to complicated processes and organisational problems.	Increase efficiency and automate certain processes. Provide ease of use and ensure responsiveness, and present information to the clinician in the most suitable and accessible. Provide context information to support primary and secondary prevention and minimisation of risk of misdiagnosis or wrong data interpretation. Be adaptable and extensible in terms of upgrades with new findings, and be as low maintenance as possible.
Supporting entities and regulatory entities	
Solutions or processes that are not economically viable. Increasing complexity of regulations; emerging fields such as digital health present new challenges. Facing resistance from certain stakeholder group or health care sector.	Maximise economic viability by leveraging cost benefit analysis, aligning to stakeholder interests and taking into account total addressable market size. Adhere to local, regional, national and supranational guidelines and legislation; conform to national and international standards. Address data ownership and user privacy issues according to local, national and supranational data privacy laws and directives.

- The targeted system is software intensive and human centred rather than market driven, and it comes together with a business model that is typical for hospital-provided healthcare services; it consists of applications, centralised server-side components as well as legacy IT infrastructure specific to healthcare, and it utilises web and cloud technologies.
- The project is constrained in time with well-set boundaries and requires fast, efficient and rather creative RE process with possibility to reiterate selected or all RE sequences in later phases of system engineering.

The guidelines are based on own experience of implementing RE best practice in software-intensive digital health. The guidelines are prepared as recommendations for engineering practitioners with a particular focus on challenges and specialities that are characteristic for digital health domain. Different aspects are addressed and

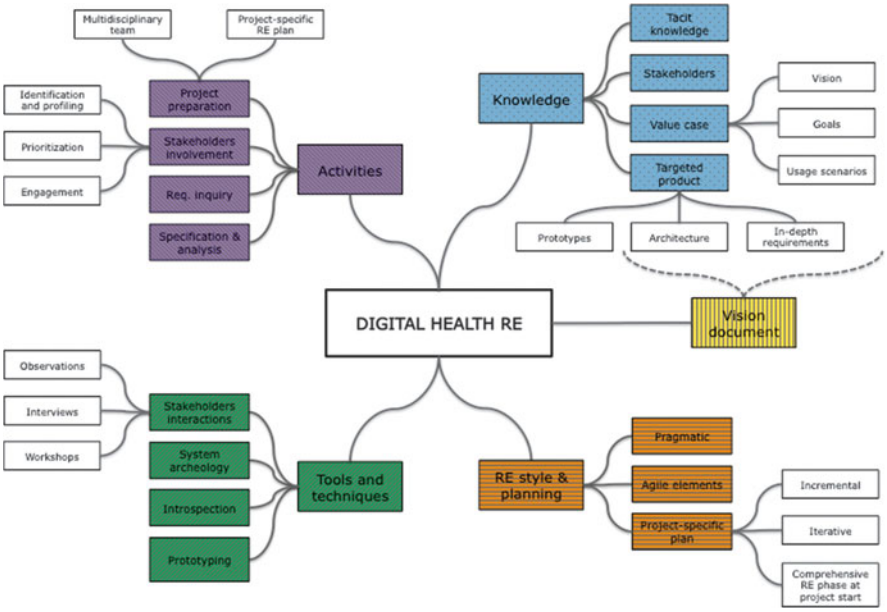


Fig. 8.2 Digital health RE elements and aspects

crucial RE elements are discussed that will help in delivering a successful digital health solution, as summarised in Fig. 8.2.

There is one guiding principle underpinning the guidelines: the pragmatic approach focusing on the *minimum feature set* that is still able to satisfy the stakeholders. In today's fast-paced and competitive environment, the key to success is to deliver the best possible solution in the shortest amount of time and with minimum spending. To be able to do so, use the RE process as a way to understand who your target stakeholders are, generate new ideas, design the solution, prototype it, expose it to the real world as soon as possible and learn.

8.2.1 Project Preparation

First, a *multidisciplinary RE team* needs to be assembled. In addition to RE engineers, architects, developers and designers, selected stakeholder representatives should also be part of your team. Consider involving a well-balanced mixture of healthcare specialists, patients and personnel, legal, regulatory and social sciences experts as well as business domain representatives. The multi-disciplinarity of the team will help you understand digital health expectations and challenges from different specialised perspectives and will lead you towards establishment of communication and shared understanding within the team itself as well as towards different stakeholder groups.

Due to the fact that digital health use cases present many interdisciplinary challenges, this will dictate the need not only for good intra-team, but also inter-team collaboration and communication.

Once the team is assembled, prepare a high-level description of the targeted digital health system. Called also a *vision statement*, it identifies the driving technologies to be considered and any major constraints related to your system, for example security and standardisation guidelines to be followed and potential ethical issues expected. This will be your guiding target for the remainder of the RE process, continuously evolving as you progress.

Discover which technologies are crucial for your system. Also, in bespoke software-intensive systems, such as digital health system, you should follow the established international standards and recommendations in preparing the architecture descriptions of systems and software. Security, privacy and data handling are of paramount importance, and you should take into account applicable regulation on national and EU levels. For EU, the European Legislation and specific national jurisdictions set guidelines for data handling and protection as well as provisions for its applicability to digital health. If you discover that actions are needed to obtain ethical approval or other similar permissions for your project, initiate the respective procedures immediately as they might take a considerable amount of time. Investigate standardisation and certification landscape for your digital health system. In particular, focus on standards and guidelines that refer to healthcare systems and medical devices. And finally, consider referring also to established standards and recommendations for implementing RE itself.

Next, plan for a *project-specific RE*. To cope with the challenging digital health characteristics and achieve high-quality outcomes, the requirements engineering process should be systematic and disciplined [3] yet flexible and open to accommodate creativity and innovation as well as to respond to project particularities and unexpected developments. Prepare the RE model and plan the requirements development sequence carefully. It is important to be explicitly aware of the particular steps in the RE sequence, even if they will be implemented implicitly. This will lead you to a well-organised and systematic RE implementation.

Plan your RE process *iteratively and incrementally*, with at least two cycles of design, prototyping and evaluations, as shown in Fig. 8.3. Use a hybrid process model that combines *one comprehensive RE phase at the beginning* of the project, which facilitates establishment of in-depth understanding of the digital health context and its particularities, and continuous RE iterations later in the project as part of the realisation of the system, which allows for agility with lightweight RE activities planned (at least) throughout system design and development phases. This might seem to contradict the agile approach but it allows for early discovery and comprehension of all relevant particularities that have vital impact on the design and prototyping of the system.

Inside each cycle, consider implementing your RE iteration as a combination of the following activities:

- Establishment of the vision and system context, stakeholder identification and profiling.

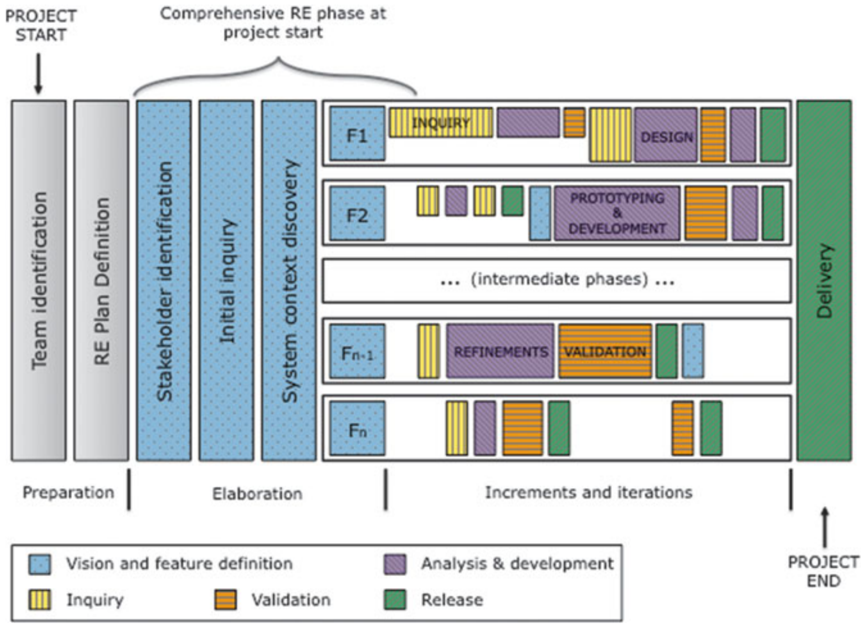


Fig. 8.3 Iterative and incremental RE process

- Requirements inquiry that confirms and details the vision and system context.
- Requirements analysis and prototyping.
- Vision, context and requirements documentation.
- Requirements validation, negotiation and refinements to assure appropriate level of quality and trust.

The goal of these steps is to explicitly define, document and understand all relevant requirements at an appropriate level of detail, as explained in more detail in later sections. As you will proceed through the iterations, the steps will become more in-depth and intermediate deliveries will be more frequent. To cope with the complexity of the goal, allow iterations inside or across steps in the RE process as necessary and acceptable for the project timeline.

The plan should include also continuous monitoring of the RE process throughout the entire system life cycle, facilitating small adjustments rather than drastic changes and deviations. However, the planned RE process probably will not go entirely smoothly. Be prepared to continuously evolve and improve your selected model to accommodate particular developments of the project. Throughout the entire process, you should allow room for ad hoc opportunistic moments, requiring restructuring of the planned sequence or even reiteration of certain activities due to increasing complexity of the process.

Hereafter, different elements of RE practice are explained in more detail in the context of specialities related to the healthcare domain.

8.2.2 Identification and Profiling of Stakeholders

Account for involvement of end users. Human-centred design implies that targeted end users are actively involved in the process from the very beginning, taking continuous part in context discovery and prototype evaluations. Hereafter, we provide guidelines that are based on recommendations of references [2], [4], which we have adapted based on our personal experiences in developing digital health systems.

Once you have initiated your project, the first step is to identify the stakeholders for the targeted solution. In digital health, targeted stakeholders are in most cases known from the beginning of the project (e.g. patients with type 1 diabetes, nurses on a pulmonology ward). Stakeholders are all persons and organisations that either have a role in or are affected by the targeted digital health system. End users are a sub-group of stakeholders, representing people who will use the solution.

To identify the stakeholders, begin with discovery of established processes in the healthcare environment that are in the context of the targeted system. Identify relevant procedures and responsible persons and organisations. To do that, use a combination of organised interviews with the client and selected end users, consult healthcare experts and if needed refer also to available documentation. Make sure to involve patient representatives, medical personnel, IT specialists in the targeted healthcare environment, security officers, representatives of national regulatory bodies, etc. This should lead you to *an initial list of patients, medical personnel and regulators* who will be representing your core stakeholder group.

Once identified, prioritise the stakeholders by power, legitimacy and urgency, and validate the list with the stakeholders themselves. This is a very important step since the healthcare processes are typically very complex and involve stakeholders in different contexts. Later on, at stakeholder workshops organised during requirements elicitation, the stakeholders' list and prioritisation should be updated based on newly discovered facts. Also, new stakeholders might be discovered, and if so, they should also be invited to participate and their roles must also be verified.

Finally, profile the stakeholders in their professional setting. This process should lead you towards understanding of the particular sub-groups of patients, professionals and regulators with specific needs and expectations towards the digital health system. Depending on the nature of the system, a sub-group could be an entire population, a particular age group, highly specialised experts with (or without) IT skills, etc. Good understanding of the targeted sub-groups is important for success since it helps understanding the needs and motivations that drive (or slow down) the adoption of the delivered system.

However, gaining such insight is not a straightforward task. Rather, one has to begin with "getting to know" the persons and discover their day-to-day routines, behaviour patterns, reactions, attitudes, etc. This so-called *tacit knowledge* should be gained as soon as possible, preferably even before the actual requirements data collection begins, and Table 8.2 summarises some techniques that might be considered.

