Hindawi Publishing Corporation
International Journal of Distributed Sensor Networks
Volume 2015, Article ID 549420, 12 pages
http://dx.doi.org/10.1155/2015/549420

Research Article

Safety and Privacy Considerations for Mobile Application Design in Digital Healthcare

Mojca Volk, Janez Sterle, and Urban Sedlar

Faculty of Electrical Engineering, University of Ljubljana, Trzaska Cesta 25, SI-1000 Ljubljana, Slovenia

Correspondence should be addressed to Mojca Volk; mojca.volk@ltfe.org

Received 31 July 2015; Revised 11 September 2015; Accepted 15 September 2015

Academic Editor: Namje Park

This paper presents a case study on security and privacy implications on the design of a mobile application in digital health, the DeStress Assistant (DeSA) app, which utilizes sensing technologies and capabilities of the Internet of Things (IoT). An analysis of the applicable legislative framework is provided and selected challenges encountered during the app design are discussed, which are related with the practical implications of provisions of the international and national legislation for software applications in general as well as medical devices and handling of sensitive data in particular. We provide insights into design choices, including different possible scenarios for classification of a mobile app as a medical device and the pertaining legal risks the app developer is faced with as a consequence of possible legal obligations, and different possibilities of specifying the intended use. Also, we propose two designs of a mechanism that enables secure sharing of the patient's health-related observations from the DeSA app with a medical professional within a treatment context. The first mechanism provides secure submission of health-related observations into a hospital information system, whereas the second mechanism enables secure short-term sharing of observations without storage.

1. Introduction

In this paper a case study is presented on security and privacy implications on the design of a mobile application in digital healthcare that utilizes sensing technologies and capabilities of the Internet of Things (IoT). IoT is a megatrend in next-generation communication and information technologies (ICT) [1], the rise of which can be to the better part attributed to advanced developments in communications and networking capabilities, sensor technologies, mobile computing, and cloud computing and network virtualization [2–4]. One of the most promising application areas for IoT is digital healthcare, an area that is currently undergoing fundamental evolution due to unprecedented demographic and socioeconomical changes of the modern society [5], which together call for a transition towards more affordable, pervasive, and patient-centred forms of care. IoT has the potential to give rise to many areas of digital healthcare, including remote real-time health monitoring, elderly care, chronic disease management, and fitness programs, by introducing a concept of a continuous treatment process requiring seamless information sharing across multiple healthcare professionals and various healthcare institutions in order to improve healthcare services and containment of related costs [6]. Digital healthcare in itself is a broad term that spans across a variety of areas, including eHealth, wellness applications, quantified self, health information systems (HIS), and Electronic Health Records (EHR). One such field of application is also mobile health (mHealth), which is a way of offering wellbeing and health-related services by utilizing the power of mobile devices, IoT, and sensor technologies. This particular domain has recently experienced prominent growth; according to industry estimates, 500 million smartphone users worldwide will be using a healthcare application by 2015, and by 2018, 50 percent of more than 3.4 billion smartphone and tablet users will have downloaded mobile health applications [7]. This is a massive opportunity for a next generation of better and more sustainable healthcare, which was recognized also by the European Commission in a green paper published in 2014 [8], but raises considerable concerns and challenges with respect to data protection and safeguarding of patient safety, privacy, and transparency of information.

Table 1: An overview of relevant documents concerning safety and privacy of digital health apps: international documents and an example of additional national provisions for the Republic of Slovenia.

International provisions	
On safety and privacy of digital health apps in general	
Legal acts passed by the United Nations	Universal Declaration of Human Rights International Covenant on Economic, Social, and Cultural Rights International Covenant on Civil and Political Rights UN guidelines concerning computerized personal data files (UN Guidelines on Computerized Personal Data Files, adopted by the General Assembly on 14 December 1990 [24]) (*specifically on the topic of the right to privacy and data protection*)
Legal acts of the Council of Europe	European Convention on Human Rights Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data [25]
Legal acts of the EU on data protection instruments	Charter of Fundamental Rights of the European Union Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data [26] Directive 2002/58/EC of 12 July 2002 on the processing of personal data and the protection of privacy in the electronic communications sector
On safety and performance for digital health apps categorised as medical devices in particular	
Legal acts of the EU	Directive 93/42/EEC concerning medical devices [23] Directive 98/79/EC on in vitro diagnostic medical devices [27]
National provisions for the Republic of Slovenia	
Constitution of the Republic of Slovenia, Article 38 on safety of personal data	Law on electronic commerce and electronic signature (ZEPEP-UPB1)
Law on safety of personal data (ZVOP-1)	Law on healthcare services and insurance (ZZVZZ)
Law on patients' rights (ZPacP)	Law on electronic commerce on the market (ZEPT)
Law on healthcare (ZZDej)	Law on data sets in the field of healthcare (ZZPPZ)
Law on health services (ZZdrS)	Law on Information Commissioner (ZInfP)

1.1. EU and National Legal Framework for Safety and Privacy of Digital Health Apps. Safety of personal data and other sensitive information represents one of the most pressing challenges in design practice of digital health solutions and has implications on aspects relevant to both developers and medical experts alike. Protection of sensitive personal data and safeguarding of privacy in EU Member States are regulated by both international legal acts and national legislations. When it comes to designing and implementing digital healthcare solutions, the aspects concerned are foremost a combination of collecting, transmission, storing, processing, and forwarding of sensitive personal information. In EU safeguarding of privacy is considered a fundamental human right, as defined in the European Convention of Human Rights as well as national constitutions of the Member States. Relevant international documents on privacy of personal data are summarized in Table 1 (international documents section). As shown, in addition to general laws and provisions, some digital health applications may fall under the category of a medical device, in which case further legislation on safety and performance applies, respectively.

Furthermore, in 2014 the European Commission issued a Commission Staff Working Document on the existing EU legal framework relating to lifestyle and wellbeing apps, providing an overview of applicable rules of the state-of-the-art legislation in EU that applies to mobile applications for wellbeing and digital health [9]. It distinguishes two broad areas, EU safety and performance requirements and users' rights to privacy and data protection. However, operationalization of the rules is in several aspects not straightforward and the document itself notes the fact that the Union legislation does not yet address latest developments in the field, hence leaving further room for its interpretation. In practice, the developers of the mobile apps as well as medical professionals are oftentimes not fully aware of the data protection requirements, which may lead to an app design with unintentional and unwanted safety and privacy risks.

In addition to the EU legislation and guidelines, individual national specifics enforced by the Member States must be taken into consideration and carefully analysed as they can in some cases complicate cross-border communications and exchange of data in digital health solutions. As the interpretation of the EU legal framework on the national level differs from one member to the other, in-depth knowledge of the national specifics on a case-by-case basis is needed. For example, in Slovenia further laws and provisions apply [10] as specified in Table 1 (national documents section). Additionally, health workers are bound by the provisions of the medical field, including the Hippocratic Oath, the Declaration of Geneva, the European Standards on Confidentiality and Privacy in Healthcare, and in Slovenia additionally also the Codex of the medical deontology of Slovenia and the Ethical Codex of the medical nurses and health technicians of Slovenia.

The presented overview is nonexhaustive; the prospective developers of the digital health apps should further consult expert guidelines on legal framework for digital health, legislation, and regulation concerning ePrivacy Directive on storing and accessing information stored in the devices of users, eCommerce Directive on requirements to be provided by providers of information society services, Consumers' Rights Directive on requirements for trading with the apps, including those categorised as wellbeing or lifestyle, and so forth.

The presented EU and national legal framework for safety and privacy of digital health apps lay down guidelines and requirements that must be considered at the time of design of a digital health app. However, interpretation and implementation of the provisions are not always straightforward and must therefore be carefully considered, planned, and executed in practice, as further illustrated in a case study in the following.

