mHealth Applications for Goal Management Training - Privacy Engineering in Neuropsychological Studies

Alexander Gabel, Ina Schiering, Sandra Verena Müller, Funda Ertas

mHealth Applications for Goal Management Training - Privacy Engineering in Neuropsychological Studies

Alexander Gabel[1], Ina Schiering[2], Sandra Verena Müller[3], and Funda Ertas[4]

[1] Ostfalia University of Applied Sciences
Wolfenbüttel, Germany
ale.gabel@ostfalia.de
[2] i.schiering@ostfalia.de
[3] s-v.mueller@ostfalia.de
[4] f.ertas@ostfalia.de

Abstract. The potential of digitalisation in healthcare based on mobile health, so-called mHealth applications, is considerable. On the other hand these solutions incorporate huge privacy risks. In the context of goal management training, a neuropsychological training used for the cognitive rehabilitation of executive dysfunction after a brain injury, the use of mHealth applications is considered. Privacy requirements of this scenario are modelled based on methodologies as privacy protection goals and privacy design strategies. Measures to realize the requirements are proposed and discussed in the context of a study. The focus in privacy engineering is on pseudonymity of patients, data minimization and transparency for patients.

Keywords: mHealth, privacy, data minimization, pseudonymity, transparency, privacy protection goals, privacy design strategies, goal management training, executive dysfunctions

1 Introduction

Based on recent technological innovations as the Internet of Things (IoT) and smart devices, the potential of digitalization is also utilized in healthcare. Especially the widespread use of smartphones and broadband internet access fosters the trend of mobile applications in healthcare which has the potential to overcome structural barriers, allow for scalability and address the need for interdisciplinary research [4]. These so called mHealth solutions allow "real-time monitoring and detection of changes in health status" [32].

On the other hand 44 percent of data breaches happen in healthcare alone [8,49]. In an evaluation of mHealth solutions and corresponding studies McKay et al. [37] point out the "lack of information in any of these studies about readability, privacy or security". The privacy risks of connected health devices and the importance of approaches as privacy by design are stated by Allaert et al.

[1]. But in the literature about mHealth solutions privacy is often reduced to informed consent in combination with an ethical approval [47]).

Although there exist a broad range of reviews and assessments of mHealth solutions stating deficits especially in the area of privacy and information security, in mHealth solutions which are used in clinical studies, privacy and information security are not in the focus of the consideration. Hence this paper presents a case study about privacy engineering in the context of the mHealth solution presented in Section 2. In this context both privacy and data protection as differentiated by the Charter of Fundamental Rights of the European Union [16] in Article 7 and 8 are considered [31].

The aim of this paper is to realize privacy by design by privacy engineering methodologies in the context of an mHealth project and the accompanying studies. The feasibility of a structured privacy by design approach [23], [25] for an mHealth solution and accompanying study is evaluated.

In this context an mHealth solution to realize the so-called goal management training (GMT) is considered. GMT is a neuropsychological training used for cognitive rehabilitation of executive dysfunction after a brain injury e.g after a stroke or an accident [35]. The realization of GMT as mHealth solution has the potential to integrate rehabilitation measurements in the daily life of the patients instead of using it solely during therapy sessions as in the traditional approach. To cope with the accompanied privacy risks a privacy by design approach is applied. Privacy risks are identified based on the model of the seven types of privacy by Finn et al. [18] to cope with the variety of privacy aspects in the context of mHealth applications where devices are equipped with a huge variety of sensors as e.g. cameras and GPS localisation. Privacy requirements are modelled based on the concept of privacy protection goals [23], [22]. These requirements are then detailed in in the architecture and data flow oriented context of privacy design strategies [25] where measurements are sketched if possible based on privacy patterns.

2 Background

2.1 Executive Dysfunctions and Goal Management Training

Executive dysfunctions are deficits of brain-damaged patients concerning "the selection and execution of cognitive plans, their updating and monitoring, the inhibition of irrelevant responses and problems with goal-directed behaviour usually result in disorganized behaviour, impulsivity and problems in goal management and self-regulation" [15, p. 17]. To address these disabilities an important therapy is the so-called goal management training (GMT) [35]. The main idea is to divide goals into subgoals and use the resulting list of subgoals to train multistep workflows. These trainings are typically realized based on standard tasks as e.g. proof reading or meal preparation with a pen and pencil approach during therapy sessions. The main steps of GMT are summarized in Fig. 1.

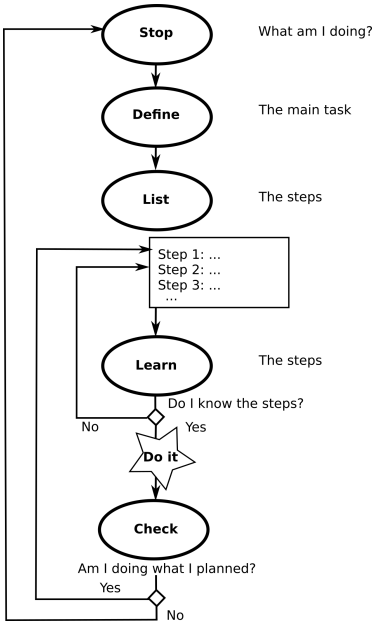

Fig. 1. Main steps of Goal Management Training [35]

Typical study populations in the area of executive dysfunctions consist of 30 to 60 participants with acquired brain injuries, executive dysfunction which are at least 18 years old.