Table 8.2 RE techniques that can be used for establishment of tacit knowledge in digital health

Technique	Key idea and benefits	Tips for digital health usage
Observations	Give insights into end users' behaviour patterns as well as uncover routines they themselves might not be aware of [6]. They also help to circumvent discrepancies between what people say and what they actually do, and are less time consuming that the majority of other techniques. Observations can be used primarily to elicit requirements that specify desired features and modalities of the system.	Consider spending 1 or 2 days in the environment where the planned system or its services and applications will be used. For example, if you plan to develop a system that provides applications for self-management of specific disease, try to arrange a 1-day visit as the observer in the doctor's office at the hospital during patient check-up appointment. Observe routines and processes, and try to establish an understanding of doctor-patient relationship, key values for the patient and the doctor, and key weaknesses in the current process that can be improved with your system.
Interviews	Give insights into expectations, opinions and motivations related to the targeted digital health system. Interviews are used to profile the stakeholders, as well as to elicit requirements that define features of the system and user experience. Pre-defined questions help guide the conversation, and if the interviewer is a highly experienced one she might uncover subconscious requirements through clever questions [2].	Plan for interviews with all key stakeholders, in particular with patient representatives and medical personnel that have an interest and are willing to participate also later in the project, as well as with key representatives of the legal/security and IT departments of the institution where your system will be deployed. Target nurses and support medical personnel in addition to doctors.
Workshops	Workshops in general and focus groups in particular are a form of group interviews where all participants are invited to act in interactive discussions directed by engineers' interests [7]. They are used to establish contexts, roles and routines that will be supported by the targeted system. A variety of creativity techniques can be applied in focus groups, such as brainstorming, apprenticing and story playing, to define and confirm typical scenarios and actors, and uncover context and its possibilities and limitations related to the system.	Plan for dedicated workshops with patients and medical personnel per deployment site, and with the customer and relevant regulators, such as IT department and legal/security office representatives, manufacturer of legacy infrastructure etc.

When discovering the domain and gaining tacit knowledge, consider using multimedia as one of the communication channels. For example, video film stakeholder's story playing, take pictures of the healthcare environment and medical personnel and record value statements during individual interviews with doctors, nurses and patients. This will add an innovative angle into the process while allowing returning back to individual situations and scenes anytime later in the RE project to (re)establish, confirm or even deepen your understanding.

Since researchers, stakeholders and end users will be actively involved, requirements elicitation and negotiation must be carefully managed to achieve *cooperation* and consolidate any conflicting opinions and interpretations of the identified requirements as early as possible. Early detection of conflicts and sufficient agreement about the requirements between the involved stakeholders and end users is a key factor for the realisation of the vision and acceptance of the resulting system [8].

8.2.3 Requirements Inquiry

Once you have profiled the patients, medical personnel and regulators and have gained sufficient tacit knowledge, the documentable *requirements elicitation* begins.

To elicit requirements, consider using the techniques explained earlier in the tacit knowledge acquisition stage, as well as those explained in Table 8.3 (please refer to [2] for further details as well as further techniques that can be used during RE inquiry).

Elicit requirements iteratively according to the (re)planned RE plan, each time resulting in more in-depth requirements specifications. In each iteration, make use of a combination of techniques that suits best, and allow for flexibility to change the combination as you advance. Consider using creative ones in the initial iterations (observations, brainstorming, introspection, prototyping), gradually adding complex and more formalised ones that will lead to in-depth RE establishment (system archaeology, document analysis). Engage stakeholders from the very beginning and at all later stages of RE inquiry. Plan for dedicated workshops with patients and medical personnel and with customer representatives, specially those from the IT department and legal/security office, to demonstrate and evaluate prototypes, and to review, refine and validate already elicited requirements and discover new ones. As you proceed to more in-depth levels, consider involving other specialised actors in addition to patients, medical personnel and customer representatives, in particular legal experts, standardisation bodies and domain experts.

8.2.4 Requirements Specification and Analysis

Requirements must be consistently documented, as well as any other important artefacts influencing the inquiry process or affecting the resulting requirements specifications (for example major decisions, workshop minutes and visual materials, persons involved).

Table 8.3 Further RE techniques that can be used for requirements inquiry in digital health

Technique	Key idea and benefits	Tips for digital health usage
System archaeology	A technique used to extract relevant information required to build a new digital health system that is based on or connected to legacy systems. It relies foremost on analysis of available documentation and implementation (software code), and allows for discovery and support of all relevant functionalities in the legacy system that must be implemented or taken into account.	Use this technique to gain understanding about the most important existing systems, such as electronic health record (EHR), patients' self-management portal, APIs to national authentication service. You might want to consider combining document analysis with perspective-based reading to elicit regulatory and standardisation requirements from available legacy system documentation, standards documents, position papers and strategy documents, etc.
Introspection	A technique in which the requirements engineers play different stakeholder roles in order to experience specific requirements and hence gain domain-specific understanding. It proves particularly useful for discovery of requirements that the stakeholders take for granted and therefore cannot elucidate.	Consider using this technique in the form of apprenticing, when the role-playing exercise is completed together with the actual stakeholders who adopt the "master" RE role and assure realistic understanding of the elicited requirements.
Prototyping	This is a particularly important technique used to inquire, illustrate and validate functional and user experience requirements in situations where stakeholders have only a vague understanding of what is to be developed. It represents a vital engineering element of any agile-oriented RE. If used early in the process it helps to refine and validate requirements in realistic settings and discover new requirements not identified previously. In particular, graphical user interface prototypes are frequently used in practice to discover additional functional requirements.	You are strongly advised to use prototyping early in your RE process as well as at all stages of system development later on. To do so, prepare an initial prototyping plan right after the first comprehensive RE iteration and build to illustrate, not to deliver. For the time being keep it small, and prioritise services or features that will be exposed to patients and medical personnel. Examples would be GUIs and selected features available in mobile applications and web portals for patients (for example gathering activity data with a mobile app and a pedometer, editing of data, and submission of data to a doctor), or an extended web-based EHR dashboard for doctors and nurses (for example a new feature in the existent GUI for viewing data submitted into the EHR by the patient). Once the prototypes are ready, engage stakeholders to demonstrate and evaluate them as often as possible and in combination with other RE methods, in particular interviews, workshops and apprenticing.

The quantity and depth of RE materials are case specific and should be decided by the project team based on the requirements for such documentation and its use by the developers (for example, application GUI snapshots needed for prototyping) as well as stakeholders (for example, system vision document required by the healthcare institution, use case description needed for further RE workshops with targeted stakeholders). However, keep in mind that agile development without any documentation only works for small projects with limited number of stakeholders and limited number of developers. Even in most extreme agile development projects with minimum documentation, it is the establishment of system vision that helps considerably in maintaining focus throughout the entire engineering and delivery of an acceptable and exciting system.

When extracting requirements from the information collected throughout the elicitation processes, you might want to consider an approach, where the elicited requirements are specified along the dimensions shown in Table 8.4.

Document the requirements incrementally as they are defined. Consider initiating documentation with less formal forms, such as notes, sketches, simple diagrams and checklists that later become part of the formal RE specifications document. Later in the process, prepare documentation in compliance with established project formats and rules, including prescribed modelling languages, templates and forms. Also, consider using *multimedia materials* to support and contextualise RE documentation, such as video interviews with stakeholder representatives, video clips from healthcare environment observation, or pictures and snapshots of early prototype evaluation workshops and planned applications. Having such multimedia materials will allow the project team to return to different stages of RE whenever needed, and can be used also for innovative dissemination and marketing.

Table 8.5 summarises some additional tips that might help you discover just the right amount of information throughout the RE process.

Finally, quality of the resulting requirements is vital. To avoid jeopardy and failure to deliver an acceptable system, elicited requirements must be continuously *checked and validated*. Bear in mind that errors, inconsistencies and misunderstandings can (and probably will occur) at anytime and as part of any of the above processes. Erroneous artefacts can entail inconsistencies and defects in all subsequent system engineering activities, including system architecture and functional design, development, implementation and verification, and must therefore be identified and eliminated as soon as possible. In part checking and validation will happen naturally throughout the RE process, in particular through prototype evaluations and introspection, system architecture drafting and scenario definitions. However, you should take additional measures by checking the produced documents through inspections (e.g. walkthroughs, peer/advisor reviews) and through establishment and confirmation of shared understanding of the elicited requirements at stakeholder workshops [9]. This will proactively engage stakeholders, allow them to contribute and help them understand the true value of the system, which altogether considerably increases chances of successful acceptance of the delivered system.

Table 8.4 Dimensions along which the elicited requirements are specified

Element	Key idea and benefits	Tips for digital health usage
Value case	Defines in brief yet clear terms what is the vision statement and what are the achievable and verifiable goals of the endeavour. It explains what goals the patients, medical personnel and regulators aspire to. It provides also the context of the planned system, such as planned integration into existing infrastructure, and measures that must be taken for safety and privacy assurance. It further consists of: • Stakeholders, and their power (priority). • Goals, which is a summary of wishes as expressed by the stakeholders. • Scenarios, which is a description of typical usage examples leading to fulfilment (or non-fulfilment) of the goals.	Value case should be prepared early and with care, and should describe in simple yet precise and concrete terms what immediate benefits stakeholders receive through the system. It will serve later in the RE process as a solid guideline during negotiations and requirements refinements at different levels of abstraction. When preparing descriptions, it should be formulated in a way that is well understandable for decision makers and marketing departments.
Targeted product	Outlines the digital health system under construction and defines its boundaries. This includes a basic outline of the product, identification of external systems the targeted product will interface, and definition of product's features.	Define the scope of the system development-wise. Focus on feature-based scope definition and prepare a initial deployment diagram that will outline major product components as well as relevant external systems that your product will be integrated with—in particular existent healthcare systems.
Solution-oriented requirements	This is a technical translation of the goals and expressed in technologists' language. Requirements explain functional, data and behavioural aspects of the planned software-intensive system as well as quality requirements. Two general types are distinguished, functional requirements, and quality requirements including usability, security and legal aspects.	Specification of in-depth technology-dependent requirements should be considered in later iterations of the RE process.

8.3 Example of an RE for a Digital Health System

In this chapter, we showcase a practical example of guidelines implementation for a new Internet-based diabetes share system (DSS).

Table 8.5 Tips how to balance the scope of requirements discovery and specification

Tip	Rationale/example
Document crucial requirements that bear fundamental effect on the architecture of the system or its core functionalities.	For example, if your system connects to an EHR system and the national regulation allows data requests only from within the EHR system and not vice versa, this is an important regulatory requirement that you should document.
Prioritise requirements.	Do not be afraid to decide importance and abandon focus on less important ones. However, keep in mind that priorities are always project-specific and this might require you to divert from general good practice now and again. For example, the above regulatory requirement could be crucial in your case and should then have high priority, while in another project interconnectivity of the system with the existent EHR would be optional and therefore the requirement would have lower priority. Typically, day-to-day artefacts and small details are of lower priority and don't need to be documented (e.g., colour scheme for GUI buttons).
While prioritising, remember the minimum feature set principle and aim at keeping a good balance between base factors and excitement factors.	Base factors are requirements and constraints that will assure your system is conformant to standards, ethically approvable and legal. On the other hand, excitement factors are different elements and aspects that make your system unique compared to other products, usable and useful—in other words, interesting and attractive for the patients and medical personnel to want using it on a daily basis. Target minimum scope of your system that can best satisfy all your core stakeholders.
On a regular basis, analyse requirements and try to produce an architecture diagram of your system.	This will help you validate elicited requirements and check their consistency and compatibility, and will gradually lead you towards in-depth system architecture outline. Consider performing intermediate validations of the architecture also with IT department, legal and security officers and other relevant stakeholders (with enough technical understanding).
Involve stakeholders.	Engage patients, medical personnel and regulators and give them opportunity to contribute. For example, organise walkthroughs of the already prepared documents, check system architecture diagrams with the IT department, and continuously evaluate GUI prototypes with patients, nurses and doctors. This will considerably increase chances for high acceptance of the system in practice.

