ONE SIZE DOES NOT FIT ALL: INFORMATION SECURITY AND INFORMATION PRIVACY FOR GENOMIC CLOUD SERVICES

Scott Thiebes  
*University of Cologne, thiebes@wiso.uni-koeln.de*

Tobias Dehling  
*University of Kassel, tdehling@uni-kassel.de*

Ali Sunyaev  
*University of Kassel, sunyaev@uni-kassel.de*

Follow this and additional works at: [http://aisel.aisnet.org/ecis2016_rip](http://aisel.aisnet.org/ecis2016_rip)

**Recommended Citation**
Thiebes, Scott; Dehling, Tobias; and Sunyaev, Ali, "ONE SIZE DOES NOT FIT ALL: INFORMATION SECURITY AND INFORMATION PRIVACY FOR GENOMIC CLOUD SERVICES" (2016). Research-in-Progress Papers. 75.  
[http://aisel.aisnet.org/ecis2016_rip/75](http://aisel.aisnet.org/ecis2016_rip/75)
ONE SIZE DOES NOT FIT ALL: INFORMATION SECURITY AND INFORMATION PRIVACY FOR GENOMIC CLOUD SERVICES

Research in Progress

Thiebes, Scott, University of Cologne, Cologne, Germany, thiebes@wiso.uni-koeln.de
Dehling, Tobias, University of Kassel, Kassel, Germany, tdehling@uni-kassel.de
Sunyaev, Ali, University of Kassel, Kassel, Germany, sunyaev@uni-kassel.de

Abstract

Most extant genomic cloud services strive to maximize information security and information privacy protection thereby neglecting the diversity of information practices in genomic research. Such a one-size-fits-all approach is not expedient and decreases the overall system usability and performance. While there is growing awareness that employed information security and information privacy measures must adapt to information security and information privacy requirements inherent to information practices, limited design knowledge exists on how to actually design genomic cloud services capable to account for differences in information practices in genomic research. In this research-in-progress, we propose a model for genomic cloud services that dynamically adapt to the diverse information security and information privacy requirements in genomic research. Our research contributes to the scientific knowledge base by capturing design knowledge for secure, privacy-preserving, and usable genomic cloud services, accounting for conflicts between information security and information privacy, and fostering understanding of information privacy as a context-sensitive construct.

Keywords: Information Security and Information Privacy, Genomic Cloud Computing, Healthcare Information Systems, Design Science Research

1 Introduction

With the advent of next generation DNA sequencing and availability of large volumes of genomic data (Koboldt et al., 2013, Stein, 2010), storage and processing of genomic data has become a bottleneck in genomic research (Afgan et al., 2011, Friend and Norman, 2013, Onsongo et al., 2014). Cloud computing (CC) has been heralded as a solution to overcome the deficits of storage and processing resources in genomic research (Friend and Norman, 2013, Stein, 2010). Hence, increasing numbers of researchers in the field of genomics are now turning to the cloud (Afgan et al., 2011, Chung et al., 2014, Heath et al., 2014). Despite the glaring benefits CC offers to genomic researchers, like its capabilities to store and process large volumes of sequencing data (Dove et al., 2015) or its increased cost-efficiency (Afgan et al., 2011), ensuring information security and information privacy (henceforth, information security and privacy) of genomic cloud services (GCS) remains a challenge (Dove et al., 2015, Heath et al., 2014).

Information security and privacy of GCS are of particular interest from an information systems (IS) perspective. A unique characteristic of genomic research is the high variability in information sensitivity ranging from freely available human genomic data in the public domain with rather low sensitivity to just-sequenced private human genomic raw data with very high sensitivity that reveals very detailed information and cannot be reliably anonymised (Gymrek et al., 2013). On the one hand, maintaining high levels of information security and privacy is increasingly important with rising information sensitivity because access to genomic data is a prerequisite for furthering medical knowledge and infringe-
ment of data donors’ privacy reduces their willingness to make their genomic data available (Dehling et al., 2015, Dove et al., 2015, Heath et al., 2014). On the other hand, unnecessary information security and privacy measures are a burden for processing information with low sensitivity due to computational overhead and the emergence of workarounds negating the effectiveness of employed information security and privacy measures (Adams and Sasse, 1999, Balfanz et al., 2004, Lampson, 2009). Depending on the information involved in performed computations, GCS have to adapt employed information security and privacy measures along a continuum emphasizing computational power and ease of use on the one end and protection of information security and privacy on the other end. For GCS, a one-size-fits-all approach to information security and privacy is therefore not feasible. A one-size-fits-all approach will either waste computational resources and bandwidth, which would incur unnecessarily high costs and slow down scientific progress, or it will fail to maintain information security and privacy, which would result in financial and legal penalties, limit data donors willingness to provide genomic data (Diamond et al., 2008), and, most importantly, result in irreparable invasions of data donors’ privacy incurring incalculable future damages.

