**Privacy Engineering: Personal Health Records in Cloud Computing Environments**

*Research-in-Progress*

**Alexander Kaletsch**  
Department of Computer Science  
Technische Universität München  
Boltzmannstr. 3,  
85748 Garching, Germany  
kaletsch@in.tum.de

**Ali Sunyaev**  
Faculty of Management,  
Economics and Social Sciences  
University of Cologne  
Albertus-Magnus-Platz,  
50923 Cologne, Germany  
sunyaev@wiso.uni-koeln.de

**Abstract**

Personal health records (PHR) enable patients to manage their health information in cloud environments. The information contained in PHRs is highly sensitive. Unintended exposure of this data threatens an intimate part of a patient's private sphere and may lead to undesirable consequences. Cloud technologies gain in momentum but also created security issues broadly discussed in academia and practice. Due to possible inherent conflicts, the collaboration of technologies like PHRs and Clouds requires work on security and privacy issues. In our study, we aim to investigate privacy issues, which may apply when using such a cloud service. The findings are supported by a real-world scenario with concrete facts and questions.

Thus, this work presents the research-in-progress by examining the theoretical foundation of PHRs in cloud environments, discussing the upcoming privacy engineering framework, and reflecting the privacy case studies performed on selected PHR systems.

**Keywords:** Privacy/information privacy, Personal health record (PHR), Cloud computing
Introduction

A possible scenario to find in everyday life: Bob and Alice, a married couple, both in their thirties are awaiting their first child. During early pregnancy, Alice was diagnosed with gestational diabetes. Following her gynecologist's advice to see a diabetologist, she went there and told him her medical history again: She has not had any major surgeries, just a weak pollen allergy and was not taking any medication. Her parents and grandparents had not been diagnosed with diabetes, but she remembered Bob's parents to be affected. The physician told her that Bob has an increased risk of also being affected by diabetes due to inheritance. Thus, later that day, she suggested him to go for a full checkup. Fortunately, he was not affected. However, he was diagnosed with high blood pressure and also with elevated LDL cholesterol. This was the moment, when Alice realized that it was time to take action. She saw the current need to gain overview of all family members' medical conditions. When searching the internet, she discovered various online platforms, which would allow storing, updating and sharing electronic health records (EHR), so called personal health records (PHR). Moreover, she found features like family trees, emergency solutions, laboratory tests and care plans. The following night, she discussed her findings with Bob. Being very concerned about privacy, Bob was very skeptical about putting his own and his family's personal medical information onto an unknown company's webserver. He felt like shooting into the dark, while analyzing various standards, certificates, privacy policies, and terms of services in order to find a solution that would meet his functional needs and offer highest security and privacy.

The presented scenario exemplifies how a desire for an online storage for medical information is raised. Not only Bob and Alice have found a PHR to be an essential support to their family’s healthcare planning, but also governments have made major investments and started large projects in recent years to support EHR technologies. In the United States, the Health Information Technology for Economic and Clinical Health (HITECH) Act, which was part of the American Recovery and Reinvestment Act (ARRA) of 2009, released a budget of at least $20 billion for the adoption and use of EHR. In Germany, a national project was set up in order to build a nationwide healthcare telematics infrastructure (HTI). Moreover with the HTI, a new electronic health card (eHC) is going to be introduced in the upcoming years. The combination of HTI and eHC will allow companies to set up secure services, like EHRs or PHRs, which can be exclusively accessed by card owners. Many governments foster EHR technology, which is to be adopted by physicians and hospitals. Those records do not only benefit medical institutions, but are also advantageous for patients. They can gain new insights about their personal state of health by providing information formerly only available at a physician’s practice.

Such a system will most likely be implemented by information technology solution providers, and not by physicians or patients themselves. Naturally, everyone wants to be best in class, offer the fanciest features to their own customers and sell at an affordable price. Hence, cheap and flexible access to storage and computing power is an important topic for these providers. One solution is the utilization of cloud computing. Like every new technology, cloud computing raises new questions as well: If no one knows exactly where data is stored, who is responsible for a piece of information and what to do with information that must not pass a geographical border? How can information security and accordingly a patient’s privacy be ensured? Whenever health information leaks to unauthorized persons, serious trouble for the patient could occur. E.g., a person, who has an increased risk for cancer due to congenital anomalies, might not get a job, because employers being aware of this fact might not hire a potentially ill employee. The stored information is hence highly sensitive and moreover, is protected by law. Such questions and concerns are not to be overcome with changes in stakeholders’ attitudes, but with “an appreciation and an understanding of lay stakeholder perceptions of the risks of technology” (Farahmand et al. 2008). Privacy engineering addresses stakeholders’ perspectives by engaging providers to first assess threats to sensitive information and then built their systems because it embeds “privacy relevant legal primitives into technical and governance design” (Kenny and Borking 2002).