8.3.1 Case Study: The Diabetes Share System (DSS)

The system addresses the problem of inadequate blood glucose levels of diabetes type 1 patients, which affects both patients and next-of-kin, doctors and nurses. The impact of this problem is severe complications for the patient and high treatment costs. A successful solution enabled the patient in effectively balancing intake of insulin and carbohydrate, physical activity and stress, using consumer-grade smartphone applications that are integrated into the digital health environment at a hospital.

The proposed DSS solution was a result of concrete real-world needs, ideas and propositions from patients, clinicians and researchers themselves, recognising it as a natural extension of the self-care smartphone applications already in use by patients. Its architecture was designed to fulfil those expectations, as well as to meet the requirements on security, data protection and operational practice (Fig. 8.4).

Fig. 8.4 Case study: Patient and physician discuss benefits of using mobile technology to manage self-care (photos taken with consent)

The DSS is a solution that integrates self-care applications on smartphones used outside the hospital with clinical systems located in the secure hospital domain. It is intended for diabetes patients, next-of-kin and physicians and nurses who train, monitor and consult an empowered diabetes patient. The solution is cloud based and enables mobile recording of health and biometrical parameters, remote counselling and comparison with other patients' anonymous observations. Unlike in-clinic treatment based upon manually recorded or lacking health parameters, DSS increases evidence to support treatments, increases the patient's knowledge base, assists in maintaining a healthy lifestyle, reduces the number of in-person appointments and hence contributes to improving the patient's diabetes condition, well-being and health. Its major features are:

- Self-reporting of diabetes and lifestyle-related parameters in a self-care smartphone application.
- Sharing of diabetes data with clinicians through its transfer from the smartphone application into a hospital EHR.

- Decision support service for clinicians through access to and visualisations of diabetes parameters, accessible through an enhanced EHR client.

We, a multi-disciplinary team working in the digital health domain, have been working with diabetes patients and caregivers in 2013 and 2014 to realise the DSS. The team comprised a broad skill set within software development, innovation, project management and research. Senior software developers and architects, project managers, graphics artists and researchers with backgrounds from industry, government, start-ups and academia are represented in the team, whose members are affiliated with the University of Ljubljana and the University Hospital of North Norway.

The following sections describe how requirements engineering for the DSS system was performed and which techniques and approaches contributed most to establishing shared understanding and an agreement between engineers, patients, clinicians and regulators.

8.3.2 Project Preparation

The DSS product was developed in an EU-funded project FI-STAR [10]. Following the description of an initial concept and general features of the solution in the project proposal phase, at the time the project was granted funding we specified a coarse project plan with budget allocations, work descriptions and milestones based upon the envisioned solution and expected deliverable dates. This information was necessary for identifying the skill set needed and suitable team member candidates. We formed the teams iteratively by profiling the project and letting senior staff members with expertise in selected disciplines (e.g. requirements engineering, software engineering, digital health security) review the project description.

The team had previous positive experience with iterative-incremental software development processes (Scrum agile), so we chose to design a customised RE plan accommodating this to benefit from already established processes. To align the RE activities with the development process we decided to distribute and iterate some of them over time, team and system features. Figure 8.5 shows the requirements activities over time (sequence of increments and iterations shown only as an example of the agile process).

Getting access to the stakeholders working in the hospital (medical personnel, hospital IT department) was a challenge because of their limited availability. However, this was expected and we found the agile process in a digital health context to be an advantage in this respect because it allowed us to be flexible about planning.

As shown in Fig. 8.5, the different requirements engineering activities were performed iteratively and incrementally, distributed over the course of the project, per system feature and aligned with stakeholder availability.

At one point we had a requirements inquiry session with clinicians regarding new user interface items in an EHR client application. New interesting functionality was revealed in that session (data aggregation methods) and we chose to use that opportunistic moment to give room for creativity and continue an informal discussion around this.

Naturally, this took additional time and we had to finish the session without having time to visit all the items on the agenda. Following this event, ideally, we could just have had another session the day after or so to cover the rest of the session. In reality though, this group of stakeholders needed a few weeks' notice to schedule a considerably long session. Consequently, since we did not have more than just a rough idea of our activities for the next 6 weeks, the developments at the last session did not have big implications for us to postpone some of the ensuing EHR client development to a later date. This in fact made it possible for us to better utilise RE results for this feature in development.

The lesson learned was that this situation could have lead us to a suboptimal product if it were developed within a process with up-front and detailed plans with little room for change (e.g. if subsequent RE or development activities would have had to start without sufficient input).

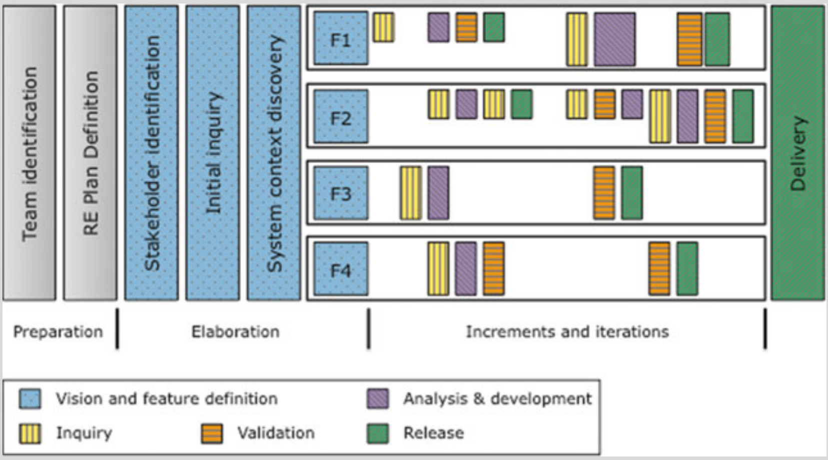


Fig. 8.5 Case study: RE activities over time (illustrative)

8.3.3 *Identification and Profiling of Stakeholders*

In the project, representatives from two target user groups, patients and physicians, were involved from the very beginning. The DSS system was a response to needs uncovered in previous projects where the same stakeholder representatives were involved, so these naturally formed the stakeholder baseline used for initial inquiry.

Table 8.6 Case study: Primary stakeholders identified for the DSS system

Power	Stakeholder type	Description	Discovery
1	Diabetes type 1 patient	Uses smartphone applications (DeStress Assistant and Diabetes Diary) to register observations and biometrics as part of their self-help treatment.	Baseline
2	Diabetologist (physician)	Responsible for treatment of the patient.	Baseline
3	Diabetology nurse	Manages, trains and distributes (glucose and insulin) equipment to patient. Helps physician treat the patient.	Interview with patient
4	Clinician	Abstract role representing the commonalities of physicians and nurses. Introduced in the model to avoid redundancy of information in documentation artefacts.	Informal modelling of use cases
5	Hospital IT administrator	Is in charge of administration and management of the hospital IT environment, as well as its maintenance and upgrades.	Through initial deployment efforts
6	Researcher	Is active in the field of scientific and/or technical research in digital health.	Through initial deployment efforts
7	Next-of-kin	Family member, close friend or partner. Requirements related to this stakeholder were postponed for later consideration.	Interview with physician

During a series of observations, interviews and workshops with the patients and physicians, and selected digital health domain experts (e.g. security experts that were part of the project owner organisation) we identified additional stakeholders having concerns about the DSS. Nurses were for example identified in an interview with a patient and the data protection officer was revealed in a workshop with the security expert.

We have then completed an impact analysis and ordered the identified primary stakeholders according to their priority and urgency as shown in Table 8.6.

In our case we neglected to realise the importance of two stakeholder groups initially, namely the researchers and the administrators. Not being primary end users their importance was being underestimated when in fact they had an important impact on successful delivery of the solution.

For example, the process of installation of the DSS system into the hospital environment would have been much more difficult without administrators' engagement and approval, and the success would have been hard to verify without scientific evidence supporting the researchers' needs.

The consequence of this was excess RE and development effort that needed to be reiterated and redone at a later stage.

Table 8.7 Case study: Additional stakeholders identified for the DSS system

Power	Stakeholder type	Description	Discovery
1	Data protection officer at UNN hospital	Responsible for patient privacy in UNN operations and fulfilment of requirements defined in legislation and through the «Code of Conduct for information security in the healthcare, care, and social services sector»	Workshop with security expert
2	Regional Committee for Medical and Health Research Ethics	Approves research projects and assesses whether research is undertaken in an acceptable manner. This entails the consideration of benefit vs. risk and whether data protection is assured.	Baseline
3	Helse Nord IKT	Local hospital network and equipment administration unit.	Interview with developer
4	The Norwegian Directorate of Health	Executive agency to the Norwegian Ministry of Health and Care Services.	Workshop with security expert
5	Northern Norway Regional Health Authority (Helse Nord RHF)	Helse-Nord is responsible for the public hospitals in northern Norway.	Baseline

In addition to primary stakeholders (end users), organisations with concerns affecting the DSS system were identified in initial workshops and interviews. These represented governing and regulatory bodies with a passive interest in the solution and had varying degrees of impact on it. They are found in Table 8.7.

These lists were revised and approved by the project teams and stakeholder representatives from the primary stakeholder group. This helped create an initial sense of ownership and commitment in the solution necessary for the inquiry activities to be prioritised.

However, we found difficulties in approaching and engaging these additional stakeholders. This was primarily due to lack of available capacity on their side, and also established internal policies that caused reluctance or inability to take decisions and responsibilities related to deployment and integration of the DSS system into the hospital environment. This had an unfortunate impact on the development progress since their engagement was found to be critical for successful delivery. As it turned out, the hospital network and equipment administration unit had severe capacity problems and was not available for requirements inquiry to a sufficient extent, resulting in delayed delivery.

8.3.4 *Requirements Inquiry*

8.3.4.1 Interviews and Workshops

During the inception phase of the project we spent significant effort on requirements inquiry and elicitation to establish the system context, high-level system features

To capture the end users' expectations and concerns on the solution we held a series of interviews and workshops with the patients and physicians, which were recorded digitally (photos, audio, video) as well as manually (note-taking). We also used role-playing within their own environment to elicit tacit knowledge on the patient consultation process and various artefacts involved (Fig. 8.6).

Fig. 8.6 Case study: Snapshots from the stakeholder workshops at the University of Northern Norway in Tromsø

and the quality properties of the solution. We find these items to be rarely changing and even while adopting an agile process they still are useful to cover and agree upon early since they help in keeping the target and scope in focus.

Throughout the process, we always allowed for enough flexibility to re-schedule or modify the planned activities. This proved necessary, in particular if proactive engagement of hospital and Norwegian healthcare representatives was needed. Flexible planning of stakeholder workshops and interviews allowed us to involve and engage crucial stakeholder representatives. However, this also required us to continuously update the RE plan and at some points even abandon certain planned steps.

We also completed an investigation of systems interfacing with the DSS. A list of specific requirements for the interfaces or expectations on responsibilities was prepared, which was later used for initial DSS system architecture drafting and prototyping (Fig. 8.7).