While there is increasing awareness among researchers that employed information security and privacy measures must adapt to information security and privacy requirements inherent to employed information practices (Chin et al., 2011, Dove et al., 2015), most existing GCS are still designed with maximum information security and privacy in mind (DNAnexus Inc., 2014, Heath et al., 2014). Limited design knowledge exists on how to design GCS capable to adapt to the diverse information practices required in genomic research, while maintaining information security and privacy without unnecessarily sacrificing computational power and usability. To facilitate development of secure and privacy-preserving, yet usable, GCS, the objective of our research is to create design knowledge for GCS capable to dynamically adjust to the varying information security and privacy requirements associated with the diverse information practices found in genomic research.

This study contributes to the scientific knowledge base by developing an architectural model for GCS with dynamic information security and privacy in form of a system component model. Our model facilitates the development of secure, privacy-preserving, and usable GCS. We also foster the understanding of information privacy as a context-sensitive construct and highlight the importance of including usability considerations in design, implementation, and application of information security and privacy measures.

2 Related Research

2.1 Genomic Cloud Services

Genomic cloud services are a particular form of biomedical cloud computing (i.e., the use of CC in biomedical settings) that primarily work with genomic data and related meta-data (Heath et al., 2014). Compared to traditional IT infrastructures, CC offers several benefits to genomic research. First, it provides researchers with seemingly unlimited resources, which allows for storage and processing of very large genomic data sets (Dove et al., 2015). Second, it increases cost-efficiency of genomic analyses because necessary computing resources can be provisioned on-demand (Afgan et al., 2011). Lastly, CC eases the sharing of genomic data between different researchers since data can be stored on a central storage server, accessible by anyone from anywhere (Friend and Norman, 2013). Despite these potential benefits there remain issues associated with using CC in genomic research. Due to the nature of genomic analyses, GCS have the potential to invade privacy. Access to genomic data is accompanied with personal, social, professional, financial, and insurance-related risks (Shoenbill et al., 2014). Although CC providers are typically able to make larger investments in security than average research facilities and may thus provide increased levels of information security (Dove et al., 2015), inherent characteristics of CC also offer new vectors for attacks and data breaches (Garber, 2012, Nanavati et
al., 2014, Sunyaev and Schneider, 2013). Thus, protection of information security and privacy in GCS is an often-voiced concern (Dulpé and Joly, 2014, Dove et al., 2015, Schatz et al., 2010).

Extant research in the areas of cloud computing and genomics focuses mainly on fundamental benefits of using CC to store and analyse genomic data (e.g., Stein (2010)), ethical and legal implications of large-scale access to genomic data (e.g., Dove et al. (2015)), or technical details of performing genomic analyses in CC environments (e.g., Chen et al. (2013)). Another issue concerns usability of GCS (Schatz et al., 2010). Setup and operation of CC instances can be a tedious process that requires technical expertise (Afgan et al., 2011, Chung et al., 2014). Since average users of GCS (e.g., medical professionals and biologists) usually do not possess the required technical expertise, GCS must provide adequate usability. Although extant research recognizes the relation between usability and information security and privacy, current research on usability of GCS centres on providing researchers with easy to use tools with graphical user interfaces (e.g., Afgan et al. (2011) and Chung et al. (2014)) and not the usability of employed information security and privacy measures.