This paper is organized as follows: The upcoming section provides the theoretical background on EHR and cloud computing (CC). This is followed by a description of the research methodology, and some questions we could already answer by performing case studies on public PHRs. We conclude by briefly framing implications and likely contributions of this research.
Theoretical Background

Cloud Computing

The classification of cloud computing by the type of delivery derives three major layers: Infrastructure as a Service (IaaS) “is a single tenant cloud layer where the cloud computing vendor’s dedicated resources are only shared with contracted clients at a pay-per-use fee” (Ramgovind et al. 2010). Especially in IaaS, the omitted initial costs are high, as a lot of hardware can be saved, e.g. servers, routers, load balancers. Those expenses are now charged monthly by the amount of usage. Platform as a Service (PaaS) “provides a high-level integrated environment to design, build, test, deploy and update online custom applications” (Xu 2010). According to (Münzl et al. 2009), PaaS targets software vendors, application developers and value adding resellers, which reengineer applications, extend existing implementations and run prefabricated services on the platform. “Software as a service (SaaS) is software that is owned, delivered and managed remotely by one or more providers” (Smith 2010). Hence, SaaS on the one hand is based on a classic outsourcing strategy and on the other hand it is based on proprietary software (Buxmann et al. 2008). The software generally is delivered with limited functionality, but can be extended and customized which is billed accordingly. A “pay-per-use costing model” (Ramgovind et al. 2010) is applied, which allows to convert fixed expenses into variables.

Another way of distinguishing clouds is the classification by type of deployment. The two basic types are private and public clouds. Hybrid clouds, which are a mix of both private and public clouds, have many special occurrences like community and government clouds. Overlapping clouds share similar characteristics which are explained in this paper. The term private cloud refers to “internal data centers of a business or other organization, not made available to the general public, when they are large enough to benefit from the advantages of cloud computing” (Armbrust et al. 2010). Hence, “all the cloud resources and applications are managed by the organisation itself, similar to Intranet functionality” (Ramgovind et al. 2010). (Ramgovind et al. 2010) state that a private cloud “is easier [than other cloud types] to align with security, compliance, and regulatory requirements, and provides more enterprise control over deployment and use”. (Foley 2008) however states, that “the drawback of private clouds is that IT departments still have to buy, build, and manage them”. A cloud is called a public cloud if “the cloud infrastructure is made available to the general public or a large industry group and is owned by an organization selling cloud services” (Mell and Grance 2010). Generally, public cloud services are based on a per-per-use model, which allows IT departments to decrease upcoming capital investments and switch those into variable operational costs. However, given the cloud’s public availability, security and privacy become important concerns when talking about public clouds. (Ramgovind et al. 2010) assert that “public clouds are less secure than the other cloud models because it places an additional burden of ensuring all applications and data accessed on the public cloud are not subjected to malicious attacks” (Ramgovind et al. 2010). “A hybrid cloud is a private cloud linked to one or more external cloud services, centrally managed, provisioned as a single unit, and circumscribed by a secure network” (Ramgovind et al. 2010). Those external cloud services can be private, public or community clouds, which all “remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability” (Mell and Grance 2010). According to the National Institute of Standards and Technology (NIST), a community cloud “infrastructure is shared by several organizations and supports a specific community that has shared concerns (e.g., mission, security requirements, policy, and compliance considerations)” (Mell and Grance 2010). Hence, a community cloud is a hybrid cloud built exclusively out of private clouds, which can be accessed by any user of those private clouds. European Network and Information Security Agency (ENISA 2011) argues, that “its strengths and weaknesses fall between those of a private cloud and those of a public one”.

