Can Transparency Enhancing Tools support patient's accessing Electronic Health Records?

Ana Ferreira[1,2] and Gabriele Lenzini[2⋆]

[1] Institute of Cognitive Science and Assessment - Univ. of Luxembourg
[2] Interdisciplinary Centre for Security Reliability and Trust - Univ. of Luxembourg

Abstract. Patients that access their health records take more care of their health and, when in therapy, commit more seriously to improve their condition. This leads to a more effective and more efficient healthcare management, and is also in agreement with European directives on data protection. However, accessing medical data can be risky. Security should be assured and it should be evident to the patients, who has access to what data and any violation to patient's privacy requirements should be reported. We call this property *transparency*.
Precisely this work looks into the Transparency Enhancing Tools that have been proposed to increase people's awareness about security and privacy on the Internet, and discusses to which extent these tools can empower transparency in healthcare.

Keywords: transparency enhancing tools; electronic health records; security and privacy;

1 Introduction

European directives state how personal medical information should be managed and protected: patients must have access and control over their information, be informed about its content and purpose and give consent about its use and distribution [1]. Medical information is however peculiar. It should be owned by patients but is generated and managed by healthcare institutions and professionals who keep it in custody for, and often from, the patients. Especially in relation with Electronic Health Records (EHR), digital databases that contain the historical of patient's medical data, this situation creates conflicts. Granting patient's access to EHR is technically possible and this on the one hand seems to embrace patients' right to have control over personal data but, on the other hand, it may threaten data security and violate people's right to privacy [2, 3].

So, why granting patient's access to EHR? The answer lies in studies that show that patients who are let to consult their medical data commit more faithfully to therapies, care more about their health, and communicate better with

⋆ This research is supported by FNR Luxembourg, CORE project "Socio-Technical Analysis of Security and Trust", C11/IS/1183245 STAST supported by FNR Luxembourg, project I2R-APS-PFN-11STAS.

healthcare professionals [4–8]. Besides, the involvement of patients is a major element for the success of long-lasting medical monitoring programs that require patients with an history of the disease to share their health data over long periods of time. Here, patient's involvement not only should be supported but must be encouraged too.

One way to support patient's involvement and to meet legislation and regulations enforced on personal medical data, is to embrace *transparency*. Transparency suggests to be readable and intelligible to patients whether, whoever manages their medical data, protects their right for privacy, and how. As well, ensuring transparency should imply revealing and informing when a violation has happened and give the means to account violators. Transparency can be a way, we believe, to gain trust and foster patients to collaborate in medical programs.

But how to ensure transparency is unclear. Incipient research in healthcare does not provide effective solutions (see Section 4). Proposals believed to guarantee a degree of transparency do exist but in other domains than healthcare. *Transparency Enhancing Tools* (TETs), for instance, are meant to inform users about how their data are collected, stored, processed and disclosed by Internet service providers [9]. These are the tools that we intend to trail out in the medical domain. But since TET's have been proposed in completely different domains and come in a diversity of options, before migrating them to the medical area, we need to carefully assess their usefulness.

This paper studies TETs and analyses if their features can provide transparency for security and privacy requirements for tools that let patient's accessing their EHR.

2 Transparency for Security and Privacy

What does transparency mean in relation to security and privacy? The first impression is that transparency conflicts with both. How can the access to a resource be secured or private, and transparent at the same time? This apparent conundrum dissolves once one clarifies that transparency does not refer to the same objects as security and privacy do. Security and privacy are properties about the data. Transparency is a property about other properties: it empowers other properties by making evident to a human user their holding. A transparent security is a security that holds evidently, in contrast to an obscure security that holds stealthily. A transparent privacy has a similar meaning.

In particular, to secure the access to information means providing access to authorised users as well as protecting access from unauthorised users. This is usually obtained with *access control* [10]. Access control is not designed to be transparent, since such tools have not been designed to address regulation requirements stating that users must be informed. To become transparent, access control should be "visualized" in how it works to protect accesses to resources. This can be obtained by showing to the data owner, when and who has accessed

his/her data, what application created them, where data are stored and whether accesses comply with the access control policies he/she has defined.