Today, most GCS employ a one-size-fits-all approach to information security and privacy. For example, DNAnexus and Seven Bridges Genomics, two leading providers of GCS, state that all data at rest or during transmissions are encrypted by their services, irrespective of individual information security and privacy requirements (DNAnexus Inc., 2014, Seven Bridges Genomics Inc., 2016). Similarly, the Google Genomics website claims that their services meet or exceed U.S. regulations for the protection of health-related information (Google Inc., 2016), whereas Amazon Web Services provides several layers of encryption, leaving the decision about what data is being encrypted up to their users (Pizarro and Whalley, 2014). Given the sensitive nature of genomic data and related strict regulation (Dove et al., 2015), this overcautious behaviour is no surprise. Nonetheless, there is a wide range of different kinds of genomic data (e.g., identifiable human genomic data, and potentially unidentifiable human genomic data) (Lowrance and Collins, 2007), which exhibit a rich diversity of information security and privacy requirements. Overprotection of genomic data caused by too tight or unfitting information security and privacy measures decreases system usability (Lampson, 2009, Yee, 2004) and performance, for instance, due to computational overhead caused by performing unnecessary encryption (Nadeem and Javed, 2005), consequentlyimpeding utility of GCS.

With our research we seek to bridge the gap between information security, information privacy, usability, and performance considerations for GCS. Our research aims to develop an architectural model for GCS that is capable to adapt to the diverse information security and privacy requirements found in genomic research. GCS that are based on our architectural model will provide usability and efficacy while maintaining adequate information security and privacy.

2.2 Information Security and Information Privacy

Information security and information privacy are complex concepts for which various definitions have been proposed. The generally accepted core conceptualization of information security is the so-called CIA triad (Dehling and Sunyaev, 2014, Kessler, 2012) that stipulates confidentiality, integrity, and availability as the three key requirements for information security. Although definitions of information security frequently include additional requirements such as, for example, authenticity or non-repudiation, we focus on the CIA triad as core conceptualization of information security in this paper.

Similar to information security there is no broadly accepted definition of information privacy (Bélanger and Crossler, 2011). In accordance with the conceptualization of information privacy as a form of control by Smith et al. (2011), we understand information privacy as an individual’s interest in controlling or at least significantly influencing the flow of her personal information (Clarke, 1999). Information privacy is a contextual concept influenced by contextual factors like cultural norms, the legal environment, or type and purpose of collected information (i.e., information practices) (Smith et al., 2011). As such, the interest individuals have in controlling the flow of their personal information varies depending on encountered contexts (Birge, 2009). As previous research shows, implementation of too tight or unfitting information security and privacy measures decreases an IS’ overall usability.
Genomic Cloud Services

(Lampson, 2009, Yee, 2004) and might as well slow down computational performance (e.g., even non-critical data is encrypted and must be decrypted before it can be processed). As a result, users circumvent implemented information security and privacy measures to be able to fulfill their tasks more efficiently (Lampson, 2009, Theofanos and Pfleeger, 2011). Thus, too tight or unfitting information security and privacy measures have a detrimental effect and render IS insecure (Balfanz et al., 2004).

3 Research Approach

Drawing from the design science paradigm (Gregor and Hevner, 2013, Hevner et al., 2004), we employ the heuristic theorizing framework (HTF) (Gregory and Muntermann, 2014) in order to develop an architectural model for GCS with dynamic information security and privacy. The HTF is a normative framework for proactive design theorizing. Its central components are heuristic search and heuristic synthesis in conjunction with concurrent evaluation. Heuristic search is an iterative problem-solving process that consists of the recurrent application of problem structuring heuristics (e.g., problem decomposition) and artefact design heuristics (e.g., modelling). Heuristic synthesis refers to engaging in “synthesizing the newly generated information from the recurrent use of heuristics“ (Gregory and Muntermann, 2014) thereby creating new design knowledge. In the following, we focus on the problem structuring process and initial artefact design.

3.1 First Problem-Structuring Round: Literature Review

During heuristic search, we performed two rounds of problem structuring. First, we reviewed extant literature on information security and privacy requirements for cloud-based health IT. We focused on cloud-based health IT instead of GCS because GCS are a specialized form of cloud-based health IT. Our search in pertinent scientific online literature databases (i.e., Proquest, EBSCOHost – Academic Search Complete, Business Source Complete, and MEDLINE –, MEDPILOT, and PubMed) yielded a total of 9,919 publications. Publications were assessed for relevance, resulting in a final sample of 38 publications deemed relevant. We excluded publications that were duplicates (1,835), not peer-reviewed (556), not written in English (115), published before 2006 since the term CC only gained widespread recognition in 2006 (1,259) (Regalado, 2011), or off-topic (i.e., they did not address information security and privacy requirements for cloud-based health IT services; 6,116). The review process was documented; a detailed protocol is available from the authors on request.