Electronic Health Records

ISO/TR 20514:2005 (International Organization for Standardization 2005) offers a very basic definition: an electronic health record is a “repository of information regarding the health status of a subject of care, in computer processable form”. Some authors distinguish between EHR, a single set of information about a patient, and whole EHR Systems (EHRS). In this paper, those terms are used interchangeable. Moreover, literature lists many terms similar to electronic health record (EHR). Those can sometimes
have a similar meaning to EHR, but they also refer to a special kind of EHR. Based on (Runyon 2010), (Rishel and Handler 2008), (International Organization for Standardization 2005) and (Waegemann 2003), the following list of frequently used terms was compiled: clinical data repository (CDR), computer-based / computerized patient record (CPR), electronic medical record (EMR), computer-based / computerized medical record (CMR), digital medical record (DMR), electronic case record (ECR), electronic patient record (EPR), health information exchange (HIE), integrated care record services (ICRS), patient-carried record (PCR), personal health management tool (PHMT), personally controlled health records (PCHR), personal health record (PHR), patient medical record information (PMRI), and population health record.

A Classification of those services is not trivial. In literature, we found the following approaches: classification by health service kind, classification by degree of shareability, classification by information allocation, classification by functionality, and classification by stakeholders. However, there are many more approaches imaginable.

Personal Health Records contain very sensitive personal information. In several countries, different laws exist in order to protect this information and the person whom it is about. Germany, as part of the European Union, has implemented the European Union data protection directive (European Union) in the federal data protection act (Bundesdatenschutzgesetz - BDSG). Thus, for all other EU member states similar privacy laws apply. In extension to privacy laws for personal health record systems, the law for medical products (Gesetz über Medizinprodukte – MPG) may apply. If MPG is applicable, medical product providers have to follow various additional norms (for details see Mauro et al. 2009).

In the United States, there is no general law protecting the privacy of individuals (Sprague 2008). The Health Insurance Portability and Accountability Act (HIPPA) and Subtitle D of the Health Information Technology for Economic and Clinical Health Act (HITECH Act) enforce privacy and security standards for organizations covered by HIPPA and moreover, gain the involved patients special rights. “The Rule confers certain rights on individuals, including rights to access and amend their health information and to obtain a record of when and why their PHI has been shared with others for certain purposes” (U.S. Department of Health & Human Services 2003). Since February 22, 2001, Federal Trade Commission's (FTC) Health Breach Notification Rule applies for all PHR vendors, PHR-related entities or third party service provider for one of those entities, which are not HIPPA covered (FTC http://business.ftc.gov/privacy-and-security/health-privacy).

Comparing German und Unites States privacy laws, a fundamental difference becomes clear: While Germany and the European Union protect personal information, “simply” because it is personal information, in the United States personal information is in general only protected if the organization processing it is covered by HIPPA.

Since there is no general and federal data protection act in the U.S., the United States are not considered to have equal data protection standards to the European Union. BDSG prohibits the transfer of individual-related data into the U.S., in general. However, due to the Save Harbor contract between the United States and the European Union an exception is made for companies which provide self-certification of complying with European Union requirements and register to the United States Department of Commerce. Nevertheless, according to the circle of Düsseldorf (Düsseldorfer Kreis 2010), European companies, which want to export data into the U.S., must not only rely on the self-certification of U.S. organizations, but extra measures have to be taken to ensure their conformance with European regulations. Whenever data exporters fail to do so legal effects can apply.

The examination of data protection laws in U.S. and European Union or Germany, unveils very different positions. Moreover, attempts trying to harmonize those discrepancies are incomplete and, insecurities exist when data shall be interchanged between EU and U.S.

**Research Methodology**

The design science paradigm seeks to solve problems by extending existing boundaries of existing capabilities, which is achieved by the creation of new, previously non-existent, artifacts (Hevner et al. 2004; Simon 1996). Due to the circumstances that this study covers, an upcoming topic in information systems research, the design science approach is utilized: (i) The presented scenario demonstrated that
physicians and patients have an exigent need to use personal health records, which offer various functions and are also affordable. (ii) By analyzing existing literature we examined PHRs and CC technologies in detail. Moreover, by performing several case studies on existing online platforms, we added a practical perspective to our research. Further upcoming research: (iii) A new artifact will be created, which will allow utilizing CC for PHR purposes. The framework will support providers, who want to create new PHRs, but also allow improving existing healthcare IT services in order to be ready for cloud environments. (iv) A web-based prototype will be used for the evaluation of our framework. Tests in laboratories as well as with physicians’ practices are planned. (v) The findings of these tests will be used for further improvement of future framework.

