DOI 10.1007/s10916-016-0653-8

Transparent Medical Data Systems

Dayana Spagnuelo[1] · Gabriele Lenzini[1]

Received: 7 June 2016 / Accepted: 28 October 2016 / Published online: 16 November 2016

Abstract Transparency is described as the quality to be open about policies and practices. It is intended to inform end users of what happens to their data. It promotes good quality of service and is believed to sustain people's demand for privacy. However, at least for medical data systems, a clear definition of the property is missing and there is no agreement on what requirements qualify it. We look into this problem. First we identify concepts that relate with transparency: openness, empowerment, auditability, availability, accountability, verifiability. We discuss them in Health Information Technology, so clarifying what transparency is. Then we elicit a list of requirements that indicate how transparency can be realised in modern medical data systems such as those managing electronic health records.

Keywords Transparency · Taxonomy · Requirements · Medical data systems

Introduction

Transparency is considered a pro-ethical principle that promotes accountability and improves the quality of service. It empowers people's choices and their demands for better services, social innovation, and economic growth [14, 24]. It has been defined as *"the possibility to access information and evidences revealed through a process of disclosure"* [38]. It has been presented as the *"practice to inform users and make policies and processes openly available"* [17] and as the *"predisposition to increase responsibility and accountability"* [9].

Transparency is also a quality that is believed to realise people's right to privacy [33]. For this reason it is a desirable quality to have in Health Information Technology where patient data, such as Electronic Health Records, contain highly sensitive and personal information. Electronic Health Records are expected to be handled properly and several laws that defend people's rights to have security and privacy measures put in place (e.g., the Health Insurance Portability and Accountability Act in US; Directives 95/46/EC, 2011/24/EU, and the new General Data Protection Regulation [6] in EU).

However, beyond the demands of the legal framework and despite the discussions about the benefits of having transparency implemented in Health Information Technology [9, 10, 22, 31, 33], there has been no consensus on the operational meaning of the property nor clear guidelines on how to establish it in medical data systems. This article fills this gap. We discuss transparency and we comment on a few security properties linked to it. We clarify how the properties relate and we present a list of requirements for transparency in the scope of Health Information Technology, keeping a patient-centred perspective.

The article deepens and extends our conference paper "Patient-Centred Transparency Requirements for Medical Data Systems" [35]. We discuss more thoroughly the concept of transparency and we qualify it better in relation to kindred properties such as openness, empowerment,

This article is part of the Topical Collection on *Patient Facing Systems*

✉ Dayana Spagnuelo
dayana.spagnuelo@uni.lu

Gabriele Lenzini
gabriele.lenzini@uni.lu

[1] Interdisciplinary Centre for Security, Reliability and Trust (SnT), University of Luxembourg, Luxembourg, Luxembourg

auditability, availability, accountability, and verifiability. On that light, we review the list of requirements initially presented in [35].

Outline Section "Medical data systems" describes three Electronic Health Records systems: they exemplify how modern medical systems work. Section "On transparency and related work" explores the related work and presents the definition for transparency that will be referred throughout the paper. Section "Related properties" discusses concepts that qualify transparency in medical data systems. They will be referred in our technical requirements. Section "Requirements for transparency" comments the requirements Section "Discussion and conclusion" discusses and concludes the paper's findings.

Medical data systems

It is true that at some extent transparency may be accomplished outside the domain of Technology Information. A conversation between the physician (or some other member of the medical team) and the patient can be sufficiently informative about how personal data are handled. Nevertheless, in this work we assume that there is, or can be, a channel for the patient to access directly a medical system, a possibility that has not been fully explored yet in current medical data systems, still it is foreseen in regulations about data protection like the General Data Protection Regulation [6].

We based our understanding of the information flow in modern medical processes, in reference to three specific systems: i) the *Integrated Telemedicine and Telehealth System* of the state of Santa Catarina, Brazil, a platform that allows accessing medical examinations (e.g., ECGs, ECHOs, MRIs) at distance; ii) the *Visual Electronic Patient Record* of the Hospital São João, Portugal, a centralised data management system that collects clinical reports from the various hospital departments and let them accessible by authorised health professionals; iii) the clinical research data system of the *National Centre of Excellence in Research Parkinson's Disease* (NCER-PD) that the Luxembourg Centre for System Biomedicine has developed to study the development of the disease.