Publications in the final sample were analysed and 413 information security and privacy requirements extracted. We aggregated similar requirements to 65 so-called master requirements in order to account for redundancies and different levels of analysis. The requirements ‘Fine-grained Access Control’ and ‘Role-based Access Control’ were, for example, both aggregated to the master requirement ‘Access Control’. Further analysis of identified master requirements revealed that there exist potential conflicts between some requirements. For instance, the master requirement ‘Recoverability’ (i.e., being able to restore lost data to a user-specified point in time) necessitates that cloud service providers keep a copy of deleted data. As such, ‘Recoverability’ is integral for ensuring the availability aspect of information security (cf. section 2.1). However, keeping deleted information available might at the same time result in a violation of data owners’ information privacy, thus causing a conflict between information security and information privacy. Ultimately, this observation led us to the conclusion that a one-size-fits-all approach to establish information security and privacy for GCS is not practicable. We thus decided to further refine our research problem and to engage in a second problem-structuring round by conducting focus groups with experts from the domains of cancer genomics and information security and privacy research in CC environments.

3.2 Second Problem-Structuring Round: Focus Groups

This research is embedded in a multi-disciplinary cancer genomics research project (short MILES), described in detail at: MILES Project Consortium (2016). It is organized in five subprojects (A to E)
and incorporates various streams of genomic cancer research as well as information security and privacy research in CC environments. In the second problem-structuring round focus groups were conducted with researchers from all involved subprojects in order to identify information practices present in the MILES research project. The results were used to inform the design of our architectural model for GCS (see section 4.1 for a detailed description of the model).

Focus groups are frequently used as a qualitative research method in diverse areas, such as market research, social research and also medical research (Stahl et al., 2011). They are an effective approach to obtain a detailed understanding of a problem and to elicit initial solution concepts (Schmidt-Kraepelin et al., 2014). Moreover, focus groups are a valuable tool for “exploring and recognizing the socio-technical nature of IS” (Stahl et al., 2011). Prior to conducting focus groups it is necessary to decide on the sample size (i.e., the number of participants in each focus group) as well as how many focus group sessions are to be held. There are no definite numbers on how many participants to include in each session and how many rounds to conduct. However, existing literature suggests between six and twelve participants per session (Kleiber, 2004, Krueger and Casey, 2000) and three to five rounds of focus group sessions (Kleiber, 2004). We conducted four rounds of focus groups with eight to ten participants in each session. Since the objective of conducted focus groups was to identify information practices for individual subprojects as well as possible information practices among subprojects, it was important that each subproject was represented at each focus group session. Hence, at least one member of each subproject participated in each focus group session, with the exception of session three, where no member of subproject A was able to attend. An important aspect of focus groups is to establish an open-minded and friendly atmosphere in order to facilitate discussions among participants (Kleiber, 2004). Accordingly, all participants introduced themselves and their role in the overall research project briefly during the first focus group session. Participants were seated in a U-shape or a circle in a modern conference room, which added to the friendly and comfortable atmosphere and facilitated discussions. Focus groups were conducted between March 2015 and July 2015 and lasted around 90 minutes each. After each focus group two researchers involved in subproject E discussed results and notes were taken. Based on this data information practices present in the MILES research project were identified, documented, and analysed.

4 Results

4.1 Architectural Model for GCS with Dynamic Information Security and Privacy

After our problem was sufficiently structured, we applied an artefact design heuristic (i.e., modelling) in order to develop our artefact design. It resulted in an architectural model for GCS that is capable of dynamically adapting to the diverse information security and privacy requirements in genomic research (cf. figure 1). In the following, we first outline our architectural model and then describe how the design of this model is informed by the information that was generated during the two problem structuring rounds in section 4.2.

Our model contains multiple data storage & processing units. Each unit stores genomic data with similar information security and privacy requirements and is enclosed in its own security & privacy unit. Security & privacy units are responsible for ensuring information security and privacy based on the information security and privacy requirements exhibited by stored data. Moreover, security & privacy units communicate information security and privacy requirements of contained data (e.g., who is allowed to access the data or what physical location the data may be stored at) to the other components of our model such as the privacy supervisor. The privacy supervisor inspects privacy requirements exposed by individual security & privacy units and ensures that all information privacy requirements are fulfilled. Any access to data must be authorized by this component.
Figure 1. Model for GCS with Dynamic Information Security and Privacy.