Case Studies

We started our case studies by searching the internet for applicable keywords like „Personal Health Record“ (PHR) and „Electronic Health Record“ (EHR). A list was created containing all fitting results offered by the full-text search engine of Google (http://www.google.de/), Google News (http://news.google.de/) and many other websites concerned with PHRs (e.g. like http://www.myphr.com/resources/choose.aspx). The final list contained over 80 entries. Although this list is considered to be quite long, we do not claim completeness. Every single website was visited. Whenever possible a user-account was created, and the service was analyzed on its own in a separate case study. We focused on the provided functions, the usability of the pages and their privacy policies (PP). Publicly accessible API, as offered by Google Health and Microsoft HealthVault, were reexamined as well (original examination cf. Sunyaev et al. 2010a and Sunyaev et al. 2010b).

The case studies’ results helped to answer the following questions for our scenario-couple Alice and Bob:

What are the “top-threats” for a patient’s privacy?

1. Social functions

Although there are great opportunities, which come with social functions, like “patients empower patients”, there might be even greater risks: E.g., it is possible that users even in a de-identified environment expose themselves by providing identifiable information. Moreover, they may also unintentionally or intentionally provide false information to other patients. In such cases, organizational structures might help, as moderating comments or ensuring that only people with same conditions meet.

2. Selling of medical information

The case studies showed that there are many PHRs, which rely on selling medical information. Mostly, the providers guarantee de-identification and aggregation of data sold. However, the authors were never able to find an explicit list of the data items shared with third parties. Hence, customers are left in the dark about what is in fact done with their medical information. Moreover, they are normally not enlightened about the risks that could appear through re-identification.

3. Advertising & Web analytics

In addition to selling medical information, advertising is often used by third parties to gain revenue from a PHR. Often, services are utilized, which scan the content of the webpage with external software in order to provide targeted advertising. The content presented to the user and, the medical information displayed, could leak to the outside. Web analytics often use similar technologies to advertising. User behavior is tracked by external tools to be evaluated later on. We found many cases where not only third party JavaScript was included, but in addition transparent images were used to trace users. One PHR even included JavaScript from a non-secure source into a secure environment. Unfortunately, this circumstance was only detected by one web browser we used.

Who has access to my medical data?

One of the greatest concerns privacy policies deal with are the access rights to medical information. In – for the user – undesirable PP the data is accessible by nearly everyone, e.g. employees, third party service providers like advertisers or maintenance, and research institutes. In general, those are bound by non-disclosure contracts to the service provider. PHRs with privacy policies that can be considered as “the
better ones”, will not gain access to any third party. However, employees will still be able to access the information. Sometimes the number and type of employees is limited. Nevertheless, it would be desirable that only the user and persons, who are directly authorized by the user, would have access. Measures like client-based encryption could support such an endeavor.

**Can European patients use U.S. services and vice versa? What are the consequences for their privacy?**

Whenever the PHR provider does not block foreign IP addresses, their usage is theoretically possible. However, many solutions cooperate with local third parties, e.g., laboratories or pharmacists. Hence, the utilization does not always make sense.

The European privacy laws are by far stricter than the U.S. ones. Therefore, European patients might relinquish some of their rights when using an U.S. service. Moreover, European physicians, who want to offer such a service to their patients, would need an in-detail compliance check before using a U.S. based PHR.

Large PHR providers, like Google or Microsoft, explicitly offer their services to U.S. citizens only. Microsoft for example cooperates with Siemens in order to establish a redesigned version of HealthVault at the German market under the new brand Assignio, which will comply to the German law.

**Can solutions, which are already on the market, be changed in order to comply with different international privacy laws?**

Sometimes this may be possible by introducing additional privacy protecting measures. However, the business model must not be in conflict with privacy laws. In particular, whenever the model contains the publishing or selling of personal medical information, compliance to European law may be doubtful.

**Is it possible to anonymously join a PHR?**

Yes it is; in some cases. In general, anonymous membership is only possible if a PHR is for free and no payment information is required. Moreover, when joining anonymously, connectivity to hospital information systems and automated data import becomes challenging. Furthermore, anonymous membership does not also mean that the user is really anonymous: There is always the threat of re-identification. Hence, anonymous membership is not a complete solution to privacy concerns.

**How likely is a vendor lock-in to one PHR?**

Many PHRs offer import functions only; then a vendor lock-in is quite possible. Especially, whenever a platform does not provide an API, which would allow the creation of export functionality. However, even if a platform has an API, it is important that the API offers support for standard exchange protocols like CCR or CCD and does not solely rely on proprietary specifications. Whenever additional frameworks or full libraries are provided for a PHR’s API, the likelihood of a vendor lock-in is even more reduced.