To ensure data *privacy* generally means to anonymize and obfuscate the data so that certain sensitive pieces of information, such as identities, are not easily revealed. For instance, medical data can have any link with patients' identification removed before being available for research. Privacy is usually obtained by applying Privacy Enhancing Technologies (PETs) [11–14]. PETs alone do not ensure transparency, again because they are not designed to address regulation requirements stating that users must be informed. To make PETs transparent, data owners should be informed that their records have been handled accordingly to declared policies and data protection laws. Notably, such practice has been proved to lead to higher perceived trustworthiness [15].

Transparency empowers security and privacy, and it can be employed to make them verifiable, auditable and accountable [16]. Finally, we believe, transparency must give assurance that the data reported to users are accurately presented and faithfully coming from official sources. This means making *integrity* and *authenticity* transparent. The relation between transparency and these two last security properties deserves a research question in itself. It is beyond the scope of this paper's research and it is left for future work.

3 Transparency Enhancing Tools

Transparency Enhancing Tools (TETs) have been proposed in the literature to provide an accurate and comprehensible insight on how Internet providers collect, store, process and disclose user's private data. TETs attempt to provide a better understanding of privacy policies and an insight on third party's tracking behaviour. In so doing, TETs aim to promote security awareness [9].

From research on currently available TETs it is agreed that there are some known desirable characteristics that they should offer. TETs should keep logs of what happens and inform a user when his/her security preferences are matched or when these are compromised. TETs should also offer functions that help a user to exert control over the personal data he/she has released [17] and should, in short, be proxies acting on the user's behalf and inform him/her when and how personal data are harvested, stored, and processed [9, 18]. For all this, the need for TETs has been repeatedly recognized [9].

Moreover, TETs must be autonomous in interpreting user's policies, reveal any violation of these policies, and they should advise the user on how to proceed or who to contact when a policy violation occurs [11].
TETs have also been proposed as tools for auditing [18]. Visual tools for auditing are expected to be transparent in themselves (i.e., to produce their own logs and audit trails), so to prove how they have been used and on what data their decisions have been based upon. The auto-transparency, a property that would be desirable in general, is however meant to be read and understood only by professionals, and it is currently unavailable to lay users.

4 Transparency for Security and Privacy in Healthcare

Transparency is believed to be a precondition for service improvement, data quality and productivity and a powerful driver for auditing and accountability: in healthcare, transparency has been suggested to empower patients and caregivers [19]. Excepting this, there is not much research on how transparency can be applied in the healthcare practice. We have not found research about transparency to empower patient's accessing their EHR, except some discussion about access control and usability requirements, which may be indirectly related to transparency issues [20]. Visualizing access control has been suggested as a mean to let a patient have an understandable overview of the EHR's network, with an inter-connected view showing which different medical departments share which sub-records of a patient's EHR. In this integrated view, a patient can select a part of his/her EHR and view in more detail who is accessing it and for what purpose. An example of such a tool was proposed in [20] and its security and privacy requirements have already been studied on previous research [21] [22]. Even less seems to exist about transparency and privacy in EHR.

In this still unexplored research, studies done in other domains can help to foresee what transparency can do for healthcare. For instance, it has been shown that personal data can be logged without compromising the privacy, and that users can verify what actions were performed on their private data and if these actions comply with a chosen privacy policy [23]. This is surely an interesting property but must be make usable before being handed-down to patients. Inspiring is the state of the art on TETs, the transparency enhancing tools introduced in Section 3. Each TET is meant to empower specific security and privacy aspects. We can thus compile a list of common security and privacy requirements for healthcare (in particular for EHR, see Section 5) and compare and discuss whether the TETs selected for analysis (Figure 1 in Section 6) can empower those requirements. This is exactly the methodology we follow in this paper.

5 Security and Privacy Requirements in Healthcare

This section presents EHR's security and privacy requirements (focusing on access control and privacy) that need to be transparent to the patient when s/he accesses the EHR.

Access Control

RBAC: Role Based Access Control has been proposed in the ISO standard for EHR communications' security [24] and in the HL7 RBAC from the Healthcare Permission Catalog [25]. The ISO standard includes a description of healthcare roles, including the patient as *subject of care*, and defines a structure to organize the content of the medical record. Further, it includes sensitivity levels to express security levels for different types of data, and which roles can access those.