1.2. Privacy by Design. Another aspect that must be taken into consideration when planning a digital healthcare app is privacy by design. Privacy by design is a concept of engineering privacy directly into the design of new technologies, business practices, and network infrastructures, which has received significant acceptance in any number of sectors [11], including digital health. The concept originates from a joint report on privacy-enhancing technologies, prepared by the Information and Privacy Commissioner of Ontario, Canada, the Dutch Data Protection Authority, and the Netherlands Organisation for Applied Scientific Research in 1995 [12], and was recently integrated into European Commission's plans for the General Data Protection Regulation [13]. The concept first gained momentum with the widespread adoption of mobile communications technology and has since become one of the core topics with the proliferation of wireless sensor networks (WSN) and Internet of Things (IoT) where privacy and safety concerns are further exacerbated. A considerable body of research work exists on the topic; the guidelines generally recognized in practice for mobile application developers are to integrate privacy into the development cycle, practice data minimization techniques (without sacrificing applications' functionality and user experience), use privacy-protective default settings, employ state-of-the-art security practices, and maintain user awareness and control over data collection and use [12].

However, many of the stated guidelines are for digital health design not always easily and transparently achievable in practice, as demonstrated, for example, in [14–17]. Strict legislation on one hand and the fast pace of advancements in ICT on the other require thoughtful and balanced planning of safety and privacy strategies from the very start and customized implementation of the privacy by design principles on a case-by-case basis, as is demonstrated with a case study in the following.

2. DeStress Assistant: A Case Study

This section presents DeStress Assistant (DeSA), an example of an iOS mobile application designed for biosensing and healthy lifestyle management for diabetes patients and for other users who want to monitor their general wellbeing. The app provides self-help services for diabetes patients in order to ease monitoring and management of their lifestyle in the context of their general wellbeing, stress exposure, and diabetes condition and can be used for private needs by the patient or in more advanced scenarios, in which the app is integrated into a digital healthcare information system (HIS). The design of the app was initially prepared within an EU project FI-STAR [18] and later extended within an EU project UNCAP [19].

The app allows the users to track multiple health and fitness observations, including (Figure 1) the following:

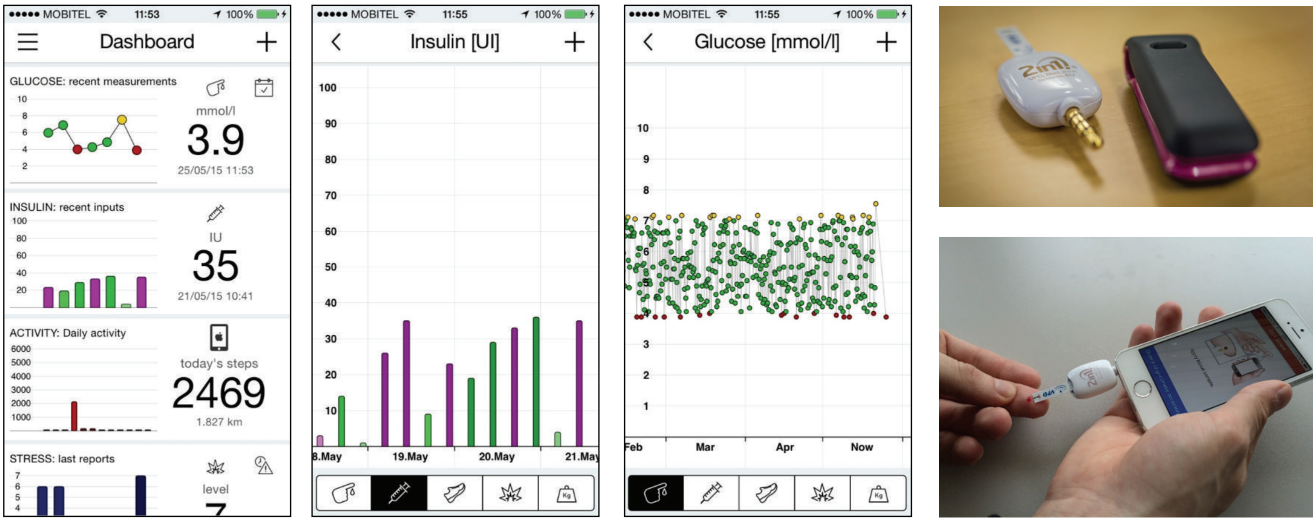
(i) manual recording of blood glucose levels, applications of short-acting and long-acting insulin, perceived stress level on a Likert scale 1 to 7, body weight, and nutritional facts;

(ii) recording of blood glucose levels with 2in1.SMART blood glucose meter (BGM), a medical device commercially available from VPD Ltd., which is connected to DeSA through the headphone (audio jack) connector; to support the use of the BGM, a proprietary library provided by VPD is integrated in the DeSA app, which establishes and monitors the connection between the smartphone app, guides the user through the process of blood glucose measurement, and retrieves the measured values from the BGM;

(iii) physical activity (step counts), either by retrieving the observations from the M7 coprocessor in the iPhone or by retrieving the observations from a Fitbit cloud (using the Fitbit APIs) [20].

The observations are represented to the user in the form of a summary of his or her health-related observations on a dashboard, on a set of simple predefined graphs, and in the form of a diabetes diary (a list of all recorded observations).

At the time of the design of the app and its later exploitation, a secure and user-controlled sharing of selected observations was needed, which would provide medical professionals access to the patient's observations, either through an existing EHR or through other data viewing means. To support sharing of sensitive data and comply with safety and privacy guidelines applicable, the app was designed following a concept of bringing software to data rather than data to software. This is a recently proposed hybrid cloud principle in IoT environments where privacy and data handling requirements are particularly demanding, such as in



(a)

(b)

Figure 1: DeSA app (a) and additional sensing devices 2in1.SMART BGM and Fitbit activity tracker (b).

the case of digital healthcare [21]. The approach brings about two crucial advantages:

(1) Sensitive data is stored locally in the environment where reliability, security, and privacy risks can be well controlled, that is, on the user's personal device, and, if the app is integrated into a digital healthcare system, in a locally provided private cloud (e.g., a secure hospital private cloud infrastructure); the sensitive data is in this case never sent to a public cloud, which considerably lowers risks associated with third-party security attacks, integrity violations, and so forth.

(2) Large volumes of sensed data are stored and processed locally, without the need for them to be (in their entirety) transmitted from the edge of the network, which sits well with the fact that massive amounts of data produced in IoT continue to grow much faster than the available bandwidth; these concepts have recently been adopted in the 5G fog computing, which is looking into the future of IoT and specifically focuses on edge computing and improved elasticity and mobility, as well as improved user experience as the core dimensions of the future of sensing and IoT [22].