**Does the utilization of cloud computing make a difference in privacy concerns?**

Unfortunately, only very few services were found which utilized cloud technologies and showed this fact openly. The ones, which did, mostly had quite convincing privacy policies. However, many services reviewed had quite disadvantageous privacy policies for their users. Thus, it would not make a difference for them whether cloud computing is employed or not.

**In a nutshell: What PHR can be recommended to Alice and Bob?**

Unfortunately, there was no single PHR that could be recommended without limitations. An alarming number of services with disadvantageous privacy policies and other critical failures exist. Hence, there is a large number of PHRs which cannot be recommended. However, there are also some promising approaches.

**PHR function assessment**

One of our primary pillars is the assessment of PHR functions, which may influence patients’ privacy. During the case studies, we collected various functions provided by the reviewed PHRs. For each function, we have performed highlighted specific risks that could apply and have given solutions in order to
overcome the issues presented. Moreover, a PHR does not only contain user-centric functionality, but also basic functions, which also need to be assessed. Table 1 contains some selected examples of PHR functions, their risks and solutions. The risks presented result from the observation of the services and from the analysis of their privacy policies. They were categorized by our team into subjective risk levels, which reflect the amount of damage the disclosure of the personal data could cause to the affected patient. We use signal lights to visualize the risk levels:

- Green represents a medium risk for privacy breaches,
- yellow represents a high risk level, and
- red represents an very high risk.

<table>
<thead>
<tr>
<th>Name</th>
<th>Risks</th>
<th>Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action Plan</strong></td>
<td>Over extensive Questionnaires: In general, before an action plan is recommended, the patient has to fill out at least one questionnaire. The case studies showed that these sometimes were quite extensive and contained many unnecessary questions.</td>
<td>Stick to the Questions needed. Do not ask too much, but also not too little.</td>
</tr>
<tr>
<td><strong>Collaboration Tools</strong></td>
<td>While collaborating via chat, phone or video, uncontrolled and unintended information may flow.</td>
<td>Allow collaboration between patients and physicians only. All communication must be covered by the physician-patient secrecy. Moreover, all communication must be documented in an accountable and non-reputable way.</td>
</tr>
<tr>
<td><strong>Emergency Card</strong></td>
<td>An emergency login will be used, whenever the originally authorized user is unable to do so. This directly implies that there is a way of circumventing the original login procedure. In the case studies, so-called emergency cards were handed out to the patients, which contained special login information. Those could be stolen and abused.</td>
<td>An emergency access must be restricted to information crucial in emergency cases. The person using the emergency login must prove its authorization to access this information in a non-reputable way.</td>
</tr>
<tr>
<td><strong>Medical History and Family Tree</strong></td>
<td>A family member may enter information about other family members, who do not want to use the service.</td>
<td>The PHR may use the information about family members, e.g. for automated calculations authorized by the enrolled family member. It must not use the data otherwise, e.g. for creating personal profiles of the other family members. Contact may only be established after a successful invitation of the family member by the information providing family member.</td>
</tr>
<tr>
<td><strong>Medical Image Exchange</strong></td>
<td>Medical images are often of quite large scale and consume high disc volumes. Thus, these are good candidates for outsourcing to storage clouds. Especially, public clouds may not be secure enough to prevent privacy gaps efficiently.</td>
<td>When public clouds are utilized all data should be sent and stored only in encrypted form.</td>
</tr>
</tbody>
</table>
Reminder

Whenever reminders are sent out through unsecure communication like email or SMS additional risks may appear.

The reminders should not contain critical personal identifiable information. Instead links or references to the secured environment of the PHR should be provided.

Social Network Elements

Users may post information to the public, without realizing that in doing so, their privacy might be threatened.

Social engineering attacks or social environment analyses may be performed.

Anti-crawling measures, word-filters, moderated discussions, and grouping of patients according to confirmed diseases, help to ensure patients’ privacy.

Practical Instantiation of the proposed Privacy Engineering Framework

The assessment of PHR functions is just one pillar of the larger framework we are currently working on. Additionally, we are creating a security model which allows ensuring patient’s privacy by technical measures, e.g., client side encryption of medical information. The framework is already being partly evaluated: A prototype was built, which allows general practitioners to securely transfer information to specialists. The online referral and appointment planer (ORAP) is built by a collaboration of researchers and physicians, who applied the introduced privacy engineering framework. ORAP is an application using cloud computing technologies while dealing with electronic health records: The prototype utilizes German healthcare telematics infrastructure (HTI) components (cf. the introductory section of this paper) in order to provide secure encryption and signatures for all documents transferred. Amazon’s S3 Cloud is used for temporary storage of largely scaled attachments, which are of course also encrypted. The collaboration with selected physicians enables the iterative improvement of the prototype and the framework. In the upcoming months, the first real patients will join the tests.