BTG: Break-the-glass has been proposed as part of access control in healthcare and gives the possibility to override (temporarily or as specified) the access control policy in a controlled manner, for instance, in emergency or unanticipated situations [26];

PURUSE: Purpose of use has been suggested by the HL7 Security Technical Committee [25] to associate the context with the access control rules. Examples of purpose of use that can be associated to specific accesses can be: emergency accesses, asking for a second opinion and research usage;

EXCEP: Exceptions were proposed by research focusing on devising a patient's access control model [22] and their aim is, for instance, to give more or less permissions to a specific user than his/her role normally detains. Private notes are an example, i.e., healthcare professionals can be allowed to have private compositions relating to a patient's EHR therefore only accessed by the professional who created them and not by all the users that may detain the same role as that professional;

TEMPCON: Temporal constraints were also proposed by [22]. These are needed to add a limited timeframe to access control permissions. TEMPCON can be specially useful for healthcare professionals that work on shifts. These constraints are also necessary in order to create temporary roles, which are defined for a specific limited time (e.g., delegation or BTG);

DELEG: Delegation is also part of the model proposed in [22] and it allows granting temporary access permissions to healthcare professionals who normally do not treat the patient (i.e., asking for a second opinion).

OBLS: Obligations in healthcare were proposed in [26]. These are secondary actions triggered by primary actions. In access control, obligations can be performed on a GRANT or DENY of an access request, for example, when a BTG is requested, an obligation can be triggered to send an email to the responsible authority to check whether that BTG access was valid or not;

AUTH: European Directives [1] state that there needs to be a description of how personal data must be collected and processed. Regarding access control, this data can refer to patient's identification and authentication information (e.g., including patient's credentials for authentication and authorisation);

SECAUTH: Secure authentication mechanisms with unique identification cards and one time passwords as well as secure authentication and authorization features are proposed in [21];

Privacy

ANONYM: The European Recommendation on the Protection of Medical Data [27] states that patient's data identification has to be anonymised for specific purposes, for instance, for research or educational purposes.

6 Comparing Security Requirements with TET's features

We have studied twenty TETs. Figure 1 summarizes our work. In the first column we name the TET together with a reference and/or the url(s) where to find the

TET's description or its specification. In the second column we give an acronym to the TET, which will be used later to identify each TET. In the third and last column we briefly describe the feature of the TET relevant to this paper's work.

The considered TETs have been presented in very disparate domains. To compare them, we highlight in each TET what features it has that, somehow, adds transparency to security and privacy. We end up having eight categories, numbered from 1 to 8. Each category represents a feature to show, represent or visualize specific elements that we have judged relevant in respect to security and privacy. Namely:

1 - what roles access what owner's data
2 - how data about credentials are used and processed
3 - what data are shared among 3rd party institutions and professionals that can give away information about who uses that data, with some implicit information about their purpose of use
4 - how data about credentials are collected by 3rd parties
5 - how authentication credentials are securely stored
6 - if log entries are encrypted so personal data can be anonymised
7 - how data about authentication credentials are stored and collected
8 - what documents with authentication credentials are disclosed and to whom.

Figure 2 shows the results of matching TETs with the security and privacy requirements listed in Section 5. TETs (listed in the first column) are compared with the requirements (listed in the first row). If a TET, say in row r, has a feature falling into categories from 1 to 8, say i, that we judge able to add transparency to a security and privacy requirement, say in column c, we write the number i in the cell standing at the intersection between r and c.

For example, in reference to Figure 2, and for *Mozilla Privacy Icons* (MPI), we find a 1 under the RBAC and BTG (among other) columns. In fact, MPI engine detects what a website does with a user's personal data. For instance it detects whether the site gives (or never gives) data to advertisers, or whether it may sell (never sell) one's personal data, or whether the site may give (gives) data to law enforcement only when a legal process is followed. All such situations are represented with icons. The same mechanism, we judge, can be as well employed to visualize what roles access what owner's data (i.e., category 1). So it can make visually explicit RBAC policies as well as exceptions or BTG accesses to patient's data.

In summary, Figure 2 shows that nine of the twenty analyzed TETs have at least one feature that helps make transparent one access control or one privacy requirement. Surprisingly, more than half (eleven in twenty) of the analysed TETs did not fulfill any of the security and privacy requirements that we have identified. These TETs are simply add-on applications that add visualization effects to PETs, or enhance them with educational and awareness capabilities (more discussion on these results in Section 7).