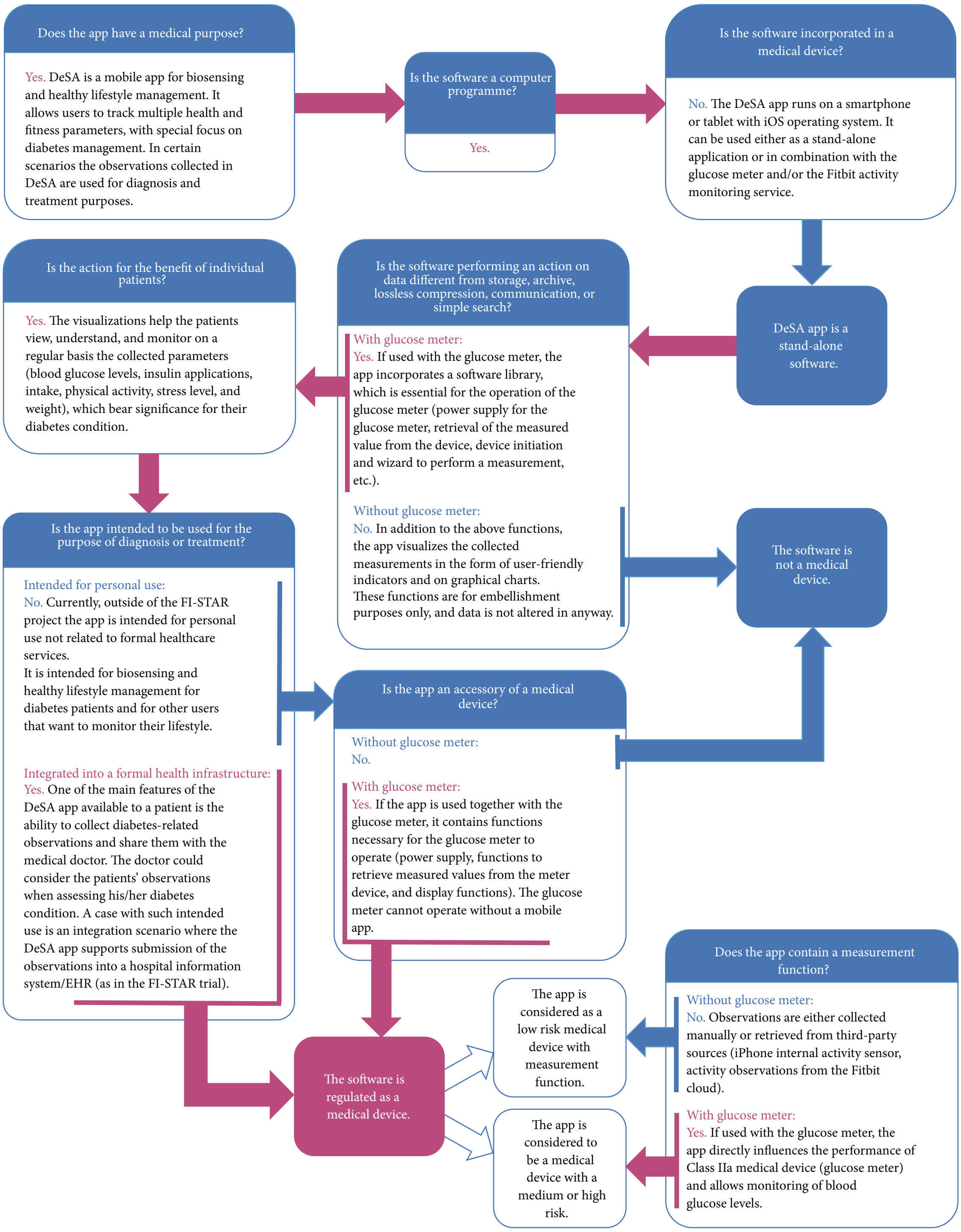
However, during the design of the app, several challenges aroused with respect to ensuring safety and privacy compliance, which bore direct implications on how the intended use of the app can be formulated, how the app is classified in the context of medical device regulations, which sensing devices can be supported and for what purposes, and how secure sharing mechanisms can be designed to remain within boundaries of the legal framework and practical feasibility of implementation. These aspects are further illustrated and discussed in the following.

3. Safety and Privacy Implications on DeSA App Design

3.1. Classification of the App as a Medical Device. When considering safety and privacy of a digital health app, the question of whether the app is classified as a medical device or not bears vital implications. According to the Council Directive 93/42/EEC concerning medical devices (MDD) [23], certain digital health apps are medical devices. When placed on the market, such apps must bear CE marking; if the app is in a development stage (e.g., built as a prototype or intended for use in a clinical trial or in a demonstrator), CE mark is not needed but the app must still pass all relevant conformity assessment procedures.

To determine which class of medical device the app belongs to, the European Commission has issued a set of guidance documents relating to the application of the MDD directive [28, 29]. However, as demonstrated hereafter, the determination of the applicable class is not always a simple and straightforward task and is heavily dependent on the concrete context of its intended use, even in the case of a relatively simple digital health app, such as DeSA. The decision process for DeSA classification is represented in Figure 2.

As demonstrated with the above example, the assigned class is directly dependent on the intended use of the app as well as the intended use of other (third-party) medical devices together with the app. For DeSA, the resulting classes range from "not a medical device" in case the app is intended for personal use unrelated to formal healthcare (not supporting diagnosis and treatment of patients) and without the BGM to "Class I low risk medical device" if considered for primarily medical use but without the use of a BGM, which is a medical device. A further and even greater challenge is the case when the app is positioned as an accessory to a medical device; according to legal directives, in such case the app is not



Does the app have a medical purpose?

Yes. DeSA is a mobile app for biosensing and healthy lifestyle management. It allows users to track multiple health and fitness parameters, with special focus on diabetes management. In certain scenarios the observations collected in DeSA are used for diagnosis and treatment purposes.

Is the software a computer programme?

Yes.

Is the software incorporated in a medical device?

No. The DeSA app runs on a smartphone or tablet with iOS operating system. It can be used either as a stand-alone application or in combination with the glucose meter and/or the Fitbit activity monitoring service.

DeSA app is a stand-alone software.

Is the software performing an action on data different from storage, archive, lossless compression, communication, or simple search?

With glucose meter:
Yes. If used with the glucose meter, the app incorporates a software library, which is essential for the operation of the glucose meter (power supply for the glucose meter, retrieval of the measured value from the device, device initiation and wizard to perform a measurement, etc.).

Without glucose meter:
No. In addition to the above functions, the app visualizes the collected measurements in the form of user-friendly indicators and on graphical charts. These functions are for embellishment purposes only, and data is not altered in anyway.

The software is not a medical device.

Is the action for the benefit of individual patients?

Yes. The visualizations help the patients view, understand, and monitor on a regular basis the collected parameters (blood glucose levels, insulin applications, intake, physical activity, stress level, and weight), which bear significance for their diabetes condition.

Is the app intended to be used for the purpose of diagnosis or treatment?

Intended for personal use:
No. Currently, outside of the FI-STAR project the app is intended for personal use not related to formal healthcare services.
It is intended for biosensing and healthy lifestyle management for diabetes patients and for other users that want to monitor their lifestyle.

Integrated into a formal health infrastructure:
Yes. One of the main features of the DeSA app available to a patient is the ability to collect diabetes-related observations and share them with the medical doctor. The doctor could consider the patients' observations when assessing his/her diabetes condition. A case with such intended use is an integration scenario where the DeSA app supports submission of the observations into a hospital information system/EHR (as in the FI-STAR trial).

Is the app an accessory of a medical device?

Without glucose meter:
No.

With glucose meter:
Yes. If the app is used together with the glucose meter, it contains functions necessary for the glucose meter to operate (power supply, functions to retrieve measured values from the meter device, and display functions). The glucose meter cannot operate without a mobile app.

The software is regulated as a medical device.

The app is considered as a low risk medical device with measurement function.

The app is considered to be a medical device with a medium or high risk.

Does the app contain a measurement function?

Without glucose meter:
No. Observations are either collected manually or retrieved from third-party sources (iPhone internal activity sensor, activity observations from the Fitbit cloud).

With glucose meter:
Yes. If used with the glucose meter, the app directly influences the performance of Class IIa medical device (glucose meter) and allows monitoring of blood glucose levels.

Figure 2: DeSA app classification as a medical device.

a medical device but falls under the MDD Directive 93/42/EEC and is in practice required to pass CE certification with a notified body as part of the certification of the medical device. For DeSA, in this case the assigned class becomes "Class IIa medical device" and the app itself cannot be considered as a stand-alone device that supports optional use of other third-party accessories (including those intended for health-related use); instead, the app becomes "an accessory to a Class IIa medical device" and should be included in the CE certification of the BGM. It is not unambiguously clear how such situation should be tackled in case the provider of the app and provider of the medical device are not one and the same entity and which intended uses can be considered if the app is provided by the app developer via an online store free of charge and for personal use, whereas it is entirely up to the user to decide if he or she wishes to purchase and use the supported BGM as an add-on. At the time of writing, this grey area is still under discussion and the DeSA app is in a development stage and does not yet bear the CE marking. However, it has already become clear that if the DeSA app is to be used to collect diabetes-related observations that are shared with formal healthcare practitioners for diagnostic and treatment purposes, CE certification for a medical device class is a requirement, which bears further implications on its safety and privacy design, as discussed in the following.