Figure 1 shows the ORAP security model, which is one instantiation of the security model we are currently working on. It is modeled in a simple use case diagram in order to be comprehensible for information systems researchers as well as physicians. The model reflects the outcome of a long ongoing planning phase in cooperation with the physicians taking the current German laws under consideration: EHR must only be stored at the physicians’ practices, which are considered to be the only trusted environments. EHRs must not leave a physician’s practice without being encrypted and signed beforehand. Solely the recipient, that is, the specialist, must be able to verify and decrypt the received EHR. Currently, there is no PHR functionality available and only EHR are exchanged. Further PHR functions are planned for the future. But today, the patient’s home is not to be considered a secure environment as there is currently no specification available of how the patients will be able to access the HTI from their homes. Moreover, the
current health card specification allows delivering electronic health cards (eHC) without signature functionality. Although the outcome is unclear, there are plans to copy the signature functionality onto the eHC later on. Therefore, it was impossible to integrate patients in the current model.

During the process of creation, the functions offered by ORAP were also analyzed similarly utilizing the PHR function analysis. It has to be mentioned that ORAP is currently not intended to be a full-scaled PHR. In particular, ORAP does not enable its users to work with single EHRs entries directly, e.g., viewing or updating them. It just allows transferring them securely when a referral is made. However, it includes elements and functions, which were found at other PHRs during the case studies. Hence, these needed to be analyzed. Table 2 shows the results.

<table>
<thead>
<tr>
<th>Name</th>
<th>Analysis</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address Book, Appointment Scheduling, Calendar, and Physician Finder</td>
<td>There will be no personal-identifiable information about patients used at any of such functions (medium risk). However, as general practitioners explicitly requested the openness of the system for new patients, the calendars and addresses of general practitioners are only open to the public. New patients are allowed to enter their basic information online, which is later validated at the physician’s practice. Due to the fact that patients currently cannot sign their entries online in the first place, this functionality has to be ranked with a high risk.</td>
</tr>
<tr>
<td>Medical Image Exchange</td>
<td>Medical images as well as an arbitrary appendix can be added to a referral. They will be encrypted with the public key of the receiving physician and hence, he will be the only one able to decrypt them. All encrypted appendices are temporarily stored at Amazon’s S3 cloud.</td>
</tr>
<tr>
<td>Referral service</td>
<td>All data leaving a physician’s practice is encrypted and signed. It can only be decrypted by the receiving specialist. This is ensured by the utilization of the healthcare telematics infrastructure.</td>
</tr>
</tbody>
</table>

**Conclusion and further research**

In particular, many PHRs are offered in the United States. The decision whenever to use such a service is not easy. Our scenario with Alice and Bob reflects common patients’ needs. Among functionality, they want to protect their privacy. This study addresses both needs and reflects their strong interactions.

Protecting patients’ privacy is the key in order to build trustworthy PHRs. Unfortunately, not all existing PHRs are to be considered trustworthy. Therefore, we have provided questions and metrics, with which risk rankings can be performed. Both, users and providers, will profit from such Privacy Engineering measures as trust claims can be more easily controlled. However, trust can also be established based on facts.

Further research is currently performed to finalize the presented privacy engineering framework. Based on a Plan-Do-Check-Act cycle, different phases of the PHR development process will be supported. The function analyses will not only be presented for PHR functions, but also for basic functionalities like storing and sharing of personal health information. There will also be a differentiation of all types of deployment and delivery for cloud computing services. The final security model will be introduced, which instantiation was presented for ORAP. For each phase in the framework, checklists will be provided helping the users to perform all activities needed. Additionally, the following questions are going to be researched in future: What are the business impacts of the framework utilization? Are physicians and patients willing to pay additional costs that may apply? Are they willing to take the efforts of using software that is especially hardened, e.g., client virtual trusted environments? How can new, upcoming security concepts, like data coloring or search over encrypted items, be seamlessly integrated to the privacy engineering framework?
References


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: 95/46/EC.