Recent studies which investigate variants of GMT [5], [15] showed that the use of real-life scenarios based on individual tasks relevant to patients foster the motivation of patients. In the traditional paper and pencil approach the use and adaptation of individual tasks is time-consuming. Instead of checking the correctness of the steps after the "Do It" phase in Fig. 1 which could potentially lead to "learning errors", it is recommended to train the workflows based on a documentation e.g. realised by task cards. This approach is called *errorless learning*.

2.2 An mHealth Solution for Goal Management Training

An mHealth solution has the potential to simplify GMT with individual tasks in combination with errorless learning based on a workflow editor and the use of mobile devices for workflow execution. The roles in this scenario, the central process and screenshots of the GMT applications are summarized in Fig. 2.

The central roles are the neuropsychologist as *therapist* and the *patient*. The therapist develops and adjusts workflows based on individual tasks in cooperation with the patient using a workflow editor based on a specific customization of

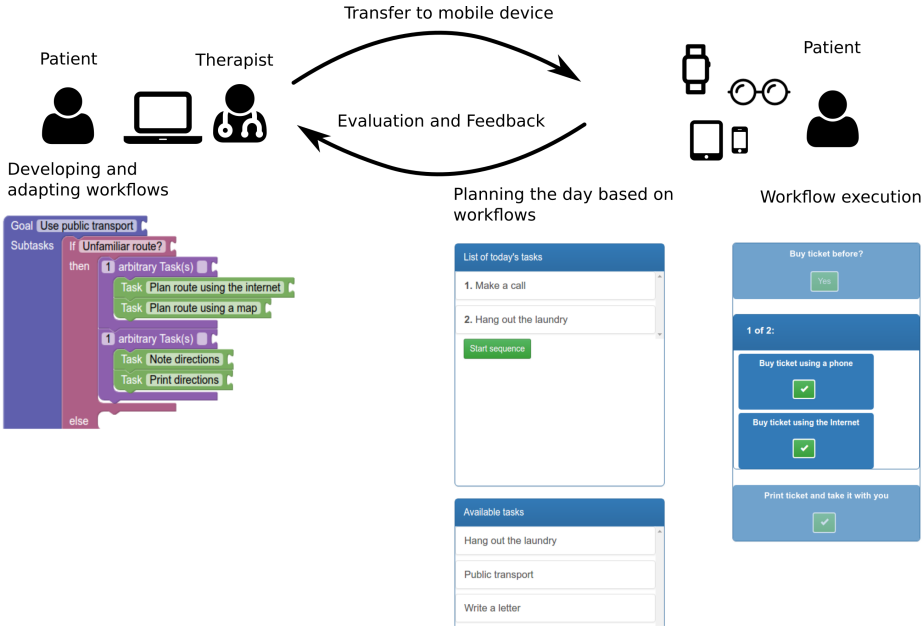

Fig. 2. Roles, process and screenshots of GMT mHealth solution

Google Blockly[5]. These individual workflows are transferred to a mobile device as e.g. a Smart Phone, Smart Watch or Smart Glasses by direct file transfer or via a server identified by a Quick Response (QR) Code. They are guided through daily tasks as e.g. taking public transport or preparing breakfast by predefined workflows which can also be combined to a daily schedule. During workflow execution the patient confirms the completion of a task by clicking it. The patient can provide direct feedback to the therapist about workflow usage and the impact.

At the moment the therapist only gains information about the time between two therapy sessions which is typically a week by the personal report of the patient. The GMT mHealth solution offers the opportunity to gain insight into this blind spot by collecting *outcome measurements* on the smart device. Examples are the number of cancelled workflows or workflows which are "clicked through" which means that a certain amount of tasks is clicked within seconds. Both measurements could give hints to problems in daily life to follow goals. On the other hand it is also possible that the patient was very confident about certain workflows and therefore skipped through the information for assurance. Combined with the personal conversation about the results during the therapy session the therapist gains more insight in the progress of the patient. Patients get training concerning GMT in general and the used GMT solution.

[5] `https://developers.google.com/blockly/`

Hence behavioural data concerning the workflow execution as a basis for the therapy session is collected whereas typical mHealth solutions collect sensor data as e.g. blood sugar level, heart rate or movement data. Since the user group of people with executive dysfunctions is very diverse with respect to the level of disability, education and technical competence, *usability and user acceptance* of the solution and of the concepts to ensure privacy and security is very important.

The GMT mHealth solution was developed in cooperation with therapists. Before the practical use in therapy the effectiveness and user acceptance of the solution has to be evaluated. Therefore a pilot study and afterwards an intervention study are planned before the use in therapy. In this context the role of the *study team* needs to be introduced. To gain first feedback from therapists and patients concerning the proposed GMT solution, a *pilot study* is planned based on a functional prototype. This prototype does not collect any data and also no outcome measurements. The focus is to get feedback from therapists and patients to improve the solution based on interviews and questionnaires. Afterwards an *intervention study* is planned to investigate the effectiveness of the approach and to validate the planned outcome measurements. To allow for comparability, which is necessary for the study, the study team needs access to the workflows and a uniform set of outcome measurements connected to a pseudonym of a patient encompassing information about aborted workflows and workflows which are clicked through..