3.2. Compliance with Essential Requirements for a Medical Device.

If a mobile digital healthcare app is categorized as a medical device, Annex I of Council Directive 93/42/EEC concerning medical devices [23] specifies *the essential requirements* that must be respected in the design and applied to any application that is either in a development stage (e.g., intended for a clinical trial) or ready for use (i.e., put on the European market). The conformity assessment procedures depend on the class assigned to the application, which denotes the extent of risks the user is exposed to during its use. Hereafter, some selected requirements are discussed in the context of DeSA application design, which have spurred discussions about how the safety and privacy should and can be tackled.

The design of the app that is a medical device must be safe when used under the conditions and for the purposes intended [23]. The DeSA app is intended for use on iOS smartphones and tablets, in combination with a third-party device, a BGM (2in1.SMART), which is a registered medical device, and a third-party public cloud-based service, the Fitbit activity monitoring. However, the notion of ensuring safe use of the app with such third-party components is not straightforward. According to Annex I of MDD *the entire combination must be safe and specific performance of the devices must not be impaired*. However, the developing team does not have control over the entire combination beyond their own source code, rendering three particular safety issues.

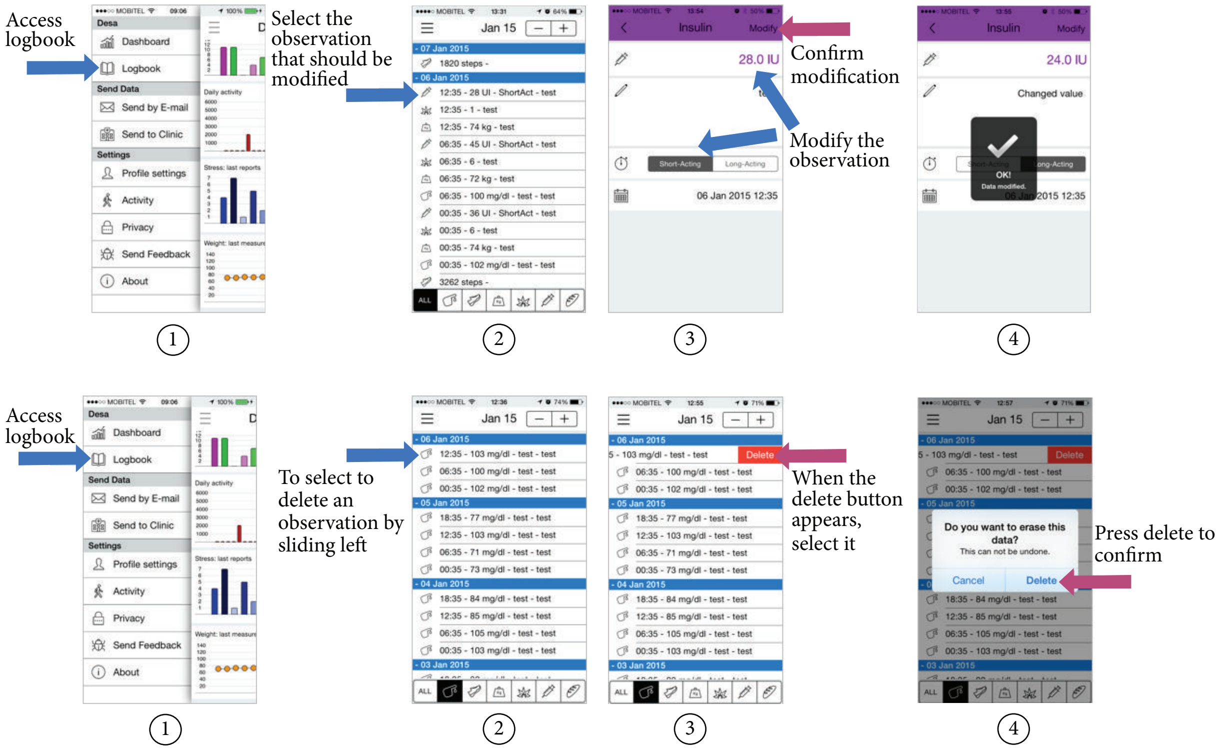
Use of Generic Devices. The functioning of the app depends on the capabilities of the iOS device and the iOS operating system, which are commercial components purchased by the user of the app. If functionalities of these components should change in the future (e.g., in a new version of the iOS operating system), the changes could possibly impair functioning of the application that the development team can neither foresee nor prevent.

Use of Third-Party Devices. To support the use of the BGM directly from the DeSA app, the development team entered a cooperating project with the provider of the device and was provided with a specific proprietary library accompanying the device, which had to be integrated into the app. Since both the device and the accompanying software library are under strict IPR protection, the development team does not have access to the source code of the library and no power of control over the BGM. This opens a series of security issues, including underperformance or even failure of app operation due to bugs in the library source code or impaired functioning of the app as a consequence of device malfunctioning or inadequate device or software support (e.g., a delay in vital upgrades to library source code required as a result of iOS operating system changes).

Use of Public Cloud Services. To collect observations related to physical activity of the user, the app utilizes the built-in M7 coprocessor in the iPhone or (optionally) retrieves activity data from the Fitbit cloud using the Fitbit resource access API [30], in which case the activity is independently collected by the user with a Fitbit activity tracker and uploaded to the Fitbit cloud. In the former case the safety assurance issue is the same as in the first point. In the latter case, however, the entire combination encompasses also a third-party public cloud resource, which is used by the app on the basis of a nonexclusive, revocable, nonsublicensable, nontransferable royalty-free license granted to the development team by the Fitbit [20], for the use of which the provider of the API removes all forms of liability and has no obligation to provide any type of support, and with the right to disable or upgrade the resource without notice and without obligation to ensure that the upgrade will continue to be compatible with the existing apps. In practice the developer of the app has no control whatsoever over the safety and performance of the used API resource, the Fitbit activity tracker, as well as the eventual processing of data collected in the Fitbit cloud and therewith cannot comply with the requirements for ensuring safety of the entire combination. This leads to a conclusion that in scenarios where intended use of the app indicates its class as a medical device the cloud-based components can only be integrated if the cloud provider is a trusted party with clear policies and mindful (and possibly certified) practices regarding access to and processing of data and use of technical and organizational security measures, which effects minimized risks of information security breaches, reduced power of access control, reduced transparency of data processing, and reduced power of safeguarding transferability of data on the side of the app provider. One additional requirement at this point is also mutual compliance of the applicable legal frameworks for the app developer and the cloud provider, in our case between the US and the EU/national legislation, which requires further investigation.

3.3. Privacy-Aware Data Processing and Secure Sharing Mechanisms.

The Directive 95/46/EC [26] imposes the obligation to take technical measures in order to ensure the adequate protection of personal data from any kind of unauthorized processing (meaning collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure, or destruction), which must be taken into account as early as in the stage of the app design. According to Article 29 Working Party [31], raw sensor data that combined with other personal data can draw conclusions about the health status of the user which is considered health data. The same is true for any medical data generated in a professional medical



Access logbook

Select the observation that should be modified

Confirm modification

Modify the observation

Access logbook

To select to delete an observation by sliding left

When the delete button appears, select it

Do you want to erase this data?
This can not be undone.