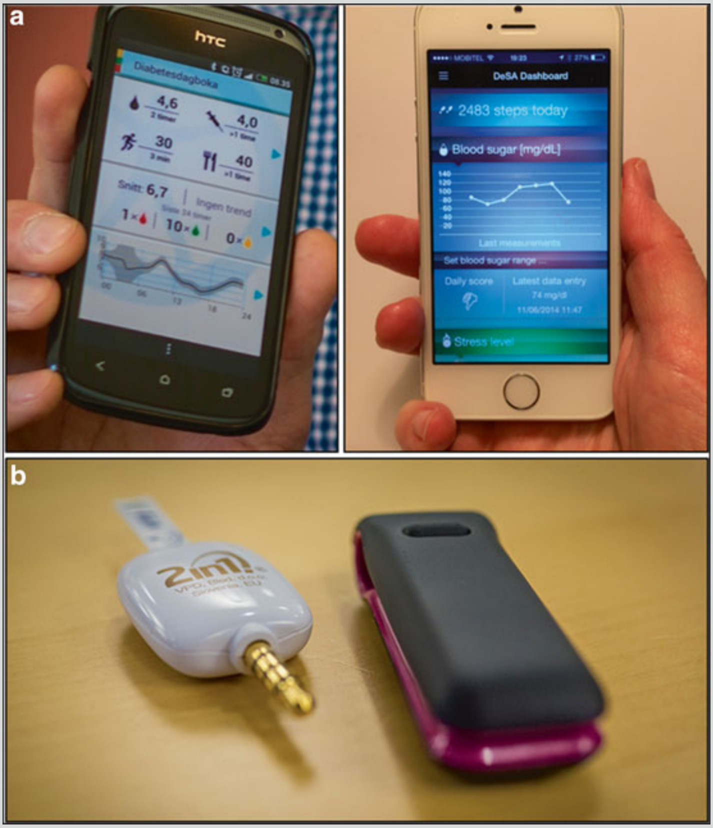


Fig. 8.7 Case study: (**a**) The Diabetes Diary smartphone app (*left*), the DeStress Assistant smartphone app (*right*), (**b**) 2in1SMART glucometer (*left*), and FitBit physical activity monitor (*right*)

8.3.4.2 Document Analysis

The DSS is a digital health solution handling sensitive, personal data and is by nature subject to a vast and detailed regulatory and legislative framework. Accompanying this are both national and international standards, policies and guidelines for how to realise solutions in the healthcare domain. A significant effort was thus put on document analysis in order to capture these kinds of requirements and constraints for the solution context. It was mainly the governing authorities found in the additional stakeholders list that owned these requirements and we did surveys of these organisations' web sites to identify document candidates for this process, as is shown through the below example.

The Norwegian Data Protection Office offers a set of guidelines explaining how to design technology integration architectures that are within the Norwegian legal boundaries. These are very concrete in certain aspects and can oftentimes be directly transferred to a specific system requirement. For example:

"All authorized access and failed access attempts to the service must be registered and stored for at least 2 years" (about information systems used for interaction with patients, freely translated from Norwegian).

8.3.4.3 System Archaeology and Prototyping

To identify constraints and requirements on the DSS interfaces towards other systems, we used system archaeology and held interviews where documentation was missing. To fully comprehend the impacts of certain interfaces we also implemented proof-of-concept prototypes.

For example, to learn about the significant details of the authentication protocol used between the patient's client application and the identity provider service, we found that the most efficient method was to "code it out", i.e. create a proof-of-concept application. As this was considered a high-risk interface (architecturally significant and high cost of overlooked requirements), creating such a prototype was useful to reconfirm that we had covered all vital details.

As expected, prototype evaluations were the crucial element, always resulting in considerable requirements refinements, identification of additional features and refinements to the applications interaction design. However, this required also continuous scope updates and feature prioritisation.

8.3.5 Requirements Specification and Analysis

8.3.5.1 Initial Vision Specification

We started to establish a product vision and feature scope in the beginning of the project. This was documented in a Vision Document and agreed upon by all primary stakeholders.

We prepared a walkthrough of all requirements elicited from initial stakeholder interviews, system archaeology, document analysis and prototyping, and normalised them into “stakeholder expectations” and the system context. These formed the basis for the initial requirements analysis, in which we used informal modelling and object oriented analysis to identify and specify the high-level functional requirements (system features and use cases) as well as quality properties and how they support the solution in fulfilling goals for the stakeholders.

From a project management perspective it was necessary to define also the minimal feature set that would be designed and developed in the first development stage. This included an informal risk vs. benefit vs. cost analysis that also indicated an ordering of features useful for project planning.

Vision Document: Table of Contents

1 Solution Positioning	
1.1 Problem Statement	A section explaining what is the problem to be addressed.
1.2 Position Statement	A section explaining what is the targeted solution and how it would contribute to resolving the problem.
2 Use Case Stakeholders	A section explaining which users, interfacing systems and other stakeholders are affected by the solution.
2.1 Users	Identified users, their background, role and expectations.
2.2 Interfacing Systems	System boundary, identification of relevant interfacing systems.
2.3 Other Stakeholders	Identification of other stakeholders that do not directly interact with DSS.
3 DSS Solution: Value Case	Establishment of the value case for the proposed solution, i.e. what are the goals in terms of effectiveness, efficiency, safety, satisfaction, etc.
4 DSS Solution Overview	An overview of system, its main components, scope of planned prototypes in phases, and specification of features including goals to be achieved, external interfaces, and expected usage scenarios.

The minimal solution scope was agreed upon in consensus between the project team and stakeholders, and proved to be very useful to help in keeping development focus and not spend effort on unwanted or extraneous features. The agreed upon scope definitions for DSS features documented in the Vision Document are shown in Fig. 8.8.

(continued)

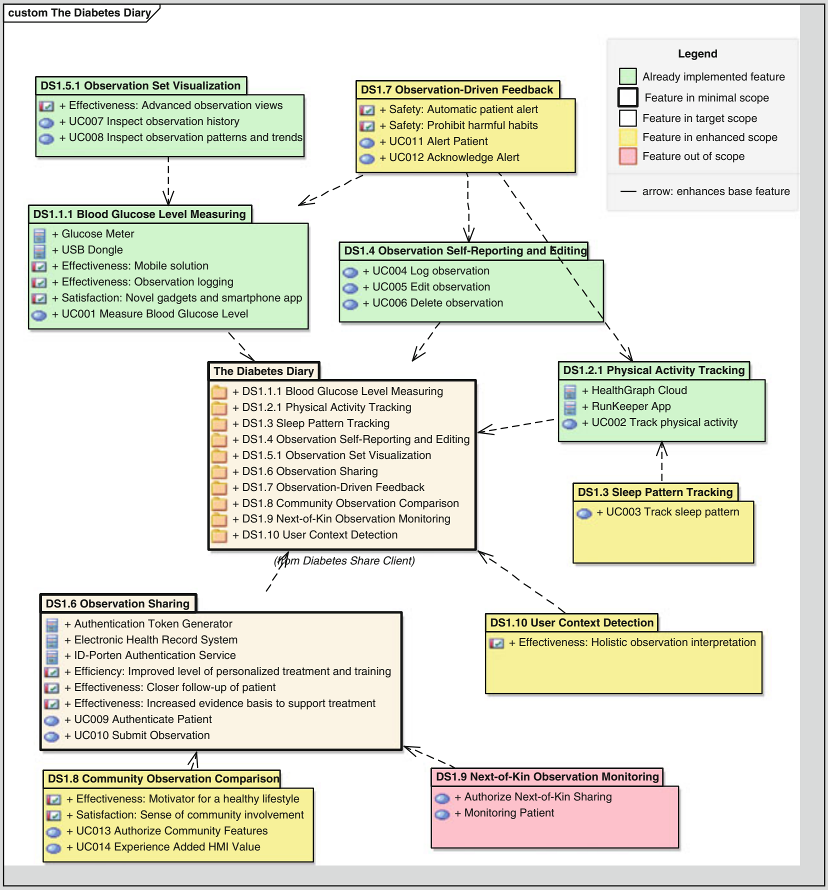

custom The Diabetes Diary
Legend
Already implemented feature
Feature in minimal scope
Feature in target scope
Feature in enhanced scope
Feature out of scope
arrow: enhances base feature
DS1.5.1 Observation Set Visualization
+ Effectiveness: Advanced observation views
+ UC007 Inspect observation history
+ UC008 Inspect observation patterns and trends
DS1.7 Observation-Driven Feedback
+ Safety: Automatic patient alert
+ Safety: Prohibit harmful habits
+ UC011 Alert Patient
+ UC012 Acknowledge Alert
DS1.1.1 Blood Glucose Level Measuring
+ Glucose Meter
+ USB Dongle
+ Effectiveness: Mobile solution
+ Effectiveness: Observation logging
+ Satisfaction: Novel gadgets and smartphone app
+ UC001 Measure Blood Glucose Level
DS1.4 Observation Self-Reporting and Editing
+ UC004 Log observation
+ UC005 Edit observation
+ UC006 Delete observation
The Diabetes Diary
+ DS1.1.1 Blood Glucose Level Measuring
+ DS1.2.1 Physical Activity Tracking
+ DS1.3 Sleep Pattern Tracking
+ DS1.4 Observation Self-Reporting and Editing
+ DS1.5.1 Observation Set Visualization
+ DS1.6 Observation Sharing
+ DS1.7 Observation-Driven Feedback
+ DS1.8 Community Observation Comparison
+ DS1.9 Next-of-Kin Observation Monitoring
+ DS1.10 User Context Detection
(from Diabetes Share Client)
DS1.2.1 Physical Activity Tracking
+ HealthGraph Cloud
+ RunKeeper App
+ UC002 Track physical activity
DS1.3 Sleep Pattern Tracking
+ UC003 Track sleep pattern
DS1.6 Observation Sharing
+ Authentication Token Generator
+ Electronic Health Record System
+ ID-Porten Authentication Service
+ Efficiency: Improved level of personalized treatment and training
+ Effectiveness: Closer follow-up of patient
+ Effectiveness: Increased evidence basis to support treatment
+ UC009 Authenticate Patient
+ UC010 Submit Observation
DS1.10 User Context Detection
+ Effectiveness: Holistic observation interpretation
DS1.8 Community Observation Comparison
+ Effectiveness: Motivator for a healthy lifestyle
+ Satisfaction: Sense of community involvement
+ UC013 Authorize Community Features
+ UC014 Experience Added HMI Value
DS1.9 Next-of-Kin Observation Monitoring
+ Authorize Next-of-Kin Sharing
+ Monitoring Patient

Fig. 8.8 Case study: Feature scope definition of one part of the DSS system from the Vision Document

8.3.5.2 Iterative Feature and Architecture Analysis

The initial DSS deployment architecture was defined using object-oriented analysis to the level of external interfaces and a component-oriented deployment scenario, as shown in Fig. 8.9a. This was specified in an architecture document, which was used in further communications with (technical) stakeholders, and was later on used as a basis for the DSS system design.

Further per-feature analysis was performed in an agile fashion, during the development process and subject to opportunities, impediments and availability of critical resources. Analysis and specification of requirements per feature was the responsibility of the development team and was performed to a level necessary for development progress. UML diagrams of system architecture, system deployment, component structuring, and use case scenarios, as well as informal drawings (sketches and white-boards), Wiki and text documents were used informally to specify and detail requirements.

For the DSS system, we prepared and continuously refined the deployment diagram, which was a result of several workshops with IT administrators at the hospital as well as DSS design work of the engineering team. For each feature, we prepared sequence diagram that corresponded to the designed architecture and its components.