For the use in therapy the patient can choose the *level of data collection*. Levels which are useful for patients and also the granularity of choice will be investigated in the context of the intervention study. Ideas for such levels are no data collection, collection of the same amount of data as in the intervention study, collect only data about some workflows or collect only statistical data aggregated about all workflows.

3 Privacy and Legal Regulations in the European Union

Prior the review of mHealth solutions from the literature and privacy modelling of the case study which is the basis of the considerations of this paper, we summarise requirements for privacy based on legal regulations in the European Union. Since the mHealth solution used as a case study in this paper is not classified as a medical device, specific legal regulations for medical devices are not considered.

The basis for the consideration about privacy and data protection in the European Union is the Charter of Fundamental Rights of the European Union [16], which considers privacy and data protection in Article 7 and 8. The aspect of privacy is in the focus of Article 7 “Respect for private and family life” stating that “everyone has the right to respect for his or her private and family life, home and communications”. Article 8 on “Protection of personal data” has the focus on data protection where in Article 8(1) it says “Everyone has the right to the protection of personal data concerning him or her” and in Article 8(2) this is detailed as “Such data must be processed fairly for specified purposes and on the

basis of the consent of the person concerned or some other legitimate basis laid down by law. Everyone has the right of access to data which has been collected concerning him or her, and the right to have it rectified.".

Concerning data protection in the European Union compliance with the General Data Protection Regulation (GDPR) [17] is considered which applies from 25 May 2018. The central basis for data protection are summarised in the principles of data protection in Article 5 of GDPR as lawfulness, fairness, transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity, confidentiality and accountability.

For the lawfulness of the processing of personal data for an mHealth application and the corresponding intervention study, *informed consent* of the patients described in Article 6(1) and Article 9(2)(a) concerning health data is needed.

Section 3 details the rights of the data subject concerning *rectification and erasure*. According to Article 20 there is in addition the right to *data portability*, and Article 25 demands the realisation of *data protection by design and by default*. Concerning the security of processing in Article 32 beside the standard technical and organisational measurements the concept of *pseudonymisation* is mentioned which is an important concept in the context of the planned study. In Article 33, 34 regulations concerning data breaches are stated and Article 35 addresses the importance of a *data protection impact assessment*.

4 Privacy and Information Security in mHealth - an overview

Based on the consideration of the legal requirements in the European Union, literature about mHealth is reviewed concerning the investigated aspects of privacy and information security. In the following an overview of scientific literature is considered including the description of mHealth solutions, studies and reviews.

In studies about mHealth solutions typically privacy aspects are only mentioned without further detail. In Volkova et al. [48] where a Food Label Trial app is investigated in a fully automated trial, it is only mentioned concerning privacy that "Ethical and security requirements have also been considered during the app development". Other studies as e.g. [28] focus solely on usability and do not even mention information security and privacy issues. Studies as [19], [50], [41] concentrate on the medical impact and mention at most the existence of an ethics approval. Vogel et al. [47] confirm this perception by stating that for legal compliance mainly informed consent and an ethical approval is needed, wheras Allaert et al. [1] point out the importance of privacy by design for mHealth.

A recent trend in mHealth are app ecosystems as e.g. Apple ResearchKit[6] and Google Study Kit[7]. Based on ResearchKit already studies as the mPower study concerning Parkinson disease [10] are performed where in addition the pseudonymised data is stored on Synapse[8], a general-purpose data and analysis

[6] `http://researchkit.org/`
[7] `https://studykit.google.com`
[8] `https://www.synapse.org/`

sharing service. Mandl et al. [36] analyse the potential for innovation by standardised app platforms. There the need for regulation and certification especially concerning "accuracy, utility, safety, privacy, and security" is stated. A further analysis of such app ecosystems would be important, but is beyond the scope of this paper.

Although in mHealth studies often privacy is not in the focus of the consideration, Peng et al. [40] mention in the context of a user study potential privacy issues of users concerning tracking behaviour and sharing of personal information. Prasad et al. [42] investigate user attitudes towards sharing of information and privacy. Evaluations of health apps [26] reveal several deficits concerning privacy and information security. Other evaluations [45] point out the lack respectively poor quality of privacy policies of mHealth apps, and furthermore the lack of regulatory guidelines and supervision [30], [46], [43], [37].

5 Methodologies for Privacy Engineering

A central requirement of the GDPR [17] is to implement the principles of data protection by design and by default. *Data protection by design* respectively *privacy by design* was first introduced by Langheinrich [33] in the context of ubiquitous systems, where the intention was to develop guidelines for designing privacy-aware systems based on EU legislation and OECD guidelines. He proposes to investigate the seven areas notice, choice and consent, anonymity and pseudonymity, proximity and locality, adequate security, access and recourse.