Press delete to confirm

Figure 3: Functions to modify, correct, or delete observations in the DeSA app.

context, even by the use of devices or apps (irrespective of whether they are marketed as medical devices). Such data is considered sensitive, and its processing is in principle forbidden and only allowed in exceptions, which for the case of DeSA are explicit consent of the user and processing of the data in a treatment relationship. This means that the data declared as health data cannot be passed on to any third parties, which includes also the app provider (unless the app provider is owned and managed by the healthcare institution providing treatment, which was not the case with DeSA). Unless otherwise provided in national laws, encryption and pseudoanonymization are not considered appropriate mitigation strategies. These provisions represented one of the baseline guidelines for DeSA app design and mean that diabetes-related observations collected in DeSA, namely, blood glucose measurements, records of insulin applications, physical activity (step count), food intake records, weight, and recorded stress levels, if combined and interpreted in terms of patient's health condition (in this case related to diabetes disease), constitute sensitive health data, which can only be accessible to

(i) the user,

(ii) medical professionals involved in formal treatment relationships with the user, provided the app is integrated with the HIS.

This leads to the following design choices. On the user's side, the observations collected with the DeSA app are stored only in the app and never leave the device unless the user chooses to share them with their physician or other treating medical professionals. The app itself is not cloud-based and does not support syncing of observations into a consumer cloud facility. To comply with the requirement for the *maintaining of quality health data and the requirement for users to have control over data*, functions were designed that enable the observations to be corrected or deleted inside the app, as shown in Figure 3.

Next, two sharing mechanisms were designed for user-controlled and secure sharing of observations for scenarios where the app is integrated with a HIS.

Secure Sharing Mechanism for Storing of the Observation in a HIS. The first mechanism (Figure 4) was a client-server based secure sharing of observations from the DeSA app into a HIS, which is intended for scenarios where the observations are to be stored in an Electronic Health Record (EHR). In light of the above data safety requirements, in this case appropriate level of security had to be ensured throughout the entire sharing infrastructure. This eliminated the choice of commercial cloud (hosting/colocation/Infrastructure-as-a-Service) for the fact that it was not acceptable to be legally responsible for data processing and at the same time not being able to fully guarantee that all appropriate security measures are taken (to ensure availability, integrity, confidentiality, transparency, isolation, and portability of data). Only infrastructure located in a secure private information environment of a healthcare establishment, a health information system backbone, or a certified provider was considered acceptable.

The second implication was that parts of the system where health data is stored should not be directly accessible

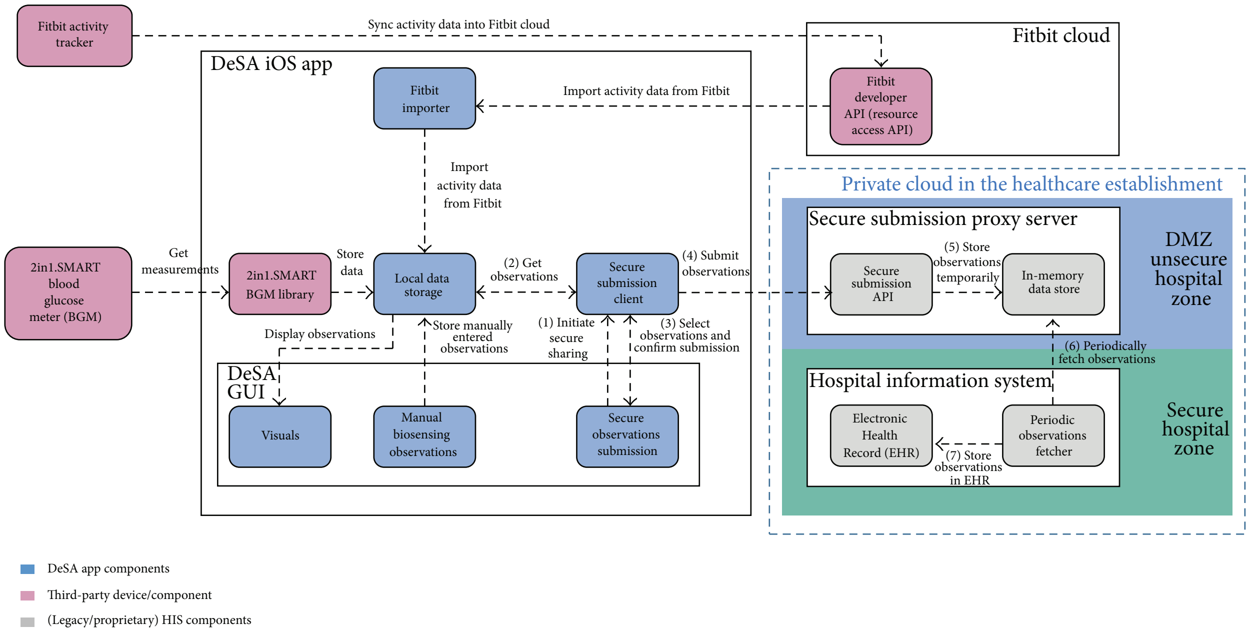

Fitbit activity tracker
Sync activity data into Fitbit cloud
Fitbit cloud
DeSA iOS app
Fitbit importer
Import activity data from Fitbit
Fitbit developer API (resource access API)
Import activity data from Fitbit
Private cloud in the healthcare establishment
Secure submission proxy server
DMZ unsecure hospital zone
2in1.SMART blood glucose meter (BGM)
Get measurements
2in1.SMART BGM library
Store data
Local data storage
(2) Get observations
Secure submission client
(4) Submit observations
Secure submission API
(5) Store observations temporarily
In-memory data store
Display observations
Store manually entered observations
(1) Initiate secure sharing
(3) Select observations and confirm submission
(6) Periodically fetch observations
DeSA GUI
Visuals
Manual biosensing observations
Secure observations submission
Hospital information system
Electronic Health Record (EHR)
Periodic observations fetcher
(7) Store observations in EHR
Secure hospital zone
DeSA app components
Third-party device/component
(Legacy/proprietary) HIS components

Figure 4: Secure sharing mechanism for storing of the observation in a HIS.

from the Internet, which includes also the final EHR. This considerably limits the choice of appropriate access types a user (a patient or a medical professional) can make use of to reach the system; users typically rely on connectivity provided by a home network, a leased line from an Internet service provider, or a mobile data connectivity service (e.g., Edge, 3G, or LTE), which are all part of a public Internet infrastructure and use IP connectivity that is relatively easily compromised by an attacker.

To overcome these considerations, we chose the architecture with an intermediate (proxy) server, located in a demilitarized zone (DMZ) of the hospital, while the EHR was hosted in a private and secure HIS zone. DMZ represents a perimeter segment of the HIS, the role of which is to serve as an access point for the HIS from the unsecure outside Internet domain; this adds an additional layer of security. The proxy server in the DMZ is accessible from the Internet and therefore capable of receiving the shared observations from the DeSA app (Figure 4, steps (1)–(4)). However, it does not store the collected observations on the hard disk but instead temporarily stores the data in the in-memory (ephemeral) data store (Figure 4, step (5)). The secure zone comprises in addition to the EHR a data fetcher, which periodically retrieves data from the proxy server in the DMZ zone (Figure 4, step (6)); once the observations are retrieved and stored in the EHR (Figure 4, step (6)), the data is deleted from the DMZ proxy server memory. This approach considerably reduces the risk of hacking the secure zone since neither the users nor the proxy server from the DMZ can connect to the secure zone infrastructure and at the same time minimizes the volume of data exposed to intrusion risks during the time window when the data temporarily resides in the DMZ.