Moreover, genomic cloud computing involves the analysis of very large genomic data sets (Dalpé and Joly, 2014, Marx, 2013). Such analyses often require access to data from various sources. Therefore, the data transfer optimization manager organizes available data such that time-consuming transfers of very large amounts of data between storage and processing units are reduced to a minimum. A possible approach is, for example, the use of neural networks, which have proven to be effective means for optimization of resources provisioning in CC environments (Islam et al., 2012).

The application provisioning panel represents the central interface for users of GCS. After authentication users are presented with all information they need to create new or access existing virtual machine instances (i.e., available data sources and data analysis applications) in order to perform their analyses. To create a new virtual machine instance users simply select the data and applications they require. The application provisioning panel will then create a virtual machine instance containing selected data and applications. The administration panel allows administrators to configure all aspects of the GCS. This includes, but is not limited to, adding, changing, or removing storage & processing units, setting up security measures, and managing genomic analysis applications available to users in the application provisioning panel. The administration panel component has only partial access to the storage & processing units since they may as well integrate external cloud services over which administrators might not have full control.

4.2 Model Design Rationale

Focus group sessions revealed that subprojects A to D employ nine different types of information practices (IP1-9, see table 1), which represent the main design rationale for our architectural model.

Identified information practices are subject to diverse information security and privacy requirements. Focus group discussions emphasized that all participating subprojects (with the exception of subproject E) require storing (IP1, IP2) and processing (IP4, IP5) of large human genomic datasets, whereas subprojects A and C also require storing (IP3) and processing (IP6) of animal genomic datasets. Clearly, animal genomic data is not as sensitive as human genomic data already in the public domain. Moreover, subprojects access private, non-published genomic data as well as published human genomic data (IP2; IP5) from sources such as, for example, The Cancer Genome Atlas\(^1\) or the International Cancer Genome Consortium.\(^2\) Similar to the distinction between human genomic and animal genomic data, private human genomic data requires tighter protective measures than human genomic data already in the public domain.

---

\(^1\) https://tcga-data.nci.nih.gov/tcga/

\(^2\) https://dcc.icgc.org
Table 1. Identified Information Practices.

<table>
<thead>
<tr>
<th>Code</th>
<th>Information Practice</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP1</td>
<td>Storage of unpublished (identifiable and unidentifiable) human genomic data.</td>
</tr>
<tr>
<td>IP2</td>
<td>Storage of published (identifiable and unidentifiable) human genomic data.</td>
</tr>
<tr>
<td>IP3</td>
<td>Storage of unpublished animal genomic data.</td>
</tr>
<tr>
<td>IP4</td>
<td>Processing of unpublished (identifiable and unidentifiable) human genomic data.</td>
</tr>
<tr>
<td>IP5</td>
<td>Processing of published (identifiable and unidentifiable) human genomic data.</td>
</tr>
<tr>
<td>IP6</td>
<td>Processing of unpublished animal genomic data.</td>
</tr>
<tr>
<td>IP7</td>
<td>Sharing of unpublished (identifiable and unidentifiable) human genomic data.</td>
</tr>
<tr>
<td>IP8</td>
<td>Sharing of published (identifiable and unidentifiable) human genomic data.</td>
</tr>
<tr>
<td>IP9</td>
<td>Sharing of unpublished animal genomic data.</td>
</tr>
</tbody>
</table>

The diversity of information security and privacy requirements for identified information practices confirms our assertion from the first problem-structuring round that a one-size-fits-all approach is inappropriate for information security and privacy management. Our model has to be designed in a way that allows for dynamic adaptation to the diverse information practices. The different storage & processing units in our model allow for logical grouping of different kinds of genomic data, each with their own level of sensitivity and of associated information security and privacy requirements. By grouping genomic data according to their particular information security and privacy requirements and enclosing each storage & processing unit with its own security & privacy unit, our model ensures that data receives as much protection as necessary, but as little as possible. This design choice is additionally useful because it reduces impacts of potential conflicts between information security and privacy requirements that we identified in the literature review.