In a more general approach Cavoukian [11], [12] introduced *seven principles of privacy by design* as a holistic model for privacy integrated in the culture of organisations. The principles proposed there are proactive not reactive, preventative not reactive, privacy as the default, privacy embedded into design, full functionality positive sum, not zero-sum, end-to-end lifecycle protection, visibility and transparency, respect for user privacy.

To realise the central ideas of privacy by design in a concrete mHealth project, we focus on methodologies in the context of privacy engineering. mHealth solutions encompass potentially various smart devices in combination with specialised apps connected to web applications and storing information in backend- respectively cloud services. Hence to start as a methodology for evaluating potential privacy risks of such a complex set of technologies, the model of *seven types of privacy* [18] is used, which differentiates the several types of privacy risks, as shown in Table 1.

Privacy requirements are modelled based on the description of privacy risks using the model of *privacy protection goals* [22,23]. As an extension of the security protection goals confidentiality, integrity and availability the privacy specific protection goals transparency, unlinkability and intervenability are introduced (Fig. 3). To realize the requirements modelled based on these protection goals in a system architecture, *privacy design strategies* [25], [13] can be utilized in the system design process encompassing minimize, hide, separate, abstract, inform, control, enforce, demonstrate (Fig. 4).

Privacy type	Description
Privacy of person	Right to keep body functions and characteristics (genetic codes, biometrics) private
Privacy of behaviour and action	Right to behave in (semi-)public/private space without monitoring or control of actions
Privacy of communication	Right to keep communications private, avoiding interception
Privacy of data and image	Right to keep indiviudals' data private and to exercise control over that data and usage
Privacy of thought and feelings	Right to keep thoughts and feelings private
Privacy of location and space	Right to move about in public or semi-public space without being identified, tracked or monitored
Privacy of association	Right to associate with whomever they wish, without being monitored

Table 1. Seven types of privacy, as proposed by Finn et al. [18]

This system design can be further detailed using *privacy patterns*. Privacy patterns are reusable solutions to recurring privacy problems [44]. These patterns often encompass security related aspects and they are proposed for different phases of the design process, such as requirements engineering, architecture, design and implementation or quality assurance [34,21,20]

Examples include [34] patterns in privacy requirements engineering [29], architectural patterns such as the Data Abstraction or the Privacy Proxy pattern [7], as well as patterns for implementation and design such as privacy transparency patterns (Personal Data Table, Privacy Policy Icons) [44] or patterns regarding the protection goal hide (Cover Traffic, Anonymity Set, Layered Encryption) [20]. Furthermore privacy dark patterns are proposed, trying to "deceive and mislead" users for malicious purposes [9].

6 Privacy Engineering in the Context of an mHealth Solution

6.1 Privacy Risk Identification

The privacy engineering methodologies presented in Section 5 are applied to the GMT mHealth solution. The central basis for the consideration of privacy risks is the level of data collected for the intervention study described in Subsection 2.2. For the use in therapy after the study the level of data collection can be controlled by the patients. There the patients can also choose not to collect any data. To consider the privacy risks especially in the context of smart devices, the model of seven types of privacy is applied (Table 2).

The central risk of the considered mHealth solution for GMT itself is the risk of behaviour tracking by outcome measurements as explained in Subsection 2.2.

In combination with names and descriptions of workflows which are associated with the outcome measurements, it is potentially possible to track behaviour and actions of patients. This is a typical risk of mHealth solutions in neuropsychology, because approaches for behavioural therapy are promising choices for digitalization. Since typical other mHealth solutions focus more on data collection with the help of sensors, the consideration differs in this point. The more general area of eHealth encompasses beside mHealth applications e.g. information systems as Electronic Patient Records which are difficult to compare.

Risk in mHealth scenario / **Privacy type**	GMT risk by outcome measure-ments	General risk of smart devices[1]	Potential risk of extensions[2]
Privacy of person			
Privacy of behaviour and action	✗	✗	
Privacy of communication		✗	
Privacy of data and image		✗	✗
Privacy of thought and feelings			
Privacy of location and space		✗	✗
Privacy of association		✗	

[1] e.g. risks from third-party apps user tracking

[2] location-based workflows, progress documentation (e.g. photos)

Table 2. Types of privacy - privacy risk modelling

Most of the other privacy risks identified here are associated with the use of smart devices in general. E.g. a personal smart phone of the patient where a broad range of apps is installed. In general it is difficult to control, limit and verify the behaviour of third-party apps on a patients device. An example of risks induced by those apps are the use of advertisement SDKs, which leak private data from the phone, such as call logs or location information, to track the users [3]. Furthermore in 2016 the browser plugin *Web Of Trust* (WOT) tracked users and sold their personally-identifiable information [38,39]. Since it is difficult to address these risks by technology, an important element of security and privacy measurements is user risk awareness and training which can be integrated in the general GMT training mentioned in Section 2.2.

Based on first feedback by therapists and job coaches there are possible *extensions* where workflows can also be triggered via location or additional markers such as QR codes. Also in some application areas for workflows it would be important to document the success of the whole workflow or certain steps by images respectively reporting of additional data. These risks are only mentioned here. Since these extensions will not be investigated further in the context of the GMT invention study which is in the center of the consideration here, these risks will not be considered further in this paper.