For countries where national legislation allows forwarding of data outside of the secure zone of the healthcare establishment responsible for the sensitive data, the use of a virtual private network (VPN) to grant medical professionals access to the data stored in the secure zone is an option, but only for trustworthy and safety/privacy-aware users, in which case an encrypted connectivity is established directly into the private network of the healthcare establishment. In case the legislation only limits the storing of the sensitive data outside of the healthcare establishment (but, e.g., allows its viewing), the use of web technologies with disabled caching of data is an option. However, in many countries, including Slovenia, the legislation is restrictive and the use of such mechanisms allowing for access to data outside of the secure zone does not apply.

Secure Sharing Mechanism with One-Time Session without Storing. Furthermore, we have designed another alternative sharing mechanism (Figure 5) based on one-time secure session establishment and sharing of observations without storing, which is intended for scenarios that do not involve storing of the observations in a HIS but instead enable sharing of observations for a limited period of time (for the duration of the session) directly between DeSA and another trusted data viewer for medical professionals (e.g., web browser), without storing the data on any remote site (anywhere outside of DeSA app). The principal rationale for such design choice is limited possibilities for integration of an app into an existing healthcare system (and an EHR in particular), which is in practice often the case due to established contractual obligations and internal policies in the healthcare establishment and/or due to technological compatibility of the existing infrastructure. This mechanism was designed for sharing of observations between the patient (user of the DeSA app) and a medical professional during a consultation or as an event that the patient and the carer prearrange between themselves

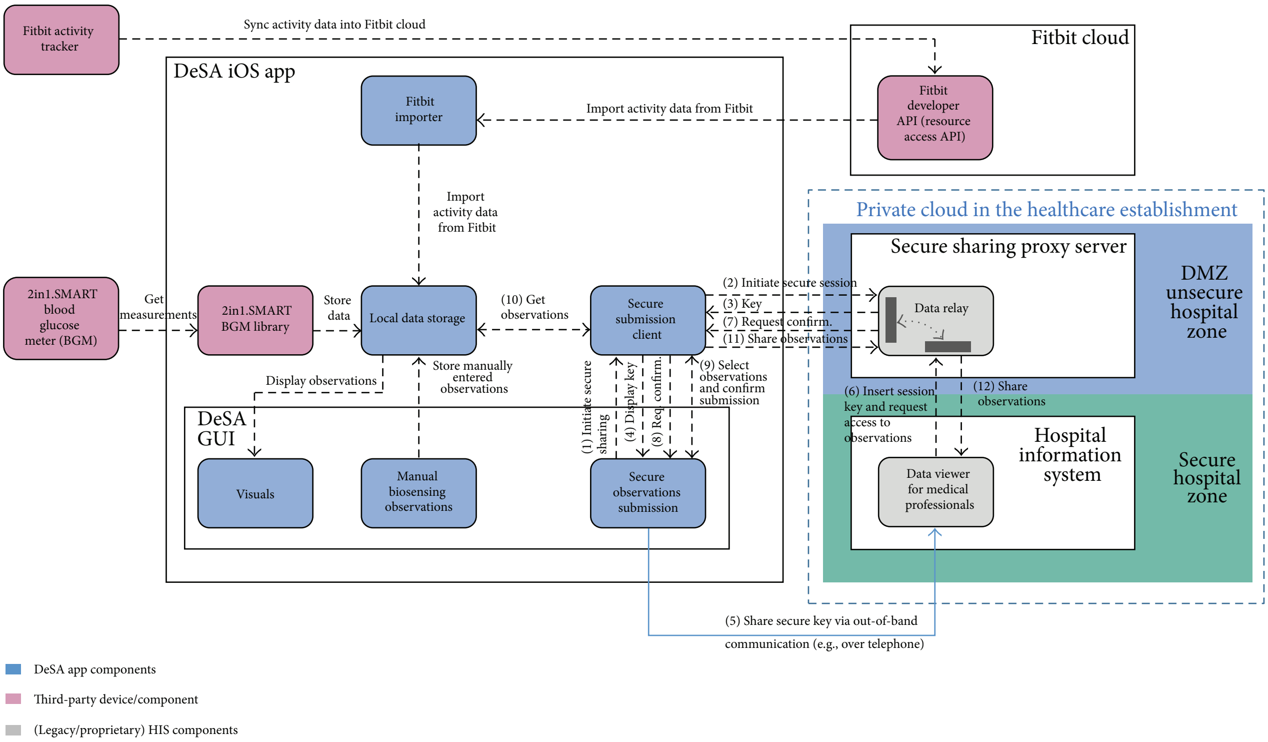

Fitbit activity tracker
Sync activity data into Fitbit cloud
Fitbit cloud
Fitbit developer API (resource access API)
DeSA iOS app
Fitbit importer
Import activity data from Fitbit
Import activity data from Fitbit
2in1.SMART blood glucose meter (BGM)
Get measurements
2in1.SMART BGM library
Store data
Local data storage
(10) Get observations
Secure submission client
Display observations
Store manually entered observations
DeSA GUI
Visuals
Manual biosensing observations
Secure observations submission
(1) Initiate secure sharing
(4) Display key
(8) Req. confirm.
(9) Select observations and confirm submission
(2) Initiate secure session
(3) Key
(7) Request confirm.
(11) Share observations
Private cloud in the healthcare establishment
Secure sharing proxy server
Data relay
DMZ unsecure hospital zone
(6) Insert session key and request access to observations
(12) Share observations
Hospital information system
Data viewer for medical professionals
Secure hospital zone
(5) Share secure key via out-of-band communication (e.g., over telephone)
DeSA app components
Third-party device/component
(Legacy/proprietary) HIS components

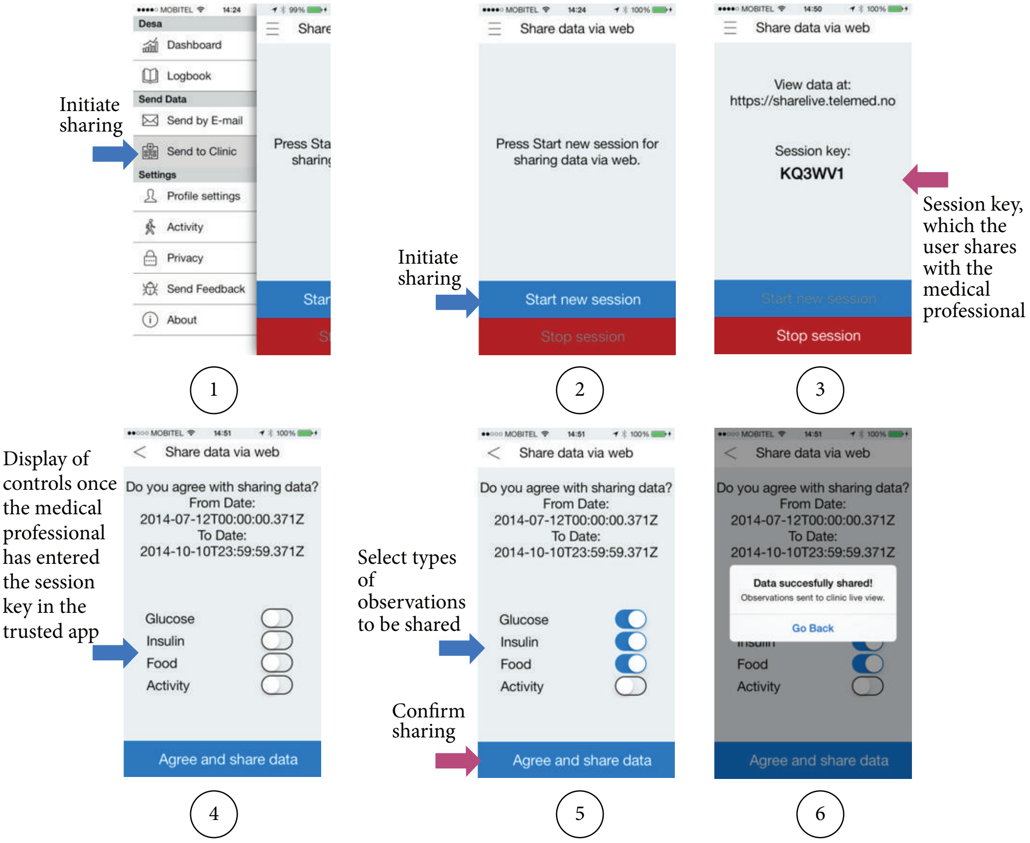
Figure 5: Secure sharing mechanism with one-time session without storing.