Among the nine TETs that instead have relevant features for our study, seven provide transparency mostly for access control requirements. They relate

TET	Acronym	Succinct description
Mozilla Privacy Icons [9] https://wiki.mozilla.org/Privacy_Icons https://disconnect.me/icons	MPI	Privacy icons help users to understand privacy policies indicating how their personal data will be transacted. Privacy policies are described with 4 icons: 1) expected use; 2) expected collection, 3) requests for data and 4) data retention.
Privacy Bird [9][17]	PB	Automatically searches for privacy policies for each website that is visited by the user, it then matches users' previously defined preferences with the policies of the website. A bird with a colour is shown to describe the matching degree.
Privacy Evidence [17]	PE	Secure logging facility and automated privacy audit component to give the user information on how well a system fulfils the promised or user provided privacy policy.
Privacy Score [9]	PS	A privacy score is computed with nine factors: 4 about the site's privacy policy and how they claim to handle personal data; and 5 about privacy qualifications of the companies collecting data on the website. It is an add-on for Firefox and Chrome.
Primelife Privacy Dashboard [9] http://code.w3.org/privacy-dashboard	PPD	Provides the user with a history function describing documents disclosed, to whom and under which conditions, with functions for accessing personal data through online remote services.
Google Dashboard [9]	GD	This website allows google users to see some of the personal data that google stores.
Collusion (now lightbeam) [9] https://www.mozilla.org/en-US/lightbeam/	COL	An add-on for Firefox, Chrome and Safari which provides real-time, interactive visualization of third parties who track user's movements across the web.
Netograph [9] http://netograph.com/	NET	An add-on for Firefox and Chrome which provides the user with a quick view of what a website on social web does before the user visits it.
Web of Trust [9] https://www.mywot.com/	WOT	An add-on for all browsers which provides reputation icons showing how much other users trust a website.
Me and My Shadow [9] https://myshadow.org/	MMS	This tool raises awareness and education about what happens to users' data and traceability on the Internet. It informs the user about existing privacy tools and digital shadow and gives tips.
Priveazy [9]	PRV	It provides education on privacy related issues and helps the user to decide how much protection s/he wants.
Firesheep [9]	FS	An add-on that allows the user to retrieve cookies from people who have logged via insecure wireless networks. Provides transparency on user's own activities and demonstrates how easy user's login information can be stolen.
Panoptic lick [9]	PA	This tool tests user's browser to identify how unique the browser is, and therefore, easier to track.
Creepy [9]	CRP	This tool allows the user to collect geolocation information about users from social networking and image hosting services. Makes the user aware of the geolocation information that s/he sends when sharing on social networks and image applications.
Privacy Bucket [9]	PBK	Chrome extension that measures the extent to which third parties can discover demographic data about the user, based on user's browsing history.
Distributed Privacy Preserving Transparency Logging [22]	DPP	A cryptographic scheme that enables data processors to inform users about the actual data processing that takes place on their personal data.
Transparent Accountable Data Mining [17]	TA	This tool allows users to run compliance checks of data usage policies on the transaction logs of web-based data flow among distributed data custodians, and generates user friendly justification for the results of compliance checks.
Amazon Book Recommendation System [17]	AMA	This service recommends different books to the user based on user's previous purchases. By clicking a link in the recommendation a window will appear which tells the user which of the previous purchases were used to generate the recommendation. The user can then choose whether s/he wants to remove any of the input purchases from the profile so that it is not used as a base for recommendations any more.
Provenance Tracker Network [14]	PTN	This is a decentralized network of peer servers that maintain the usage logs. No single entity can exercise ownership over the entire collection of log records. Usage logs are encrypted such that only the owner or the data subject of the sensitive data item included in the log record will be able to access it.
FPDetective https://github.com/	FP	Framework for the detection and analysis of web-based fingerprints, instead of relying on information about known fingerprints or third-party-tracking blacklist.

Fig. 1. Succinct description of the TETs analysed in this paper.

with showing how personal data are used, processed and collected both by the application at hand as well as by third parties (i.e., categories 1 to 4, 7 and 8). This includes the collection and processing of authentication credentials (e.g., user identification and passwords). Only two among these nine TETs fulfill the privacy requirement *ANONYM*. They do so because they provide a way to detect and flag whether encryption is used on logs (i.e., category 6).