6.2 Modelling with Privacy Protection Goals and Privacy Design Strategies

In the privacy engineering process we model privacy requirements via the use of privacy protection goals (Fig. 3). The risk modelling is based on the risk areas identified with the model of seven types of privacy in Subsection 6.1.

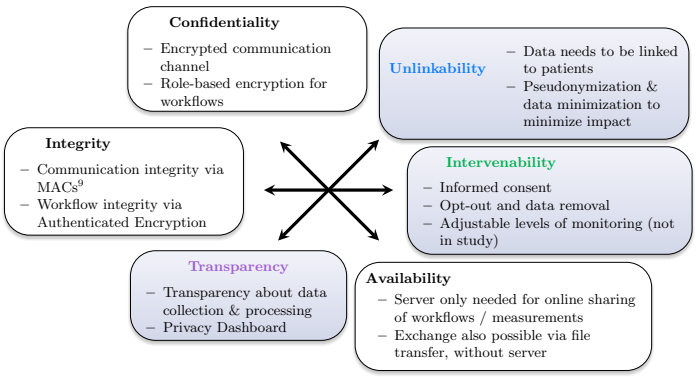

Fig. 3. Privacy Protection Goals in an mHealth scenario

To address the modelled privacy protection goals in the system design process, we use privacy design strategies (Fig. 4). The privacy design strategies are considered in the context of the privacy protection goals with a focus on the privacy goals unlinkability, tranparency and intervenability. There the connection between privacy protection goals and privacy design strategies as proposed in Fig. 4 is used to structure the consideration. Based on the description of these strategies, possible measurements are discussed. If possible privacy patterns are proposed.

Unlinkability: In the context of this use case it is important for therapists respectively the study team to be able to get feedback in terms of outcome measurements linked to a specific patient. The aim to collect personally identifiable data in the context of the GMT mHealth solution, i.e. workflows and associated outcome measurements, is that therapists and the study team get insights in the progress of the therapy of a single patient. Aggregated data about several patients does not make sense to evaluate the progress of a single patient. Because of the number of participants in the intervention study, which is typically between 30 and 60 in the field of GMT [5], and data which is collected continuously over a time-frame of several months, full anonymisation would not be not achievable because of the risk of re-identification.

[9] Message Authentication Codes

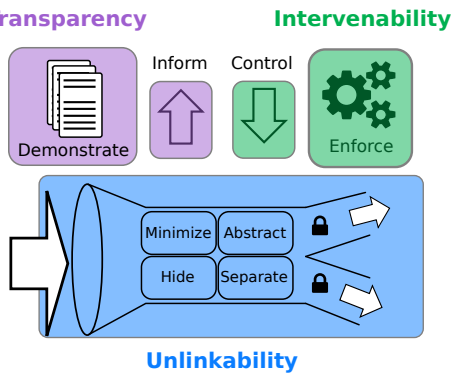

Fig. 4. Privacy Design Strategies

Since all measurements need to be connected to patients, full unlinkability is not possible. Therapists need to know the patient, in the context of the intervention study pseudonyms are sufficient.

The four, *data-oriented* privacy design strategies foster the unlinkability of personally identifiable data to a patient:
MINIMIZE: The collection and processing of personally identifiable data should be minimized as much as possible. Hence the modelling of outcome measurements must be restricted to necessary measurements and patients must be trained adequately. Outside of the intervention study patients can choose to store data only on the device of the user (pattern: Personal Data Store [14]).
HIDE: Strong pseudonymisation techniques should be applied in the context of the study. An option to share workflows between patients and therapists using the server, which is currently implemented, is to share a private link realised by QR codes. This is also known as the Private Link Pattern [14]. The intended encryption measurements are considered for the goal confidentiality.
SEPARATE: In the context of the intervention study it is intended to use a distributed pseudonym table, which is stored on the therapists sides. A similar approach, the so-called Pseudoynm Broker Pattern, which also avoids the use of a central pseudonym table by separation, was proposed by Hillen [24].
ABSTRACT: In addition to data minimization also the collected data should be abstracted as much as possible by data obfuscation [2] respectively statistical disclosure control [27]. Examples of these techniques are the choice of restricted granularity for time and location information, e.g. instead of storing a timestamp for every "click" of the user to detect clicked through workflows, only a specific feature, i.e. several tasks were clicked within a few seconds, is considered.

Transparency: Transparency is important since the user needs to be informed about the processing of personal data and the rights of the data subject concerning opt-out of the study, deletion, rectification and portability of data to foster trust in the mHealth solution and to comply with legal regulations (Section 3).

INFORM: An important pattern to realize transparency is a Privacy Dashboard [44] [14], which is a central place for privacy information in an application and allows the user in addition also to intervene, i.e. to modify, delete and stop processing of personal data, opt-out of the study. In addition the user needs to be informed about potential data breaches.
DEMONSTRATE: Measures as data protection impact assessments, privacy seals respectively certifications are important additional transparency measurements will be potentially considered.