(e.g., before or during patient's examination, the patient and the doctor agree on sharing blood glucose and activity data for the past three weeks).

In this case, a secure sharing proxy server (data relay) is located in a DMZ unsecure zone, the role of which is to bind secure one-time sessions from DeSA and from the data viewer and to forward the observations without storing them anywhere in the DMZ zone. The trusted data viewer is located in the secure zone of the hospital information infrastructure (private cloud), again to comply with the requirements for the health data not leaving the secure zone similarly to the first mechanism.

The user triggers establishment of a one-time secure session with transport layer security mechanisms (TLS; e.g., https) from the DeSA app (Figure 6, Figure 5, steps (1)-(2)), which triggers a request to the data relay. A session key is generated (a one-time, random access code, 6 characters: numbers and letters) and sent back to the DeSA app, which the user shares with the medical professional using out-of-band communication (e.g., in a telephone conversation or face to face at an appointment) (Figure 5, steps (3)–(5)). The data relay waits to receive a session request with the correct session key from the data viewer (after the medical professional has inserted the session key into the data viewer and then selected to request observations from the patient's DeSA app) (Figure 5, steps (6)-(7)). When received, the data relay binds both sessions and sends a prompt into the DeSA app for the user to confirm and initiate sharing of observations (Figure 5, steps (8)–(12)).

All data that passes from the DeSA and through the private cloud (data in transit) is completely anonymous, that is, completely stripped of all identifying information. No personally identifying information is added to the observations selected by the user for submission (e.g., no name or birth date is transferred together with the data). The identity of the patient is exchanged only using out-of-band communication (Figure 5, step (5)). In this way, there is no identifying data in transit, which would be exposed to interception or other forms of compromising (e.g., by taking advantage of application vulnerabilities or attacking physical infrastructure). Also, the data relay for the private cloud can be attached to the public Internet, and access can happen over any means of connecting to Internet, most commonly through WiFi or mobile networks (e.g., Edge, 3G, and LTE). For the duration of the session, data is temporarily stored in the data viewer located in the secure zone (e.g., in memory of the web browser); data is never stored in the DMZ and there is no data at rest outside of the DeSA app. The session can be broken on either side (DeSA or data viewer) at any time, which effects deleting the data everywhere in the system except in the DeSA app. Hence, the mechanism ensures also that data is retained for a minimum required period (one session only), which is according to the data minimization practice as specified in [11]. The implementation of this mechanism was demonstrated in the FI-STAR Diabetes Share System trial [18] together with a back-end infrastructure and a Diabetes Share Live application (acting as a data viewer) implemented in a private cloud environment at the University Hospital of North Norway.



Press Start new session for sharing data via web.

View data at: https://sharelive.telemed.no

Session key: KQ3WV1

Do you agree with sharing data?
From Date:
2014-07-12T00:00:00.371Z
To Date:
2014-10-10T23:59:59.371Z

Data succesfully shared!
Observations sent to clinic live view.

Figure 6: Establishment of the one-time session from the DeSA app.

With both mechanisms, before confirming sharing of the observations, the user has power to control which data and/or for what period of time he or she wishes to share with the medical professional, which meets the requirement for users to have control over data. According to the *least privilege by default* principle [11] the default state is that none of the types of observations are selected and the user has to select (change button to “on”) the data types he or she wants to send.

4. Conclusion

This paper presented a case study on security and privacy implications on the design of a mobile application in digital health, which utilizes sensing technologies and IoT capabilities. Selected challenges encountered during the app design were discussed, illustrating that practical application of legislative provisions is not always straightforward and must therefore be thoroughly addressed on a case-by-case basis. We presented an analysis of the process of mobile app classification as a medical device and demonstrated that the outcome depends on the specified intended use of the app as well as sensing devices and other third-party components (and cloud services in particular) the app is to be used with. It was further demonstrated that the interpretation of the legislative framework in most cases recognized the discussed app as a medical device for the fact that the collected observations if interpreted in a treatment context could indicate the health status of the patient, leading to two particular challenges. Firstly, the app developer is faced with a legal obligation to ensure safety of the entire combination, which he or she cannot always guarantee; this particular issue needs further research and regulatory attention as it is highly probable that most digital health solutions relying on third-party components such as sensor devices, cloud services, and IoT middleware platforms will be faced with it. Secondly, the classification of the app as a medical device has concrete implications on the design of data sharing mechanism. In addition to the mechanism for secure transmission of health-related observations into a health information system, which is today typically used in connection with EHRs, we proposed a design of a secure sharing mechanism within a one-time session without storing of sensitive data outside of the app. As demonstrated, the design is in compliance with legislative provisions for handling health-related data; the facts that the only transaction of sensitive data (i.e., the session key) is carried out using already established practice (i.e., by the patient in person or over the telephone) and that the observations from the app are completely anonymized prior to sharing and then not stored anywhere outside of the app eliminate several legislative obligations and constraints regarding protection of sensitive data in transit and at rest. At the same time, the proposed approach is not burdened by the often encountered obstacles associated with technological incompatibility or restrictive policies for implementation of such solutions into existing health information systems.

Conflict of Interests

The authors declare that there is no conflict of interests regarding the publication of this paper.

Acknowledgments

The research and development work has received funding from the European Union's Seventh Programme for research, technological development, and demonstration under Grant Agreement no. 604691 (FI-STAR), from the European Union's Horizon 2020 research and innovation programme under Grant Agreement no. 643555 (UNCAP), and from the Slovenian Research Agency under Grant Agreement P2-0246.

References

[1] S. M. Riazul Islam, D. Kwak, M. Humaun Kabir, M. Hossain, and K.-S. Kwak, "The internet of things for health care: a comprehensive survey," *IEEE Access*, vol. 3, pp. 678–708, 2015.

[2] M. Abomhara and G. M. Koien, "Security and privacy in the Internet of Things: current status and open issues," in *Proceedings of the International Conference on Privacy and Security in Mobile Systems (PRISMS '14)*, pp. 1–8, Aalborg, Denmark, May 2014.

[3] A. Štern and A. Kos, "Mobile phone as a tool in the areas of health protection," *Zdravniski Vestnik*, vol. 78, no. 11, pp. 673–684, 2009.

[4] K. Peternel, Poga, R. Tavčar, and A. Kos, "A presence-based context-aware chronic stress recognition system," *Sensors*, vol. 12, no. 11, pp. 15888–15906, 2012.

[5] C. Thuemmler, L. Fan, W. Buchanan, O. Lo, E. Ekonomou, and A. Khedim, "E-health: chances and challenges of distributed, service oriented architectures," *Journal of Cyber Security and Mobilit*, vol. 37, no. 52, 2012.

[6] N. K. Janjua, M. Hussain, M. Afzal, and H. F. Ahmad, "Digital health care ecosystem: SOA compliant HL7 based health care information interchange," in *Proceedings of the 3rd IEEE International Conference on Digital Ecosystems and Technologies (DEST '09)*, pp. 329–334, Istanbul, Turkey, June 2009.

[7] R.-G. Jahns, *500m People Will Be Using Healthcare Mobile Applications in 2015*, research2guidance, 2010, http://research2guidance.com/500m-people-will-be-using-healthcare-mobile-applications-in-2015/.