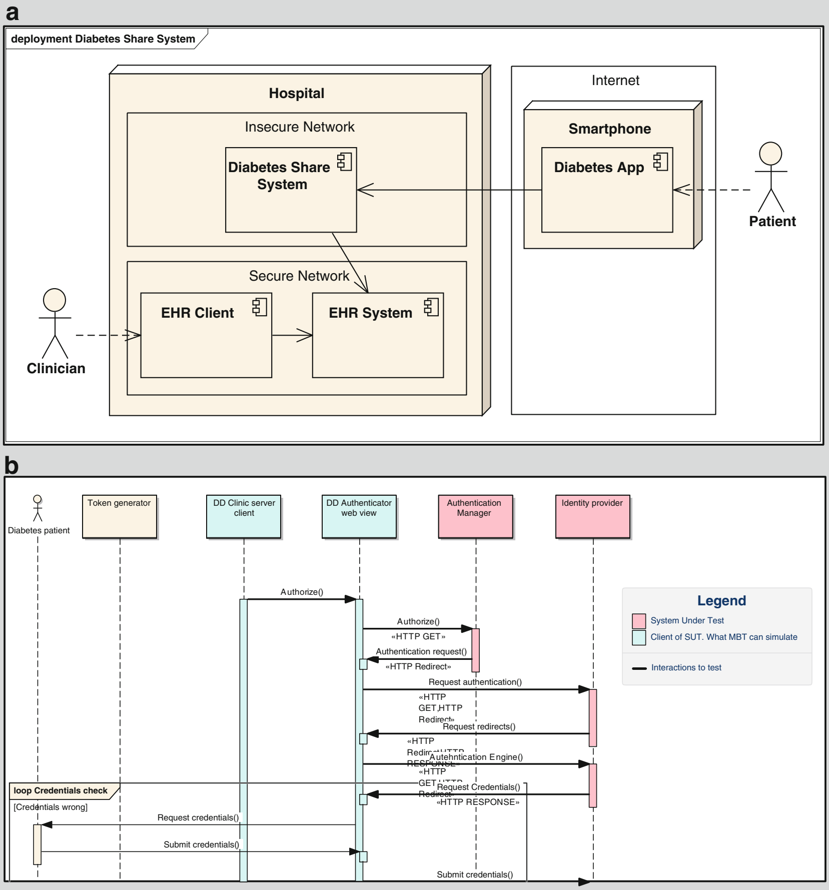


Fig. 8.9 Case study: (**a**) UML DSS architecture, (**b**) UML Sequence diagram of the DS1.14.1 Patient Privacy feature

8.3.5.3 Iterative Prototype Analysis and Review

For example, for development of the DeSA graphical user interface screens, we have used both kinds of artefacts successfully. We first presented paper-based and whiteboard sketches (monochrome wireframes) during initial requirements inquiry to help focus on overall functionality rather than design details. These were recorded as photos (Fig. 8.10a) and used in preparations for the next increment during which we presented digital wireframes first (Fig. 8.10b), followed by interactive prototype screens on the smartphone (Fig. 8.10c) based upon consensus and ideas resulting from the wireframe session.

Figure 8.10c shows on the left hand side two screens from the first interactive prototype demoing the DeSA GUI idea from Fig. 8.10a. This variant was later on refined and re-organised based on patients' feedback and additional interaction designer inputs as shown on the right hand side of Fig. 8.10c.

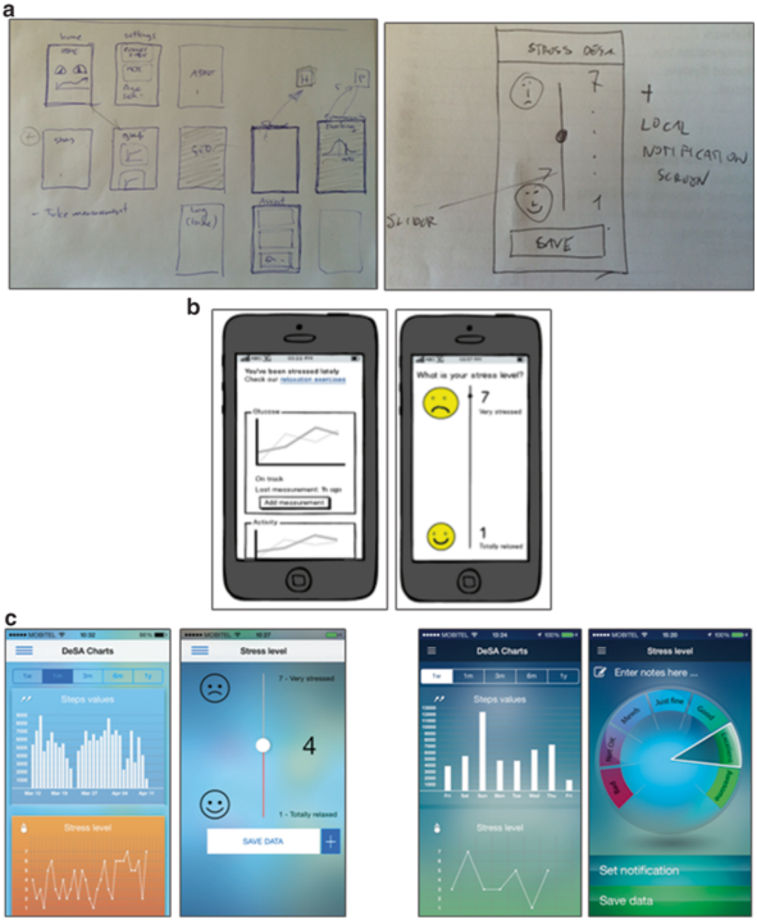


Fig. 8.10 Case study: (**a**) Initial low-fidelity wireframes (sketches) of the DeSA GUI, (**b**) digital wireframes of the DeSA GUI, (**c**) interactive prototype of the DeSA GUI

As part of the requirements analysis and validation process we employed prototyping in the workshops with end-users to elicit new requirements and also to validate previously specified ones (prototype reviews). We used wireframes with varying fidelity and interactive prototypes incrementally and per system feature (with graphical user interface mock-ups). These became both specifications and a basis for analysis. At the time, the prototypes did not meet all feature and quality properties but were fully functional. For evaluation of the stakeholders' degree of delight or annoyance (quality of experience) we used questionnaires and digital recordings of the sessions.

8.3.5.4 Tools

We used a mix of software tools for specifying and managing the requirements. Different team members used them for different purposes and requirements were specified on different levels of detail in the process. To avoid inconsistency and managerial chaos we implemented a simple scheme for traceability based on application-native hierarchical structures and labelling of requirements with numbers. This labelling was applied already in the vision statement definition (in the Vision Document) and present down to code unit level and logging. Table 8.8 gives an overview of these tools.

Table 8.8 Case study: Used requirements specification tools

Tool	Used for	Negotiation	Analysis	Traceability	Storage
SparxSystems Enterprise Architect	UML Modeller		X	X	X
	UML modelling was used on a high level to keep track of relationships between stakeholders, requirements, features and application modules, to define system boundaries, feature scope as well as to prepare system deployment diagram, architecture and usage scenario flows.				
MediaWiki	Web-Wiki	X		X	
	Development progress, quality and status were reported on a project Wiki, making this information available to the team, the stakeholders and project partners.				
Atlassian Jira	Issue Tracker		X	X	X
	Developers mainly used an issue tracker for specifying and breaking down features into units-of-work useful for the development process. This tool supported traceability and reporting so that progress and code units were traced back to the system features and corresponding stakeholder goals.				
Microsoft Office Word	Word processor	X		X	
	For negotiation with stakeholders we used text documents written in natural language with descriptions of design, RE specifications and status, including UML views of requirements and architecture.				
Microsoft Office Excel	Spread sheets		X	X	X
	Spread sheets were used to track mapping between system features and designed system components using the pre-defined application-native labelling.				

The tools were chosen pragmatically according to needs and available usage skills and were used to the extent necessary for progress. However, as we were building the medical applications we were also obliged to meet requirements on traceability and documentation as stated by the IEC 62304 [11] standard and implemented that as described.

8.4 Discussion

As presented in the case study, we made an effort to implement all basic RE steps as defined in the guidelines. Key lessons learned from this experience and some crucial take-away messages to practicing engineers, developers, researchers and stakeholders are provided hereafter.

The guidelines propose preparation of project-specific RE plan, which allows for optimised dynamics planning. However, we had prepared the project's time plan at the time of EU project proposal preparation. This had imposed considerable time constraints on the RE, resulting in a plan for engineering and development dynamics for the duration of 24 months. The approach was incremental, organised into two major iterations (alpha and beta), and using a pragmatic engineering approach with agile elements as recommended. Compared to waterfall methodology, this allowed for flexibility and adaptability at all times, which was particularly important during stakeholders interactions and engagement. Also, it facilitated prototype-driven engineering, which was an important excitement element for all involved parties and was positively stimulating the progress. However, the chosen approach required additional RE management efforts in order to assure that all important RE elements were covered and that the process converged according to plan.

Good understanding of domain specifics is emphasised in the guidelines, and this was re-confirmed in our case (Table 8.9). We recommend to plan for one comprehensive RE phase at the beginning of the project to establish in-depth understanding of the context. Also, in our case one of the team members was a digital health expert and a type 1 diabetic, and we had the benefit of already established tacit knowledge from previous projects. This was extremely beneficial as it allowed us to shorten the tacit knowledge establishment phase and outline the vision statement and value case very early in the process.

The case confirmed also the importance of stakeholder involvement. We had an already established link to some stakeholders in the hospital (diabetology department personnel, diabetes patients) as well as a user base of diabetes type 1 patients from a previous project, which again was very beneficial as it allowed us to shorten slightly the stakeholders' profiling phase. However, this bore a negative consequence in the fact that we did not analyse the stakeholder landscape thoroughly enough, and underestimated the importance of two types of stakeholders, IT administrators and researchers. This imposed delays to the RE process due to late identification, profiling and engagement of these stakeholders, and due to limited availability and some reluctance to participate in the RE activities from their side. We therefore recommend all practitioners to pay considerable attention to stakeholders' identification early on and double-check that they have identified all

Table 8.9 Healthcare-specific aspects of RE that the engineers and developers should pay attention to

Step	Specifics of the healthcare environment
Project preparation	Healthcare specialists, patients and personnel, legal, regulatory and social sciences experts should be part of the multidisciplinary RE team. Consider security, privacy and data handling legislation and governance rules. Ethical approval or other similar permissions for the project from the involved healthcare organisations should be obtained as soon as possible. Plan pragmatically; this will help you deliver a real-world product that is accepted by stakeholders.
Stakeholder identification	Establishment of tacit knowledge is crucial for the success of the project. Medical personnel, IT department representatives and regulator representatives will be crucial players, but their availability and readiness to cooperate will be constrained in time. Double-check that all relevant stakeholders have been identified and involved. Make sure that stakeholders have or acquire ownership to the system and the process, to help in getting access to them for elicitation.
Requirements elicitation	Prototypes (and GUIs in particular) are a highly recommended tool to inquire, illustrate and validate functional and user experience requirements in situations where patients and medical personnel have only a vague understanding of what is to be developed. Dedicated workshops help to establish constructive communication and cooperation between RE engineers and patients, medical personnel and customer representatives, especially those from the IT department and legal/security office. Multimedia can be a powerful communication channel to capture, discover and understand the healthcare context.
Requirements validation	Engaging patients, medical personnel and regulators and giving them opportunity to contribute will considerably increase chances for high acceptance of the system in practice. Establishment of shared understanding is crucial and will help them understand the true value of the system.

relevant players in the domain. Also, we advise the involved stakeholders to engage proactively in the RE processes and try to be available. This will enable the RE team to have deeper understanding of the problem and better chances to deliver an applicable and useful solution.

For research, the implications are on new methodologies and processes that will facilitate motivation of stakeholders and establishment of good-enough understanding on their side. This will lead to proactive stakeholders' engagement and hence increased adoption of the solutions. Furthermore, specifics of digital health come from the fact that the domain is heavily regulated. Presently, digital health infrastructure in Europe is heavily fragmented. Healthcare infrastructures are implemented based on individual choices of individual institutions and there is a lack of national and cross-border regulation. Further research is necessary in the context of European and national legislations, and guidelines for global regulation strategies are needed. RE research should focus also on development of concrete security and data handling requirements patents.

8.5 Summary

With rising trends on diabetes prevalence and further transfer of treatment responsibility upon patients, awareness of "self-care treatment" is becoming increasingly important. In this context, new technologies present immense opportunities for innovative digital health solutions and novel patient pathways, by putting high computing, integrating and presenting power into the hands of the patient, hence helping them to become more autonomous and achieve increased quality of life.

This chapter provided an insight into requirements engineering specific in digital health domain from a practical perspective. It provided guidelines for implementation of requirements inquiry in a clinical environment. This included recommendations for project-specific preparation of RE plan with incorporated elements of iterative, incremental and agile engineering, an insight into thorough stakeholders' landscape research, tips how to establish comprehensive tacit knowledge and how to identify and engage crucial stakeholders, and how to elicit and document requirements pragmatically yet to appropriate level of detail. Next, a real-world case study was shown for the case of the diabetes share system, which was engineered and implemented at the Hospital of the University of North Norway in Tromsø. Experience gained through this case have shown that the key to succeeding and achieving high adoption rates in daily practice lay in the following requirements:

- Digital health systems can only reach long-term patients' and caregiver needs and provide acceptable and trustworthy services if integrated into the official healthcare services.
- The key to successful adoption into daily practice and establishment of trust lay in patients' empowerment and ownership over their personal data, and assurance of high level of security and privacy.
- Establishment of tacit knowledge, early identification and adoption of patients, medical personnel and regulators and establishment of shared understanding are crucial for success of such systems in practice.
- Requirements engineering is a vital discipline in digital health systems engineering that establishes understanding and leads to fulfilment of goals and expectations, and should hence be studied and appreciated for its importance by practicing engineers, developers and researchers.