Intervenability: Intervenability in connection with transparency is important to ensure the rights of the data subject.
CONTROL: To control processing of personal data and access to it a Privacy Dashboard is intended to be used. During the intervention study opt-out of the study is possible, which could be also stated to the therapist respectively the study team. When used in therapy, also the level of collection of personal data can be adjusted via this planned dashboard.
ENFORCE: Access to personally identifiable data needs to be restricted. Workflows are transfered with the help of the Private Link pattern. Access to outcome measurements should only be possible for the responsible therapist and during the intervention study also for part of the study team. This can be realized by role-based access control.

Confidentiality Beside the restriction of access by role-based access control and the use of pseudonyms, information security measurements as encryption are important to ensure confidentiality of the information.
HIDE: To strengthen the role-based access control *attribute-based encryption* is planned to use. In general, this type of encryption needs an authority, which issues keys, certifying certain attributes to each user. In ciphertext-policy attribute-based encryption [6], a monotonic tree-access structure can be specified, such that a user has to satisfy a boolean formula of attributes to be able to decrypt a certain ciphertext. This concept could be combined with *authenticated encryption* to furthermore ensure authenticity and integrity. In addition the secrets involved in encryption and decryption should be kept on the client side (pattern: Encryption with User-Managed Keys [14]).

Availability Standard measurements concerning availability of the server are applied, as e.g. backups, etc. As a work around if the server is unavailable, workflows and outcome measurements can also be exchanged via file transfer. The availability of the mobile device which belongs to the patient is not considered.

Integrity Integrity of communication and data is ensured via TLS, using a profile which also provices MACs. Workflow integrity is ensured by authenticated encryption (cf. confidentiality). Integrity does not have an obvious representative in the design strategies, however one may argue that at least the data controller

needs to be aware of data inconsistency to address the problem and inform the user. Hence this can be seen as connected to the process oriented strategies *INFORM, CONTROL*.

7 Discussion and Final Remarks

Privacy engineering methodologies proved to give helpful guidelines for the development of mHealth solutions in neuropsychology and the preparation of the accompanying intervention study. Therefore the chosen structured privacy by design approach was very helpful. The general approach as specified in Section 5 can be transferred to mHealth and eHealth projects in general, but as the risk modelling (Subsection 6.1) showed, the risks in these areas differ.

Identifying privacy patterns which are applicable in a certain situation is still an intricate task: Pattern catalogues[10] and pattern languages [20] are an important first step, but still whole catalogues have to be checked to find the most appropriate pattern. There is a considerable variety concerning levels of abstraction of privacy patterns. Some patterns merely represent a general idea as the Pseudonymous Identity Pattern [7] whereas others focus on very special situations as e.g. the Pseudonym Broker Pattern [24].

In future work the focus will be the investigation and development of privacy patterns in areas which are important for the mHealth environment investigated here. These areas encompass data minimization including data obfuscation, pseudonymization techniques, key management and key exchange.

Based on these design considerations presented here a detailed system design needs to be developed and the usability of the mHealth solution needs to be investigated in depth encompassing measurements for privacy and security. Beside the mere technical design processes and additional organisational measurements to address the rights of the data subjects, also information and training for patients, therapists and the study team needs to be implemented.

Acknowledgment This work was supported by the Ministry for Science and Culture of Lower Saxony as part of SecuRIn (VWZN3224).

References

1. Allaert, F.A., Mazen, N.J., Legrand, L., Quantin, C.: The tidal waves of connected health devices with healthcare applications: consequences on privacy and care management in european healthcare systems. BMC Medical Informatics and Decision Making 17, 10 (January 2017), http://dx.doi.org/10.1186/s12911-017-0408-6
2. Bakken, D.E., Rarameswaran, R., Blough, D.M., Franz, A.A., Palmer, T.J.: Data obfuscation: Anonymity and desensitization of usable data sets. IEEE Security Privacy 2(6), 34–41 (November 2004)