7 Discussion and Conclusion

We believe that TETs features can be a starting point to provide patients with information regarding how their personal data are being used, who has accessed them, for what purpose, when and where data are stored. This visual information can be extended to the parts of a patient's EHR that are being shared among third parties and, hopefully, also for what purpose. This information can be presented to the user depending on specific needs, roles, contextual information and other variables. Almost half of the analyzed TETs can be useful in this situation as they can provide for transparency in such different ways (i.e., with images, icons, text, visual interactive interfaces). However, further analysis is required to decide which of these features better adapt to the patient's centered tool, not only in terms of usability as described, but also in terms of security goals. A patient's access control model may require more fine-grained access control and versatile accesses (e.g., access by a patient's guardian or by family members) and this may necessitate the integration of different features, such as those required to distinguish roles and identities. For this purpose, we need to look more carefully and in deep detail in the TETs' features and techniques available, in future research.

In this paper we considered only one privacy requirement which, in more precise terms, relates to anonymization. Only two TETs provide features that can be applied to add transparency, in order to show that data are anonymized. Again, the TETs in question have ways to flag that encryption is used on data. This can be a first step to protect patients' identity as well as more sensitive information, but anonymization cannot simply be achieved by encrypting data. Other solutions for transparency beyond flagging that encryption is used are thus required to detect and report that anonymization is guaranteed. It seems that we may have to look into research outside TETs for this purpose.

Other Considerations. Our analysis of TETs revealed features, not shown in Figure 2 and not directly related with transparency, which we believe deserve to be mentioned and discussed.

(a) Current TETs are mostly about improving PETs by adding "easier to understand" visual features into the way information regarding privacy policies is presented, so to improve usability features: we have seen that TETs can provide transparency for most of our proposed access control requirements but, during our analysis, we could not find details on what techniques and mechanisms are

			Security and privacy requirements for healthcare									
			Access control									Privacy
			RBAC	BTG	PURUSE	EXCEP	TEMPCON	DELEG	OBLS	AUTH	SECAUTH	ANONYM
Transparency Enhancing Tools	MPI	shows expected use of personal data	1	1		1	1	1	1	2	2	
		shows expected collection of pers. data by 3rd parties	3		3			3		4	4	
	PB											
	PE	the owner can inspect his/her own logs	1	1		1	1	1	1			
		all logs are encrypted									5	6
	PS	shows how personal data is collected								7	7	
	PPD	what docs with personal data are disclosed & to whom	1	1		1	1	1	1	8	8	
	GD	shows how some of the personal data is stored								7	7	
	COL	shows how 1st & 3rd party sites user interacts with	1	1		1	1	3	1			
	NET											
	WOT											
	MMS											
	PRV											
	FS											
	PA											
	CRP	shows geolocation information about users						3				
	PBK											
	DPP	shows how personal data is processed								2	2	
	TA											
	AMA											
	PTN	maintains usage logs	1	1		1	1	1	1	2	2	
		all usage logs are encrypted									5	6
	FP											

1 – what roles access what owner's data; **2** – how data about credentials is used/processed; **3** – what data that are shared among 3rd party institutions or professionals that can give away some information about who uses that data, and some implicit information about their purpose of use; **4** – how data about credentials is collected by 3rd parties; **5** – how authentication credentials are securely stored; **6** – all log entries are encrypted so personal data can be anonymized; **7** – how data about authentication credentials is stored and collected; **8** – what documents with authentication credentials are disclosed and to whom.

Fig. 2. Comparison between patient's security and privacy requirements and TET's.

used to, for instance, detect, collect and process user's private data in relation to Internet browsing. Some TETs features can provide (simple) visual means to display information usage and checking of what private data users and third-parties can access and for what purpose. These visual means are a key factor to provide transparency for patient's access control. It must be possible for lay and non-lay users to easily see and understand whatever is in compliance with their privacy policies but also what has been breached.