This opens also new avenues of research, in particular in the domains of security, privacy and data handling, legal aspects and regulation strategies in Europe, as well as innovative RE practice for digital healthcare. Advancements in these areas will help strengthen trust in digital health systems and will lead towards successful roll-out of such systems into daily practice.

References

1. Topol EJ (2012) The creative destruction of medicine: How the digital revolution will create better health care. Basic Books, New York
2. Pohl K, Rupp C (2010) Requirements engineering fundamentals. Rocky Nook Inc, Sebastopol
3. Martin S et al (2002) Requirements engineering process models in practice. Paper presented at the AWRE'2002
4. Velsen LV, Wentzel J, Van Gemert-Pijnen JE (2013) Designing eHealth that Matters via Multidisciplinary Requirements Development Approach. JMIR Res Protoc 2(1):e21
5. Vasiliki M et al (2007) Identifying healthcare actors involved in the adoption of information systems. Eur J Inf Syst 16(1):91–102
6. Mays N, Pope C (1995) Qualitative research: observational methods in health care settings. BMJ 311(6998):182–184
7. Morgan DL (1996) Focus groups. Annu Rev Sociol 22(1996):129–152
8. Pohl K (2010) Requirements engineering. Springer, Berlin
9. Glinz M, Fricker S (2012) On shared understanding in software engineering. SE 2012: invited paper
10. European Commission, Future Internet—Public Private Partnership Programme (FI-PPP) (2014) Future Internet—Socio-Technological Alignment Research (FI-STAR). www.fi-star.eu Accessed 14 Jun 2014
11. IEC 62304:2006 (2006) Medical device software—Software life cycle processes. International Standard, International Electrotechnical Commission

Chapter 9
Barriers and Strategies for Scaling Innovative Solutions in Health Care

Jakob Rasmussen and Mats Löfdahl

Abstract European countries are facing an increasing challenge of funding the public health care programs. In other industries, technology and innovation have provided improvements in efficiency and effectiveness that have reduced *costs* and improved productivity. Similar cost reductions and productivity gains have long eluded the industry of public health care. New generations of technologies are promising to bring those gains to the public health care sector in the form of innovative solutions built on new generations of information technology. However, several barriers remain that prevent these innovative solutions from scaling across the European health care system. These barriers are examined and strategies to circumvent them are proposed to aid developing scaling strategies.

9.1 Introduction

Europe is facing an impending health crisis. The cost of providing health care to European citizens is rising faster that the economy of Europe is growing. At the current rate of growth, the European countries might not be able to cover the costs of public health care systems in the near future. There are many reasons for this development including aging populations and rising costs of innovative treatments. However, unlike other industries, the health care industry is not experiencing that innovation is driving down costs. Defiant of economic logic, innovations in health care provisioning seem to drive costs up with increasingly expensive treatments with each generation of innovation. To combat this, some European governments have shifted to procuring older generation medical devices or shifting to generic medicines to drive costs down. However, this has the adverse consequence of decreasing demand for innovation and putting strains on the R & D budgets for European

J. Rasmussen (✉)
Living Labs Global, Copenhagen, Denmark
e-mail: jr@livinglabs-global.com

M. Löfdahl
Blekinge Institute of Technology, Karlskrona, Sweden
e-mail: mats.lofdahl@bth.se

S.A. Fricker et al. (eds.), *Requirements Engineering for Digital Health*,
DOI 10.1007/978-3-319-09798-5_9

firms. To avoid having to scale down quality of service, European governments increasingly have to look at opportunities to increase efficiency, effectiveness, and productivity. One option is the prospect of introducing information technology and automation into the health service provisioning at scale.

In many industries, information technology and automation have significantly increased productivity and decreased costs of service provision [1]. The primary drivers have been more efficient and effective operations. As an added benefit, the advent of technology and automation has also led to new strategic opportunities, such as the availability of new services or new options for communication. A wide range of industries have seen new technology-driven business models emerge, including logistics, retail, and entertainment among others. Increasingly, health care is targeted as a market for similar development. However, public provision of health care still seems to be resistant to the opportunities of technological innovation in the shape of information technology.

Information technology can potentially have similar positive effects on costs in the area of health care. As some of the cases in this chapter show, on the patient level applications for screening conditions online before visiting the doctor can reduce the number of unnecessary visits, thereby reducing costs or freeing up resources for more serious conditions. Services that link patients or relatives with medical personnel through means such as teleconferencing can offer new opportunities for delivering health care. As another of the cases in this chapter shows, it can for example allow patients to stay at home and thus reduce costs and at the same time improve quality of life for patients and relatives.

Across Europe, new solutions emerge that address these and similar challenges, and that provide opportunities for improving efficiency and effectiveness, as well as provide new strategic opportunities for delivering health care and improving quality of life. However, to have an impact on the cost of providing health care across European countries it is central that these solutions can scale both locally and across Europe.

Scaling is important for many reasons. Scaling allows providers to drive down the cost of solutions, as the costs of R & D can be divided across many customers. To have a significant impact on the cost of delivering health care in Europe, the savings and productivity gains have to be significant. This requires the new and efficient solutions to substitute a large enough part of the current and less efficient services to create measurable impact. Many solutions based on information technology harvest their gains in efficiency and effectiveness from phenomena such as network effects [2] that by their nature require implementation at scale to have relevance. Finally, the cost of technology adoption should not be underestimated [3]. Technology-shifts require significant investment in society to introduce new procedures and competences; investments that often have to be made upfront and that can be of such magnitude that significant adoption is required to justify the upfront costs.

This chapter provides an introduction to the barriers to scaling in Europe, and discusses some of the options available to providers of solutions for the health care industry to overcome or circumvent these barriers. It focuses on a few key concepts as a framework for understanding the basic market dynamics.

9.2 Terminology

The organizations financing the provisioning of health care, such as regional health procurement authorities, the state or national insurance providers are called *buyers.* The firms or other organizations developing and selling solutions to the buyers using information technology to improve the delivery of health care are called *providers*. There are many providers selling solutions or products to the buyers. However, the special emphasis in this chapter is on providers using *information technology* to develop new solutions to improve efficiency, effectiveness, or create new strategic opportunities for delivering health care to the citizens in European countries. These solutions can also be called *technological innovations.* The area this chapter is especially focused on is the process from when a solution has been developed, piloted, and perhaps sold in a local market and then is ready to be sold outside of the local market. This process is called *scaling* which is defined as the process of selling the solution many times over to different buyers across Europe.

9.3 Barriers to Innovation

The dominant explanation for the spread of technological innovations emphasizes processes of influence and information flow. The fundamental diffusion of innovation is often seen as a process in which organizations that are connected to preexisting users of an innovation learn about it and adopt it. The innovation then slowly diffuses through the networks of organizations tied to the early adopters. However, it is increasingly understood that organizations have internal barriers to innovation that result from lack of technical know-how, political and power issues, operational constraints, and other factors that prevent them from effectively adopt innovations as they arrive [4].

The public health care industry contains several barriers to efficiently adopting technological innovations. The barriers might explain why the public health care industry is currently slow at adopting new technologies and innovations. The slow adoption of new technologies and innovations in turn decreases the rate at which efficiency and effectiveness gains are harvested by the public health care industry. The consequence is that costs are higher than they would necessary have to be. The problem is further exaggerated by exogenous factors such as aging populations that are more care intensive, thus increasing the adverse consequences of having higher costs and less productive health care systems.

Another challenge is that piloting of new innovations in health care usually can take a long time. The health care industry is highly regulated, which poses a significant challenge to scaling. There are considerable requirements for documentation of safety, compliance with procedures, quality, and the economic benefits of the innovations that needs to be met to introduce solutions to the market.

Furthermore, important innovations in health care to replace or improve existing solutions are rarely revolutionary quick-fixes, but can take many years to succeed and acquiring approval. It can be difficult to relate savings, efficiency gains, and health gains in health care to a single innovation because it takes a very long time to develop and implement. Consequently, many other developments can influence the final result of innovations.

Organizational factors also need to be taken into account. Doctors and managers can be important barriers. Power structures, jobs, budgets, and other factors can affect decisions or can bias decisions toward solutions that maintain existing status quo.

Finally, the lack of common international and European standards is a perpetual challenge to scaling. Without standards, scaling becomes expensive and difficult, as solutions have to customized to each health care system. The idea of Big Data, for example, promises significant opportunities for developing new solutions that can harness the data kept by the health care sector and transforms it into new solutions, and has already been used in areas such as infection and disease surveillance. However, the quality and accessibility of Big Data still needs be adequate and standardized to support scalability of solutions across Europe. Consequently, as new solutions need to prove safety and efficacy to be accepted into the procurement systems, the above factors contribute to the uncertainties and therefore business risk associated with scaling.

In 2010, a study was conducted on societal economic efficiency gains of the services of the Swedish start-up iDoc24 [5]. The provider was pioneering teledermatology. The service allows the patient to send an image of any skin anomaly via MMS to a team of trained dermatologists for quick and efficient evaluation. The dermatologist provide the patient with medical information for self-treatment which includes a most probable diagnosis, information, treatment possibilities, and if the patient needs to see a doctor in person.

The service offered several advantages for citizens, industry, and public health care providers. The solution adds value to the health care system as it reduces costly visits to the doctor. Insurers may discover the service as an attractive and low-cost addition to their portfolio of services. iDoc24 is also attractive to mobile phone operators gain revenue from billing services and data usage, as do application resellers like Apple's App Store receive a commission on selling the software or service. Doctors benefit from an extra revenue stream by providing diagnoses based on images. Users, benefit from confidential and anonymous responses to their enquiries, saving them a trip to the doctor. However, the provider found it very difficult to get the public health care authorities to realize the benefits and to procure the services and make them available to citizens. The main challenges were that public health authorities found it difficult to justify why the public health service should pay for additional services that were already covered by the standard provisioning of general practitioners and dermatologist. The consequences for the solution were thus that the buyers—in this case the public health authorities—were not willing to make the solution part of the offering of the public health care system.

To understand the business case, a study of the economic and societal upsides was made. In Sweden, it is estimated that 15 % [5] of all general practitioner visits are skin-related. The data from iDoc24 showed that 50 % of the tele-dermatology MMS sent during the first pilot resulted in the user not having to visit the doctor. The service could potentially save up to 50 % of all skin related visits to the doctor. Since there an approximate 14M visits to general practitioners every year in Sweden, tele-dermatology could ultimately save around 1 m visits to the doctor. At EUR 170 costs to society for a visit to the doctor's the cost savings for Sweden could reach EUR 170 m per year [5]. The savings could either be reinvested in doctors using their capacity on other illnesses or reinvested in better treatment in other area.

Of even more interest is the potential of scaling of the technology to serve an even larger market. With 7.4Bn visits to general practitioners in OECD countries the potential costs savings could reach EUR 94Bn [5]. A simple service such as an MMS-based tele-dermatology application could suddenly have a potentially massive impact on the costs of health care provisioning across the OECD. The benefits of this being a more efficient health care system, the ability to shift spending to other areas, job creation in application provider providers such as iDoc24, additional tax revenues from jobs and so on. The direct dynamic effects would thus be considerable.