[10] https://privacypatterns.org/

3. Bauer, A., Hebeisen, C.: Igexin advertising network put user privacy at risk (August 2017), https://blog.lookout.com/igexin-malicious-sdk
4. Becker, S., Miron-Shatz, T., Schumacher, N., Krocza, J., Diamantidis, C., Albrecht, U.V.: mHealth 2.0: Experiences, possibilities, and perspectives. JMIR mHealth and uHealth 2(2), e24 (May 2014)
5. Bertens, D.: Doin' it right: Assessment and errorless learning of executive skills after brain injury. [S.l. : s.n.] (2016), http://repository.ubn.ru.nl/handle/2066/149530
6. Bethencourt, J., Sahai, A., Waters, B.: Ciphertext-policy attribute-based encryption. In: 2007 IEEE Symposium on Security and Privacy (SP '07). pp. 321–334 (May 2007)
7. Bier, C., Krempel, E.: Common privacy patterns in video surveillance and smart energy. In: Computing and Convergence Technology (ICCCT), 2012 7th International Conference on. pp. 610–615. IEEE (2012), http://ieeexplore.ieee.org/abstract/document/6530407/
8. Bitglass: The 2014 bitglass healthcare breach report (2014), https://pages.bitglass.com/pr-2014-healthcare-breach-report.html
9. Bösch, C., Erb, B., Kargl, F., Kopp, H., Pfattheicher, S.: Tales from the dark side: Privacy dark strategies and privacy dark patterns. Proceedings on Privacy Enhancing Technologies 2016, 237–254 (July 2016)
10. Bot, B.M., Suver, C., Neto, E.C., Kellen, M., Klein, A., Bare, C., Doerr, M., Pratap, A., Wilbanks, J., Dorsey, E.R., Friend, S.H., Trister, A.D.: The mPower study, parkinson disease mobile data collected using ResearchKit. Scientific Data 3, 160011 (March 2016), http://www.nature.com/articles/sdata201611
11. Cavoukian, A.: Privacy by design: The 7 foundational principles. Implementation and mapping of fair information practices. Information and Privacy Commissioner of Ontario, Canada (2009)
12. Cavoukian, A., Taylor, S., Abrams, M.E.: Privacy by design: essential for organizational accountability and strong business practices. Identity in the Information Society 3(2), 405–413 (2010)
13. Colesky, M., Hoepman, J.H., Hillen, C.: A critical analysis of privacy design strategies. In: 2016 IEEE Security and Privacy Workshops (SPW). pp. 33–40 (2016)
14. Colesky, M., Hoepman, J.H., Bösch, C., Kargl, F., Kopp, H., Mosby, P., Le Métayer, D., Drozd, O., del Álamo, J.M., Martin, Y.S., Gupta, M., Doty, N.: Privacy patterns (2012), https://privacypatterns.org/
15. Emmanouel, A.: Look at the frontal side of life: Anterior brain pathology and everyday executive function: Assessment approaches and treatment. Ph.D. thesis, Radboud University (2017), http://repository.ubn.ru.nl/handle/2066/166754
16. Charter of fundamental rights of the european union (2012/C 326/02)
17. Regulation (EU) 2016/679 of the european parliament and of the council of 27 april 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing directive 95/46/EC (general data protection regulation). Official Journal of the European Union L119, 1–88 (May 2016), http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC
18. Finn, R.L., Wright, D., Friedewald, M.: Seven types of privacy. In: European data protection: coming of age, pp. 3–32. Springer (2013)
19. Gamito, P., Oliveira, J., Lopes, P., Brito, R., Morais, D., Silva, D., Silva, A., Rebelo, S., Bastos, M., Deus, A.: Executive functioning in alcoholics following an mHealth cognitive stimulation program: Randomized controlled trial. Journal of Medical Internet Research 16(4), e102 (2014), http://www.jmir.org/2014/4/e102/

20. Hafiz, M.: A pattern language for developing privacy enhancing technologies. Software: Practice and Experience 43(7), 769–787 (2013)
21. Hafiz, M., Adamczyk, P., Johnson, R.E.: Growing a pattern language (for security). In: Proceedings of the ACM International Symposium on New Ideas, New Paradigms, and Reflections on Programming and Software. pp. 139–158. Onward! 2012, ACM, New York, NY, USA (2012), http://doi.acm.org/10.1145/2384592.2384607
22. Hansen, M., Jensen, M., Rost, M.: Protection goals for privacy engineering. In: 2015 IEEE Security and Privacy Workshops. pp. 159–166 (May 2015)
23. Hansen, M.: The standard data protection model - a concept for inspection and consultation on the basis of unified protection goals (March 2017), https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1_EN1.pdf
24. Hillen, C.: The pseudonym broker privacy pattern in medical data collection. In: 2015 IEEE Trustcom/BigDataSE/ISPA. vol. 1, pp. 999–1005 (August 2015)
25. Hoepman, J.H.: Privacy design strategies. In: ICT Systems Security and Privacy Protection. pp. 446–459. Springer, Berlin, Heidelberg (June 2014)
26. Huckvale, K., Prieto, J.T., Tilney, M., Benghozi, P.J., Car, J.: Unaddressed privacy risks in accredited health and wellness apps: a cross-sectional systematic assessment. BMC Medicine 13, 214 (2015), http://dx.doi.org/10.1186/s12916-015-0444-y
27. Hundepool, A., Domingo-Ferrer, J., Franconi, L., Giessing, S., Lenz, R., Longhurst, J., Nordholt, E.S., Seri, G., Wolf, P.: Handbook on statistical disclosure control. ESSnet on Statistical Disclosure Control (2010)
28. Jenkins, A., Lindsay, S., Eslambolchilar, P., Thornton, I.M., Tales, A.: Administering cognitive tests through touch screen tablet devices: Potential issues. Journal of Alzheimer's Disease 54(3), 1169–1182 (January 2016)
29. Kalloniatis, C., Kavakli, E., Gritzalis, S.: Addressing privacy requirements in system design: the PriS method. Requirements Engineering 13(3), 241–255 (September 2008), https://link.springer.com/article/10.1007/s00766-008-0067-3
30. Kao, C.K., Liebovitz, D.M.: Consumer mobile health apps: Current state, barriers, and future directions. PM & R: the journal of injury, function, and rehabilitation 9(5S), S106–S115 (May 2017)
31. Kokott, J., Sobotta, C.: The distinction between privacy and data protection in the jurisprudence of the CJEU and the ECtHR. International Data Privacy Law 3(4), 222–228 (2013), http://dx.doi.org/10.1093/idpl/ipt017
32. Kumar, S., Nilsen, W., Pavel, M., Srivastava, M.: Mobile health: Revolutionizing healthcare through transdisciplinary research. Computer 46(1), 28–35 (January 2013)
33. Langheinrich, M.: Privacy by design—principles of privacy-aware ubiquitous systems. In: Ubicomp 2001: Ubiquitous Computing. pp. 273–291. Springer (2001)
34. Lenhard, J., Fritsch, L., Herold, S.: A literature study on privacy patterns research. In: 3rd Euromicro Conference on Software Engineering and Advanced Applications (SEAA). Vienna, Austria (August 2017)
35. Levine, B., Robertson, I.H., Clare, L., Carter, G., Hong, J., Wilson, B.A., Duncan, J., Stuss, D.T.: Rehabilitation of executive functioning: An experimental-clinical validation of goal management training. Journal of the International Neuropsychological Society 6(3), 299–312 (March 2000)
36. Mandl, K.D., Mandel, J.C., Kohane, I.S.: Driving innovation in health systems through an apps-based information economy. Cell systems 1(1), 8–13 (2015)