Next to ensuring information security and privacy of genomic data in GCS, usability and data transfer performance of GCS emerged as central topics during focus group sessions. While grouping data with similar information security and privacy requirements in different storage & processing units enables our model to dynamically adapt itself to the various levels of sensitivity induced by stored data, it might as well increase complexity if too many storage & processing units are operated at the same time. Adding to this, storage & processing units are not the same as a virtual machine instances. A single storage & processing unit may host several virtual machine instances. A storage & processing unit is also not equivalent to a single cloud service and may as well integrate multiple public or non-public cloud services. Eventually, this level of complexity might result in users losing track of where (i.e., in which storage & processing unit) required data is stored and how it can be accessed. In order to counteract this potential obstacle of growing complexity, we added a privacy supervisor component and an application provisioning panel component to our model. The privacy supervisor component aims to hide privacy management complexity of individual storage & processing units from users and makes sure that good usability levels are maintained. Furthermore, average users of GCS do not possess the necessary technical expertise to setup and operate CC services, which is also highlighted by the fact that members of subproject B perform the majority of computational analyses for the other subprojects. The application provisioning panel provides a central user interface to setup and operate virtual machines making it easier for involved project members to perform their analyses.

Members of the subprojects involved in MILES also stated that they frequently have to share large amounts of (un-)published human genomic data (IP7; IP8) and unpublished animal genomic data (IP9). They were particularly concerned about the duration and costs of exchanging large amounts of genomic data between involved subprojects. We, therefore, included a data transfer optimization manager that keeps track of data accesses and reorganizes data such that access times and costs are reduced. However, in some cases it might not be permitted to exchange private genomic data even between involved subprojects for reasons of information privacy. Hence, each access to storage & processing units is routed through the privacy supervisor.
Finally, it must be noted that the local university data centre is responsible for providing each subproject with required cloud services (public or private). We assume that it is the norm for most research projects to be supported by some sort of IT department and therefore we also added an administration panel in our model.

5 Conclusion and Next Steps

Information security and privacy of GCS are a current concern in research and practice (DNAnexus Inc., 2014, Dove et al., 2015, Heath et al., 2014). Aiming to provide ‘ideal’ information security and privacy, existing GCS are often designed with maximum information security and privacy in mind, neglecting the existence of diverse information security and privacy requirements for genomic data and sacrificing usability and performance for seemingly secure design. Based on extant research and our experiences in a multi-disciplinary cancer genomics research project, we identified various information practices that exhibit a wide range of diverse information security and privacy requirements. We thus argue that a one-size-fits-all approach to information security and privacy for GCS is not expedient. Contrarily, extant research shows that application of too tight or unfitting information security and privacy measures decreases an IS’ overall usability and causes users to circumvent those measures (Adams and Sasse, 1999, Lampson, 2009), effectively achieving the opposite effect and rendering the concerned IS insecure (Balfanz et al., 2004). Too tight protective measures also impede computational performance, which is a central goal of using CC for genomic research (Stein, 2010). Hence, we propose an architectural model in form of a system components model for GCS capable to dynamically adapt to the diverse information security and privacy requirements associated with information practices employed in cancer genomics research.

Clearly, a limitation of our study is that our architectural model has not yet been instantiated in form of an actual CC platform. It will have to prove its utility and effectiveness in real-world scenarios. In future research, we will implement instantiations of our model in the form of an actual GCS and put it into active use by members of the MILES research project. Hence, the model will be subject to in-depth, authentic evaluation. Another limitation concerns the narrow scope of our conducted focus groups, which are solely based on researchers from one particular cancer genomics research project. Although we are confident that our model is applicable to a wide range of genomic research undertakings due to the fact that MILES incorporates different cancer genomics subprojects, other research projects in the field of genomics might exhibit additional, unaccounted for information practices that might necessitate changes to the proposed model. Future research should therefore investigate information practices in genomic research from additional points of view.

Our research contributes to the scientific knowledge base by developing an architectural model for GCS with dynamic information security and privacy. The proposed model facilitates the development of secure, privacy-preserving and usable GCS, thus supporting the advancement of genomic analyses and personalized medicine (Fernald et al., 2011). While maximizing protection of information security and privacy is desirable in theory, it imposes undesirable consequences in practice, like performance degradations or impediments of researchers’ abilities to develop new therapies for diseases (Dove et al., 2015). Our work demonstrates that implementation of information security and privacy measures cannot be considered a goal in itself. Information security and privacy measures must be adapted to the information sensitivity of involved information so that unnecessary impediments of usability and computational power are avoided.
References