In the summer, a pilot study was conducted in a popular Swedish beach area. The result was that a considerable number of images of the private parts of teenagers were received at iDoc24. In the beginning they thought this must be teenagers joking and abusing the free MMSs that came with the pilot. However, they soon realized that it had a more serious side. In the anonymous context of tele-dermatology, teenagers were more willing to inquire about potential symptoms of sexually transmitted diseases (STDs). iDoc24 had stumbled upon a potential solution for a massive societal problem that countless public information campaigns had not managed to solve. iDoc24 allowed teenagers to quickly inquire about potential symptom of STDs, which in turn allowed them to get treatment quickly. The positive effect of this is of course massive. The earlier STDs can be diagnosed and treated, the less chance the teenager has of infecting others. The earlier STDs can be diagnosed and treated, the less expensive it will be to treat and the less severe the long term effects. The personal and societal upsides of this are considerable, as are the economic upsides.

Even though the iDoc24 calculations are vastly simplified, and does not take into account challenges such as false positives, liability and potentially increasing the number of request as costs and the hassle of going to the doctor is remove, it makes a point in how the business case for new solutions can also be calculated. However, in the long term better and more scientifically valid methods for more comprehensive cost-benefit, impact and return-on-investment analysis in the area of new solutions in domain of health care could be of benefit, to create standardized and comparable measurements of efficacy.

There are countless other technology providers developing new ways of approaching societal health care challenges with technology and innovation. The Human Diagnosis System[1] is trying to create an open diagnostic system for the

[1] https://www.humandx.org/.

global medial community. Mobile Fitness[2]is creating municipal platform for promoting exercise and healthy lifestyles. Mobile Wellbeing[3] provides personal health monitoring.

When analyzing the business cases the economic and societal return-on-investments are often very positive. However, most of them find the same barriers to get their technologies to market. As a consequence of the above, iDoc24 has today launched a company[4] focusing solely on STDs and launched it in the USA. Not Europe. However, with the considerable public spending on health care, the European health care market could constitute a significant lead market [6] for similar innovative services. This would be provided that the procurement systems were more embracing of solutions to existing challenges in health care based on services.

The prospect of using services and information technology to create impact in the area of public health is an increasingly attractive option for health authorities. Traditionally, many health procurement systems are built around medicine and medical devices [7]. This leaves a blind spot in the procurement services that can have disruptive effects on the health care system and the provisioning of health. In 2013, the City of York[5] opted to approach the problem of unequal access to health in a new way. The problem was that even though life expectancy was higher than the national average at 79.6 years for men (England 78.3) and 83.2 years for women, health is substantially worse in York's most deprived areas. Furthermore, there is a gap of nearly 10 years in life expectancy for males between the most and least deprived communities. Instead of implementing specific programs designed and funding by health authorities, York opted to pose the problem as a challenge to the international business community. The challenge was to present existing solutions that could increase physical activity particularly in men aged 35–65. Solutions were proposed from across the world. The City of York finally selected a solution from an organization in San Francisco called Sunday Streets. The solution was quite unorthodox in that it reuses existing assets in society, in this case streets and local community leaders, to create recreational spaces. By removing cars and other obstacles on Sundays, the streets are clear and local events involving physical activity are arranged. The events furthermore have the advantage that they span different communities, thus breaking isolation and opening up the local communities.

While being low-cost and low-footprint, the solution brings both economic and social upsides to the community. It also taps into the idea of a sharing economy [8]. By utilizing existing unused assets and evolving business models around sharing such assets, solutions such as Sunday Streets can scale quickly and at low cost. This creates the opportunity for a significant return-on-investment in a short time, a highly attractive proposition for targeting societal health challenges as well as raising capital. However, utilizing publicly owned assets often requires special permissions and adherence to regulations such as safety and environmental

[2] http://www.mobilefitness.dk/.

[3] http://www.mobilewellbeing.com/.

[4] http://stdtriage.com/.

[5] http://llga.org/.

standards. To a certain extent, solutions reliant on access to publicly owned assets require an active involvement of local governments, and can get into trouble with procurement regulations if a private company obtains unfair access to public goods.

An increasing number of communities are taking the opportunity to rethink their procurement systems to harness innovation and radical solutions rather than routine thinking when it comes to health. Depending on the design of the health care system and the cost structures associated with this, different parts of the patient lifecycle can be distributed over different political structures. In European countries where prevention and recuperation is the responsibility of the individual municipality there can be incentives to down-prioritize prevention. There can be many reasons for this, including that it can be less expensive for municipalities to save on prevention and rather have citizens hospitalized or that the effects of prevention are long term and thus key priority for short-term election cycles. The lack of focus on the total cost of care can be costly for society, since prevention in many cases is less expensive than treatment.

To target these challenges, the Steno Diabetes Center,[6] a research foundation owned by Novo Nordisk A/S, has worked with the societal challenges of health care. They have taken a different perspective on prevention. Many of the costs that emerge in the health care system as costs of treating lifestyle related diseases, such as obesity, diabetes, and hypertension might actually have their root cause in social factors. Factors such as social isolation and poverty, often contribute to a lifestyle that puts the individual citizen at risk. Traditional methods of the health authorities communicating better lifestyle choices are often failing to the target groups for various reasons such as that they do not listen, they do not consume the information through the media channels used by the health authorities, or that they simple prefer their lifestyle to compensate for their situation. New and innovative solutions are thus required to tackle the challenge of reducing costs of treating lifestyle-related diseases. As seen with York, many of the innovative solutions are more focused on changing behavior through community action or leveraging consumer technologies. Some of the focus areas of the Steno Diabetes Center's work with municipalities, for example, are to focus on balancing risk factors rather than eliminating them, i.e., a holistic and positive approach. This makes marginal lifestyle changes more palatable, and thus more effective on the societal level.

Another approach has been seen in Canada[7] where the Portland Hotel Society is experimenting with teaching extreme alcoholics to make their own booze. On the surface, this might seem completely counterproductive. But apparently, it has positive effects. One of the effects is that the alcoholics reduce their intake of alcohol that has been produced in ways that are harmful or even poisonous, and exchanging this with alcohol that is produced in the right way. This has an immediate health impact. Furthermore, the brewing options create other effects such as pride, community, and other factors that for some can help them balance their alcohol intake.

[6] http://steno.dk/.

[7] http://www.cbc.ca/news/canada/british-columbia/portland-hotel-society-teaching-alcoholics-to-make-booze-1.2543588.

In Eindhoven, the Netherlands, the authorities have experimented with rehousing drug addicts before they are being put through rehabilitation programs. This has had positive effects on reducing relapses, as having a home provides stable base and often keeps the drug addict away from the streets and other environments where the temptation to break the rehabilitation program is increased. In Västervik, Sweden, the authorities have experimented with providing teleconference facilities to elderly couples where one suffers from a degenerative disease, such as Alzheimer. This allows the sick person to stay at home longer that would otherwise be advisable, and thus save significant costs for places in care homes [9].

A challenge to many of the solutions invented to solve specific problems in health is the fragmentation of the market. Municipalities in Europe have a tendency to spend funding to solve a specific problem locally. Often that might involve being inspired by solutions developed elsewhere, but asking a local provider to come up with a similar solution. There can be many reasons for this type of decision, including that the municipality might trust the local providers more than they trust providers from outside the region. This can create a preference for choosing local providers to implement untried solutions as these carry additional risk. There might also be political pressure for municipalities to spend public money on local providers, based on the premise that the money therefore stays in the local economy and create jobs and dynamic effects.

By asking local providers to reinvent existing solutions, the municipalities are in effect asking the local providers to do customized solutions and end up paying for the entire R & D process. There is little learning as the local providers have to develop the solution for the first time and thus invariably repeat the mistakes of other solutions developed before them. If the municipalities instead bought the best-in-class solution already available from the global market, the municipalities could share the costs of R & D between them. The municipalities could then spend the cost-savings on other areas in need of funding.

Buying from a few solution providers globally, instead of ordering custom-made solutions would also mean that the average solution provider got to do more implementations. Doing more implementations create learning from repeat implementation that would benefit the municipalities. Allowing a few providers to do repeat implementation also has the chance of creating dominating standards that can subsequently be used as platforms for add-on services and other innovations. This would allow local providers and start-ups to invent and market new products using the dominating standards as a sales pipeline.

The decision to fund the R & D of local providers is often based on the promise of these providers developing services that can subsequently be sold to the global market. However, as a large number of municipalities are subscribing to this idea, many providers do not get to sell their solutions to the global market, as all the prospects are inventing their own solutions. Making is difficult to sell solutions outside of your home region, makes it costly to sell solutions and inhibits growth of the providers. This reduces economies-of-scale in services economy. It also has the effect that many—especially smaller—municipalities are not offered the available solutions. As they might not have the budgets to fund a local provider to custom-develop a solution, some challenges in smaller municipalities are simply not solved. This has a potential welfare loss as the positive effects of technological shifts are not available at the same level and scale for the part of the population living in smaller municipalities. The existing practices thus work detriment to establishing an efficient global market for service innovation. The consequences are often more expensive solutions and less welfare technologies available to the municipalities.

9.4 Strategies for Scaling Digital Health Innovations

The health care sector in Europe is not a single homogeneous market [7]. The European Union's member states have different health care regulations and have national variations in their procurement systems, even though procurement is regulated on the European level. Furthermore, several of the major European markets have special certification systems, special procurement systems, or are structured slightly differently. All of the above makes adoption to local market conditions pivotal to scaling across borders. Numerous languages as well as cultural and legislative differences lead to market fragmentation and make it costly for any business to scale efficiently in Europe.

Procurement poses a specific challenge to scaling solutions aimed at the public health care sector. Depending on the nature of the solution, it can be procured directly through a call for tender procedure initiated by the hospital, health authority or municipality, can be added to the list of solutions approved for procurement at the local hospital pending a review by the procurement committee, or can be part of a framework contract. The process poses many barriers to diffusion of innovation as it involves many stakeholders that first need to be made aware of the existence of the solutions before they can actively start a process of evaluating the solution for potential procurement. Making stakeholders aware can be costly and time-consuming, and can be very difficult since the decision-makers can be difficult to reach. Once awareness has been established, stakeholders and decision-makers need to be convinced that the solution is in fact improving current state of the art. For many medical technologies there is a requirement that a technology review and cost–benefit assessment is conducted that can prove how the solution can reduce costs and/or improve on current solutions available and in use.

Furthermore, any new solution might change power structure, ownership, or in other ways adversely impact certain stakeholders. This in turn can create resistance to change disregarding the potential of the solution. There might be local requirements that require expensive customizations or favor local providers, or political pressure to buy local. This might lead to standardized solutions being disregarded instead of local customized solutions that are more expensive, or tailored to the demands of local stakeholders. Finally, many public health care systems in Europe are known for taking a long time to settle their invoices, leading to significant cash flow challenges for providers.

The procurement process thus introduces costs and uncertainty for external providers. The process also takes time and creates other timing problems. Procurement lists are typically reviewed only once a year. Framework contracts are often negotiated for 5 years at a time, locking down the market until the new wave of contracts are negotiated. Tendering procedures take time to complete and subsequently start delivery. Payment times might negatively impact cash flow, preventing small solution providers from reinvesting profits into further R & D and growth.

In Tromsø, the team behind the solution Diabetes Share System (DSS)[8] has tried another way of developing solutions for the public health care system. Instead of develop the solution first and then marketing it, the aim is to co-develop the solution with the representative of the local public health care system, and then subsequently diffuse the solution to partners in other public health care systems across Europe. The development and subsequent sales process thus more resembles co-creation and collaboration, rather than traditional internal R & D and subsequent marketing and sales. The DSS is a solution that addresses the problem of managing blood glucose levels of diabetes I patients. Ideally, blood glucose levels can be managed through effectively balancing intake of insulin and carbohydrate, physical activity, and reducing stress. However, for many patients managing their lifestyle requires support from relatives and surrounding in addition to medicine and monitoring by health care professionals. Management of diabetes I is thus as much a social challenge as it is a medical problem. Given the geography of Norway, frequent monitoring and interacting with patients face-to-face is not feasible. Consequently, the DSS solution allows virtual communication between patients, relatives, and health care professionals.