37. McKay, F.H., Cheng, C., Wright, A., Shill, J., Stephens, H., Uccellini, M.: Evaluating mobile phone applications for health behaviour change: A systematic review. Journal of Telemedicine and Telecare p. 1357633X16673538 (October 2016), http://dx.doi.org/10.1177/1357633X16673538
38. heise online: Abgegriffene Browserdaten: WOT-Anbieter will Datenschutz-Vorwürfe prüfen (November 2016), https://www.heise.de/ho/meldung/Abgegriffene-Browserdaten-WOT-Anbieter-will-Datenschutz-Vorwuerfe-pruefen-3455466.html
39. heise online: Daten zu Surfverhalten von Millionen Deutschen als "kostenlose Probe" (November 2016), https://www.heise.de/ho/meldung/Daten-zu-Surfverhalten-von-Millionen-Deutschen-als-kostenlose-Probe-3451556.html
40. Peng, W., Kanthawala, S., Yuan, S., Hussain, S.A.: A qualitative study of user perceptions of mobile health apps. BMC Public Health 16, 1158 (2016), http://dx.doi.org/10.1186/s12889-016-3808-0
41. Pfaeffli, L., Maddison, R., Whittaker, R., Stewart, R., Kerr, A., Jiang, Y., Kira, G., Carter, K., Dalleck, L.: A mHealth cardiac rehabilitation exercise intervention: findings from content development studies. BMC Cardiovascular Disorders 12, 36 (2012), http://dx.doi.org/10.1186/1471-2261-12-36
42. Prasad, A., Sorber, J., Stablein, T., Anthony, D., Kotz, D.: Understanding sharing preferences and behavior for mHealth devices. In: Proceedings of the 2012 ACM Workshop on Privacy in the Electronic Society. pp. 117–128. WPES '12, ACM, New York, NY, USA (2012), http://doi.acm.org/10.1145/2381966.2381983
43. Ranchordas, S., Kaplan, B.: MHealth for alzheimer's disease: Regulation, consent, and privacy concerns. SSRN Scholarly Paper ID 2765976, Social Science Research Network, Rochester, NY (April 2016), https://papers.ssrn.com/abstract=2765976
44. Siljee, J.: Privacy transparency patterns. In: Proceedings of the 20th European Conference on Pattern Languages of Programs. pp. 52:1–52:11. EuroPLoP '15, ACM, New York, NY, USA (2015), http://doi.acm.org/10.1145/2855321.2855374
45. Sunyaev, A., Dehling, T., Taylor, P.L., Mandl, K.D.: Availability and quality of mobile health app privacy policies. Journal of the American Medical Informatics Association 22(e1), e28–e33 (April 2015), https://academic.oup.com/jamia/article/22/e1/e28/700676/Availability-and-quality-of-mobile-health-app
46. Tirman, V.J.: The current state of mHealth applications and the need for improved regulatory guidelines to protect the privacy of patient health information. Ph.D. thesis, Alliant International University (2016)
47. Vogel, M.M.E., Combs, S.E., Kessel, K.A.: mHealth and application technology supporting clinical trials: Todays limitations and future perspective of smartRCTs. Frontiers in Oncology 7 (March 2017), http://www.ncbi.nlm.nih.gov/pmc/articles/PMC5346562/
48. Volkova, E., Li, N., Dunford, E., Eyles, H., Crino, M., Michie, J., Mhurchu, C.N.: "smart"RCTs: Development of a smartphone app for fully automated nutrition-labeling intervention trials. JMIR mHealth and uHealth 4(1), e23 (2016), http://mhealth.jmir.org/2016/1/e23/
49. Vrhovec, S.L.R.: Challenges of mobile device use in healthcare. In: 2016 39th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO). pp. 1393–1396 (May 2016)
50. Zmily, A., Mowafi, Y., Mashal, E.: Study of the usability of spaced retrieval exercise using mobile devices for alzheimers disease rehabilitation. JMIR mHealth and uHealth 2(3), e31 (2014), http://mhealth.jmir.org/2014/3/e31/