(b) Current TETs are mostly introduced to provide awareness and education to the user: in fact, the majority of users do not regularly read privacy policies, and even when they do, these are very hard to understand and do not usually support user's decisions on what to do on a website [28]. Nevertheless, other research shows that people appreciate that a website is concerned about their privacy. People buy more often and more expensive goods from web sites that publicly declare that they care about protecting the privacy of their customers (e.g., see [29]). Besides, it has been proved that usable privacy policies foment trust [30]. Therefore, usability is a fundamental requirement that must be considered in addition to security and privacy. Unfortunately, there was not much data available concerning usability experiments and results for the TETs analysed in this paper.

(c) Current TETs mostly analyse user's behaviour on the Internet to profiling their needs in terms of privacy: the information of insecure behaviour derived from this profiling can help the user to be more careful of their privacy when using the Internet. Profiling techniques can be used as well in a patient's access control tool, raising alarms to patients when an access violation occurs, so making them more attentive for signs and specific issues that would be normally ignored.

Limitations. The TETs reviewed in this paper have been described in other reviews [9, 18] or in proprietary websites that give insight about TETs features. We did not use, test and analyze the TETs ourselves. This is left for future work. Also, we did not discuss usability of the considered TETs. But usability is a key feature, since a TET may fail to communicate its message clearly. How to measure this gap between intention to communicate a message and success in communicating that same message is intensively debated in usable security. We have considered usability requirements out of scope in this paper's analysis.

Conclusion. We looked into Transparency Enhancing Tools (TETs), and discussed whether such technology can provide for transparency of security and privacy policies in healthcare. We question whether TETs can help foster patient's trust on how their personal and medical data are handled. TETs have promising features, and our analysis reveals that they are a valid starting point for our research. But further research is needed: there is the need for user studies to make sure that TETs work in practice and, more importantly, in the healthcare practice where user interactions with technology are very diversified and therefore very challenging.

References

1. E. P. E. Commission, "EU Directive 95/46/EC - The Data Protection Directive - IP/12/46 - 25/01/2012," October 2005 and 2012.
2. K. D. Mandl, D. Markwell, R. MacDonald, P. Szolovits, and I. S. Kohane, "Public standards and patients' control: how to keep electronic medical records accessible but private." *BMJ*, vol. 322, no. 7281, pp. 283–287, 2 2001.
3. A. Bakker, "Access to ehr and access control at a moment in the past: a discussion of the need and an exploration of the consequences," *International Journal of Medical Informatics*, vol. 73, no. 3, pp. 267 – 270, 2004.
4. A. Ferreira, A. Correia, A. Silva, A. Corte, A. Pinto, A. Saavedra, A. L. Pereira, A. F. Pereira, R. Cruz-Correia, and L. F. Antunes., "Why facilitate patient access to medical records." *Stud Health Technol Inform.*, vol. 127, pp. 77–90, 2007.
5. R. P. Burke, A. F. Rossi, B. R. Wilner, R. L. Hannan, J. A. Zabinsky, and J. A. Jeffrey, "Transforming patient and family access to medical information: utilisation patterns of a patient-accessible electronic health record," *Cardiology in the Young*, vol. 20, pp. 477–484, 10 2010.
6. C. Bartlett, K. Simpson, and A. N. Turner, "Patient access to complex chronic disease records on the internet," *BMC Medical Informatics and Decision Making*, vol. 12, no. 1, pp. 1–7, 2012.
7. R. Vaart, H. C. Drossaert, E. Taal, and A. Laar, "Giving rheumatology patients online home access to their electronic medical record (emr): advantages, drawbacks and preconditions according to care providers," *Rheumatology International*, vol. 33, no. 9, pp. 2405–2410, 2013.
8. K. Pareshi, P. Wood, and M. Martin, "A pilot study on the views of elderly regional australians of personally controlled electronic health records," *International Journal of Medical Informatics*, vol. 83, no. 3, pp. 201 – 209, 2014.
9. M. Janic, J. Wijbenga, and T. Veugen, "Transparency enhancing tools (tets): An overview," in *Socio-Technical Aspects in Security and Trust (STAST), 2013 Third Workshop on*, June 2013, pp. 18–25.
10. S. Harris, *Cissp All-In-One Exam Guide*. McGraw-Hill Osborne Media; 4 ed., 2007.
11. G. van Blarkom RE drs. J.J. Borking dr.ir. J.G.E. Olk, Ed., *Handbook of Privacy and Privacy-Enhancing Technologies: The Case of Intelligent Software Agents*. College bescherming persoonsgegevens, 2003.
12. C. Ardagna, M. Cremonini, E. Damiani, S. De Capitani di Vimercati, and P. Samarati, "Privacy-enhanced location services information," in *Digital Privacy: Theory, Technologies and Practices*, Acquisti, De Capitani di Vimercati, Gritzalis, and Lambrinoudakis, Eds. Auerbach Publications (Taylor and Francis Group), 2007, pp. 307–326.
13. Z. Erkin, T. Veugen, T. Toft, and R. Lagendijk, "Generating private recommendations efficiently using homomorphic encryption and data packing," *Information Forensics and Security, IEEE Transactions on*, vol. 7, no. 3, pp. 1053–1066, 2012.
14. O. Seneviratne and L. Kagal, "Enabling privacy through transparency," in *2014 Twelfth Annual International Conference on Privacy, Security and Trust, Toronto, ON, Canada, July 23-24, 2014*, 2014, pp. 121–128.
15. T. Lauer and X. Deng, "Building online trust through privacy practices," *International Journal of Information Security*, vol. 6, no. 5, pp. 323–331, 2007.
16. S. Sackmann, J. Strüker, and R. Accorsi, "Personalization in privacy-aware highly dynamic systems," *Commun. ACM*, vol. 49, no. 9, pp. 32–38, Sep. 2006.