By co-developing the solution with the local public health care system the DSS not only get a closer integration and feedback from the health care system on the performance of the solution. The team behind the DSS can from the onset make the solution compatible with the business system, organizational, political, and other soft factors that might not be directly related to the functionality requirements of the solution. Furthermore, the solution can be validated by the local health care system, which in turn might improve the chances of positive reception in other public health care system across Europe. Finally, awareness about the DSS can be diffused through the networks and contacts of the health care professionals in Tromsø, providing a cost-efficient network-based marketing channel for subsequent scaling of the solution to other public health care system.

Some solution providers consider the option of targeting the business-to-consumer (B2C) markets to scale their solutions, as an alternative to targeting the business-to-government (B2G) markets.

Started by a group of McKinsey consultants, Endomondo[9] created an application for fitness enthusiasts that could be used on mobile devices. The application combines features such as recording statistics and information relation to the sports the

[8] http://www.telemed.no/runkeeper-in-the-diabetes-diary.5387240-77933.html.

[9] http://www.endomondo.com/.

user fancies to making the user part of a social network around the particular sport the user is participating in. From the beginning, they targeted consumers, in this case a clearly defined target group of running enthusiasts. Though the provider had a hard time in the beginning getting a grip on the market, with the help of investors, they launched the application in the USA. That led to a sudden rise in users and subsequent considerable scaling.

An application like Endomondo promotes a healthy lifestyle through exercise and uses incentives such as being part of social community around sports. The aim is thus similar to exercise advice from the health authorities and public health aims to combat for example lifestyle relation diseases. However, instead of selling the application to the health authorities, providers such as Endomondo might find it easier to go directly to the consumers. Aiming for the consumer markets carries many advantages such as being able to reduce the set of features required to go to market, faster market introduction, working with clearly defined target groups, faster payment cycles, and less or no need for certification.

When citizens can start taking ownership of their own medical data, new opportunities emerge. Citizens can use the new solution to connect health care providers as well as other citizens with similar conditions. They can ultimately take more control of their lives.

However, it can subsequently be difficult to reenter the public markets. The case of Microsoft's health vault[10] serves as a case in how difficult it can be to market a product aimed at the consumer market and subsequently trying to use this as a lever into the public health care systems.

As an alternative to using the procurement of services through the public health systems to scale the solutions, providers can opt for targeting the consumer markets of the business-to-business (B2B) markets instead. For some solutions, this might provide better alternatives for scaling.

Cure4You[11] started in Denmark where they provided online booking systems for general practitioners aimed at reducing costs and improving patient communications. Cure4You managed to subscribe a large part of the practices in Denmark to their online portal. The business model was based on the platform and basic functionality being provided free-of-charge, with the patients having the possibility to buy extra services for a fee. As Cure4You did not manage to have the public health care system pay for the services, the provider instead scaled in the UK, India, and the USA targeting doctors and patients in the same way as in Denmark. By directly targeting general practitioners, who have large autonomy over how they manage their practices and what services they want to offer, Cure4You could scale quickly to get critical mass and economic-of-scale that allowed them to finance development and expansion outside of their home region. However, the expansion path quickly followed a pattern focusing on the economies with large autonomy in the B2B segment of the health care market. As with STDTriage, many European countries are thus quickly disregarded as potential markets and lose out on technology shifts and the associated efficiency gains associated.

[10] http://www.healthvault.com.

[11] http://us.cure4you.pro/.

Medichem[12] in the UK developed a solution in collaboration with a local pharmacy chain to track-and-trace medicine sold by the pharmacies using 3D barcodes. By co-developing the solution, Medichem had access to the competences and knowledge about logistics and business processes of the pharmacy. In return, the pharmacy got a first-mover advantage in terms of the benefits of the automated track-and-trace system. The benefits include cost-reductions in handling and dispensing of drugs, reducing of errors rate, reducing of costs during recalls, and improved customer services. By being able to validate the business case with one pharmacy chain, Medichem stands a much better chance of convincing other pharmacies to engaging to harvest the same advantages.

9.5 Discussion

The existing regulations and special market conditions in the health care industry create a number of barriers to scaling solutions in health care. In the following table, we have summarized the barriers identified in the chapter.

Summary of barriers to scaling

Barrier	Description
Non-local providers perceived as high risk	Public buyers prefer local suppliers to minimize risk and maximize the chance of the solution being compatible with local standards, technology, culture and politics.
Job creation stance	Public buyers prefer local suppliers to reinvent solutions, as this promises to create local jobs and to support the chance of their local suppliers becoming the next global vendor of the solution.
Local patriotism	Buying from a non-local provider can have a negative impact on the perception of the decision makers by the local community and give grounds to political attacks.
Additional investments required	Getting the first internal order can be a significant barrier for many providers. For small and medium-sized providers, expanding into the first international market can be a significant risk requiring significant resources.
Lack of trust	Public buyers have a tendency to prefer local vendors even though European procurement laws require them to make tenders above a certain size available to international vendors. Concerns can range from not trusting non-local vendors to difficulty encountered while validating references. In addition, non-local vendors can be difficult to control. Similar trust issues can be found in the consumer and the business markets. Although for the consumer markets, applications are increasingly bought from any global vendor. For the business markets, validated references can still play a significant role.

(continued)

[12] http://www.medichemonline.com/.

Barrier	Description
Lack of local networks	Many industries rely on local networks for resources. This creates advantages of proximity and agglomeration. However, providers that enter new markets have to build up these networks first. Therefore, it can be difficult and costly to get a foothold within the financial and time frames available to the provider.
Fragmented markets	Europe is a difficult market to scale in comparison to the USA. Slight differences in preferences, regulatory systems, special certification models, differences in the structure of procurement systems, language, culture, and religion makes uniform strategies to scale difficult to implement.
Burdensome procurement processes	Procurement processes can be complex, time-consuming, expensive, and opaque. Furthermore, they can create timing problems for providers that do not have the patience or cash to work on the timeline of the procurement process.
Impenetrable power structures	Decision-makers might not take decisions based solely on economic or technological criteria. Instead, they might try and preserve power even though it does not benefit the patients. Especially disruptive and radical innovations can upset the power structure and might thus have difficulties finding their way into the markets.
Additional certifications required	Certifications, local standards, and other specificities continue to play a role in local market acceptance. Even though European legislation continually strive to eliminate these and other technical trade barriers, many providers might still find that certifications are used to control access to procurement.
Complex interactions	Documenting efficacy and obtaining approval can take a long time and on the away be impacted by other developments in the field. Consequently, it can be difficult for solution providers to document the real impact of the solution.

Successful scaling would need to address the barriers outlined above. This is not an easy task. Minimizing the risk for buyers—perceived or real—requires both structural changes such as common European standards, and more subtle changes such as alignment of business cultures. However, for many decision-makers the perceived risk might also be linked to the lack of trust, which again rests on the lack of information. Today, it can be very difficult for municipalities and regional authorities to validate the references and implementations of non-local providers. It can also be very difficult for the non-local providers to understand in advance the peculiarities of other countries and market outside of their home region. Some providers circumvent these barriers by actively engaging in partnerships with local providers in the markets they want to expand into, while other providers elect to form partnerships with for example large infrastructure providers or other providers with cross-border experience. The difficulties for providers to enter other European regions often result in local providers reinventing solutions or products already invented elsewhere. Whether this is local patriotism or lack of intelligence that leads to the high degree of parallel innovation in Europe is difficult to conclude.

However, some municipalities in Europe, such as Barcelona and many municipalities in the UK such as York and Sheffield, have recognized that it is inefficient to invest resources into reinventing solutions already invented, tried, and tested in other places. Consequently, they elect instead to support providers to come their region by developing special landing programs or open procurement processes. The landing program scan provides advice, network, fast-track processes, and a host of other services that speed up the integration of non-local providers into the local business system. The open procurement processes actively involve non-local providers, and provide a high degree of transparency in contracts. Still, a major challenge for many European providers is the costs of expanding into their first non-local market. Due to the fragmentation of the markets, the costs can in some cases be equal to setting up an entire new company, or they can require considerable resources and management focus as described previously. Consequently, many European providers choose to invest their non-local scaling in the USA where the market is bigger, more homogenous, and potentially also more fast-moving. The European markets are then something the provider can later return to, once a considerable operational base has been secured. However, currently the European Commission and a number of infrastructure providers and technology companies are jointly developing a platform for scaling health care applications across Europe, named FIWARE. This development might change the picture in the future and facilitate easier scaling of health care applications across Europe by solving issues around standardization etc.

However, several strategies are emerging that can circumvent or lessen the impact of the aforementioned barriers to innovation. In the following table, we have summarized the strategies identified in the chapter.

Summary of scaling strategies

Strategy	Description
Co-development	Co-developing solutions with public health care providers, as seen in Tromsø case, can reduce the risks and uncertainties, and build critical trust with the health care provider. Furthermore, co-development ensures that the solution is already embedded in the local settings of the health care provider, and allows developers to use the network of the health care provider to scale the solution to other local providers.
Target business-to-consumer markets first	The number of consumer health care applications is growing considerably, and the barriers to access consumer markets have been significantly reduced via selling applications and solutions directly to users via for example application stores or the Internet. Targeting consumers directly thus represents a significant opportunity for scaling.
Target business-to-business markets first	The business segment, including private actors in the health care systems such as general practitioners, insurance companies, clinics, and pharmacies, can more easily take decisions on purchasing new solutions. These actors represent a significant untapped market. Furthermore, some of them are connected to the public health care system and can thus serve as a bridge to the public markets.
Transfer of ownership to citizens	Transferring ownership of data and responsibility for monitoring their conditions creates new opportunities for harnessing the power of citizens to either take control of their own health or to pressure the public health care systems to embrace new services. This strategy is still underdeveloped, and few successful cases can back the strategy up.

(continued)

Strategy	Description
Shared economy	Utilizing unused assets and focusing on connecting citizens or users of these assets represent a significant opportunity to scale solutions on very low-cost models. Some solutions such as community exercise are already tapping into this market, but there are still significant opportunities to identify other unused assets as well as to create and scale communities-of-interest.

9.6 Conclusion

In this chapter, we have provided an introduction into some of the barriers to scaling innovative solutions in health care and strategies that can be implemented to circumvent or reduce some of these barriers. We have seen that even though the underlying economics in the European health care systems facilitate introductions of innovation to reduce costs and improve care, there are several barriers to be taken into consideration while taking innovations to market and scaling business processes across the European countries.

The main barriers outlined in this chapter include that non-local providers perceived as high risk, job creation stance, local patriotism, that additional investments required to enter local markets, lack of trust, lack of local networks, fragmented markets, burdensome procurement processes, impenetrable power structures, that additional certifications are often required, and complex interactions between technology, innovation, and organizational development.

There is a number of existing strategies that can potentially allow products and solutions to be scaled. Strategies outlined in this chapter are co-development, targeting business-to-consumer or business-to-business markets, instead of public markets, transfer ownership of key assets to citizens, and looking towards the opportunities of the shared economy.

Further research is needed to elucidate additional strategies and to determine the ways in which they can be employed to help scale products and solutions targeted at the European health care sector.

References

1. Oliner S, Sichel D (2000) The resurgence of growth in the late 1990s: is information technology the story? Federal Reserve Board, Washington
2. Shapiro C, Varian H (1999) Information rules: a strategic guide to the network economy. Harvard Business School Press, Boston
3. Rasmussen J (2004) Business perspectives on E-learning, Copenhagen Business School, PhD series
4. Attewell P (1992) Technology diffusion and organizational learning: the case of business computing. Organ Sci 3(1):1–19
5. Esteban A, Haselmayer S, Rasmussen J (2010) Connected cities. Imperial College

6. Aho E et al (2006) Creating an innovative Europe: report of the independent expert group on R&D, European Commission
7. Rasmussen J (2007) Innovation financing in the European medical device sector, European Commission
8. Gansky L (Fall 2010) The mesh—why the future of business is sharing, Penguin Group
9. Rylander et al (2006) mWatch Europe 2006, Living Labs Europe