[8] European Commission, "Green paper on mobile Heath (mHealth)," 2014, http://ec.europa.eu/digital-agenda/en/news/green-paper-mobile-health-mhealth.

[9] European Commission, "Commission Staff Working Document on the existing EU legal framework applicable to lifestyle and wellbeing apps," 2014, https://ec.europa.eu/digital-agenda/en/news/commission-staff-working-document-existing-eu-legal-framework-applicable-lifestyle-and.

[10] B. Pirkovič, *Normativna ureditev ravnanja z občutljivimi osebnimi podatki v zdravstvu [Magistrsko delo]*, Univerza v Ljubljani, Fakulteta za upravo, 2012.

[11] Privacy by Design Research Lab and Information and Privacy Commissioner, *The Roadmap for Privacy by Design in Mobile Communications: A Practical Tool for Developers, Service Providers, and Users*, Privacy by Design Research Lab, Information and Privacy Commissioner, Ontario, Canada, 2010, https://www.ipc.on.ca/images/Resources/pbd-asu-mobile.pdf.

[12] P. Hustinx, "Privacy by design: delivering the promises," *Identity in the Information Society*, vol. 3, no. 2, pp. 253–255, 2010.

[13] 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)," 2012, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2012:0011:FIN:EN:PDF.

[14] C. George, D. Whitehouse, and P. Duquenoy, "Assessing legal, ethical and governance challenges in eHealth," in *eHealth: Legal, Ethical and Governance Challenges*, pp. 3–22, Springer, Berlin, Germany, 2013.

[15] A. G. Fragopoulos, J. Gialelis, and D. Serpanos, "Imposing holistic privacy and data security on person centric eHealth monitoring infrastructures," in *Proceedings of the 12th IEEE International Conference on e-Health Networking Applications and Services (Healthcom '10)*, pp. 127–134, IEEE, Lyon, France, July 2010.

[16] E. Kindt, "Best practices for privacy and data protection for the processing of biometric data," in *Security and Privacy in Biometrics*, pp. 339–367, Springer, London, UK, 2013.

[17] G. S. Brost and M. Hoffmann, "Identifying security requirements and privacy concerns in digital health applications," in *Requirements Engineering for Digital Health*, pp. 133–154, Springer, 2015.

[18] European Union's Seventh Programme for Research-Technological Development and Demonstration, "Future Internet—Social Technological Alignment Research (FI-STAR)," Grant agreement No 604691.

[19] European Union's Horizon 2020 Research and Innovation Programme, "Ubiquitous iNteroperable Care for Ageing People (UNCAP)," Grant agreement No. 643555.

[20] 2015, https://dev.fitbit.com/terms.

[21] C. Thuemmler, J. Mueller, S. Covaci et al., "Applying the software-to-data paradigm in next generation e-health hybrid clouds," in *Proceedings of the 10th International Conference on Information Technology: New Generations (ITNG '13)*, pp. 459–463, IEEE, Las Vegas, Nev, USA, April 2013.

[22] S. Yi, C. Li, and Q. Li, "A survey of fog computing: concepts, applications and issues," in *Proceedings of the Workshop on Mobile Big Data (Mobidata '15)*, pp. 37–42, ACM, Hangzhou, China, June 2015.

[23] Council Directive 93/42/EEC of 14 June 1993 concerning medical devices, OJL 169, 1993, http://www.emergogroup.com/sites/default/files/file/europe-consolidated-mdd-93-42-eec.pdf.

[24] United Nations General Assembly Resoultion 45/9, "Guidelines for the regulation of computerized personal data files," in *Proceedings of the 68th Plenary Meeting*, A/RES/45/95, December 1990, http://www.un.org/documents/ga/res/45/a45r095.htm.

[25] Council of Europe, "Convention No.108 for the Protection of Individuals with regard to the Automatic Processing of Personal Data," 1981, http://www.coe.int/web/portal/home.

[26] Directive 95/46/Ec Of The European Parliament And Of The Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en.

[27] *Directive 98/79/EC of the European Parliament and of the Council of 27 October 1998 on in Vitro Diagnostic Medical Devices*, OJ L 331, 7.12, 1998, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:31998L0079.

[28] European Commission, DG Health And Consumer, Directorate B, Unit B2, Cosmetics and medical devices, 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, 2010, http://ec.europa.eu/health/medical-devices/files/meddev/2_4_1_rev_9_classification_en.pdf.

[29] European Commission, DG Health And Consumer, Directorate B, Unit B2, Health Technology, and Cosmetics, "MEDICAL DEVICES: guidance document; Qualification and classification of stand alone software (guidelines on the qualification and classification of stand alone software used in healthcare within the regulatory framework of medical devices)," MEDDEV 2.1/6, 2012, http://ec.europa.eu/health/medical-devices/files/meddev/2_1_6_ol_en.pdf.

[30] 2015, https://wiki.fitbit.com/display/API/Fitbit+Resource+Access+API.

[31] Article 29 Data Protection Working Party, "Opinion 02/2013 on apps on smart devices," WP 202, p. 18, February 2013, http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf.

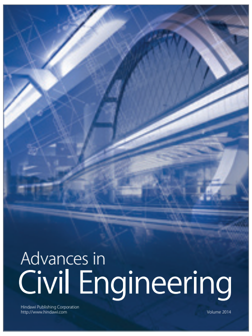
Journal of
Engineering

The Scientific World Journal

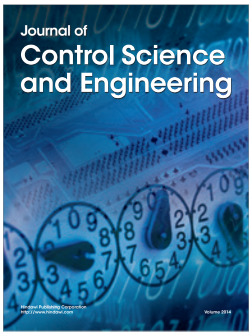
International Journal of
Rotating Machinery

Journal of
Sensors

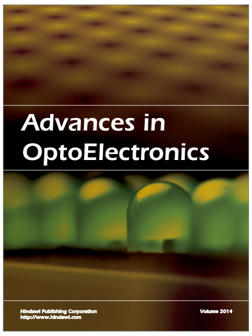
International Journal of
Distributed Sensor Networks


Advances in
Civil Engineering

Journal of
Robotics

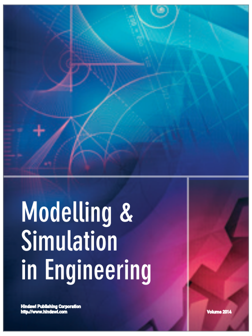

Journal of
Control Science and Engineering

Journal of
Electrical and Computer Engineering

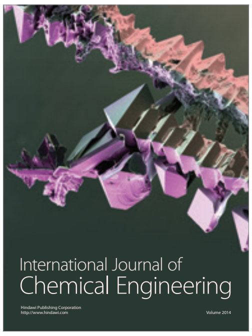

Advances in
OptoElectronics

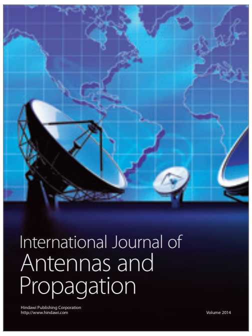
VLSI Design

International Journal of
Navigation and Observation

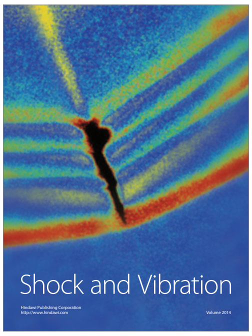

Modelling & Simulation in Engineering

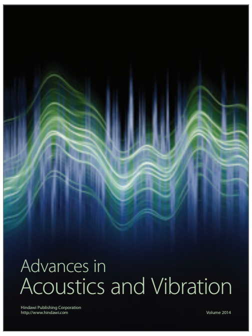
International Journal of
Aerospace Engineering


International Journal of
Chemical Engineering


International Journal of
Antennas and Propagation

Active and Passive Electronic Components


Shock and Vibration


Advances in
Acoustics and Vibration