17. M. Hansen, S. Fischer-hbner, J. S. Pettersson, and M. Bergmann, "Transparency tools for user-controlled identity management."
18. H. Hedbom, "A survey on transparency tools for enhancing privacy," in *The Future of Identity in the Information Society*. Springer Berlin Heidelberg, 2009, vol. 298, pp. 67–82.
19. H. International., "Transparency - the most powerful driver of health care improvement?" McKinseys Health Systems and Services Practice, 2011.
20. A. Ferreira, G. Lenzini, C. Santos-Pereira, A. B. Augusto, and M. E. Correia, "Envisioning secure and usable access control for patients," in *IEEE 3rd International Conference on Serious Games and Applications for Health*, 2014.
21. A. B. Augusto and M. E. Correia, "OFELIA - A Secure Mobile Attribute Aggregation Infrastructure for User-Centric Identity Management," in *Information Security and Privacy Research*, ser. IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg, 2012, vol. 376, pp. 61–74.
22. C. Santos-Pereira, A. B. Augusto, M. E. Correia, A. Ferreira, and R. Cruz-Correia, "A mobile based authorization mechanism for patient managed role based access control," in *Information Technology in Bio- and Medical Informatics*, ser. Lecture Notes in Computer Science, C. Bahm, S. Khuri, L. Lhotska, and M. Renda, Eds. Springer Berlin Heidelberg, 2012, vol. 7451, pp. 54–68.
23. R. Peeters, T. Pulls, and K. Wouters, "Enhancing transparency with distributed privacy-preserving logging," in *ISSE 2013 Securing Electronic Business Processes*, H. Reimer, N. Pohlmann, and W. Schneider, Eds. Springer Fachmedien Wiesbaden, 2013, pp. 61–71.
24. ISO/TS, "ISO/TS 13606-4 - Health informatics - electronic health record communication - Part 4: Security." 2009.
25. H. S. T. Committee, *HL7 Role-Based Access Control (RBAC): Healthcare Permission Catalog*, HL7 Security Technical Committee Std., 2010.
26. A. Ferreira, D. Chadwick, P. Farinha, R. Correia, G. Zao, R. Chilro, and L. Antunes, "How to securely break into rbac: The btg-rbac model," in *Proceedings of the 2009 Annual Computer Security Applications Conference*, ser. ACSAC '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 23–31.
27. C. of Europe, "Recommendation No. R (97) 5 of the Committee of Ministers to Member States on the Protection of Medical Data," 1997.
28. M. A. and C. L., "The cost of reading privacy policies." *Journal of Law and Policy for the Information Society*, 2009.
29. J. Y. Tsai, S. Egelman, L. Cranor, and A. Acquisti, "The effect of online privacy information on purchasing behavior: An experimental study," *Info. Sys. Research*, vol. 22, no. 2, pp. 254–268, Jun. 2011.
30. W. Pieters, "Explanation and trust: what to tell the user in security and ai?" *Ethics and Information Technology*, vol. 13, no. 1, pp. 53–64, 2011.