The Brazilian telemedicine system (see Fig. 1) foresees the interaction between the patient and the system. This is limited to access medical examinations with no interaction with the physician although patients have to contact the nurse or technical team that handle the medical equipment in the regional medical facility.

The Portuguese medical information system (see Fig. 2) foresees no interaction between the patients and the system. In a regular scenario, the patient goes to the specialised medical facility and is treated by the physician who accesses the system to retrieve the patient's health history.

Finally, the Luxembourgish clinical data research system (see Fig. 3) aims to aid the management of medical information about patients participating on a long-term clinic research. In the current implementation, the patients have no access to the system nor have they contact with the researchers and medical team that handle their data. The patients entrust their data to be used in a clinical research with the goal of studying a specific disease.

A peculiarity of the medical domain is that, unlike other domains, the content produced about patients is actually created not by the patients but by others subjects, generally

Fig. 1 Telemedicine system

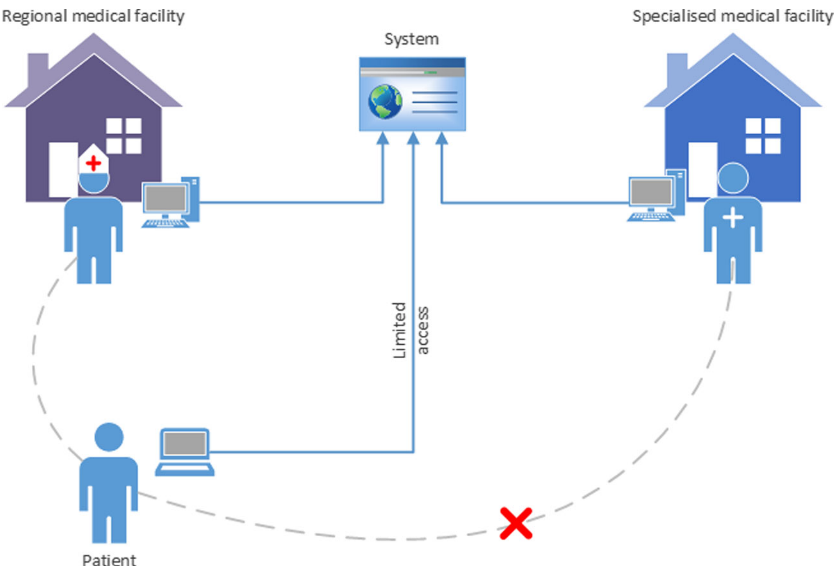
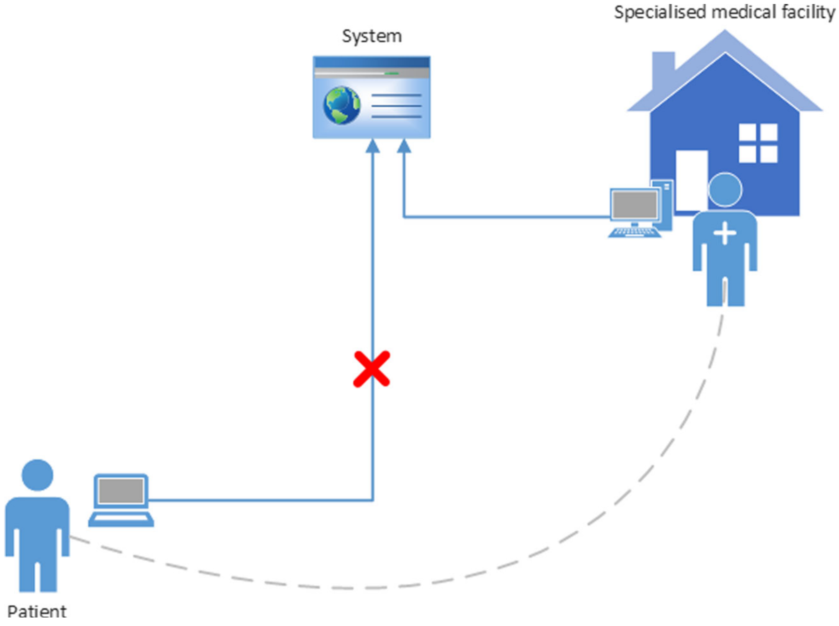


Fig. 2 Hospital information system

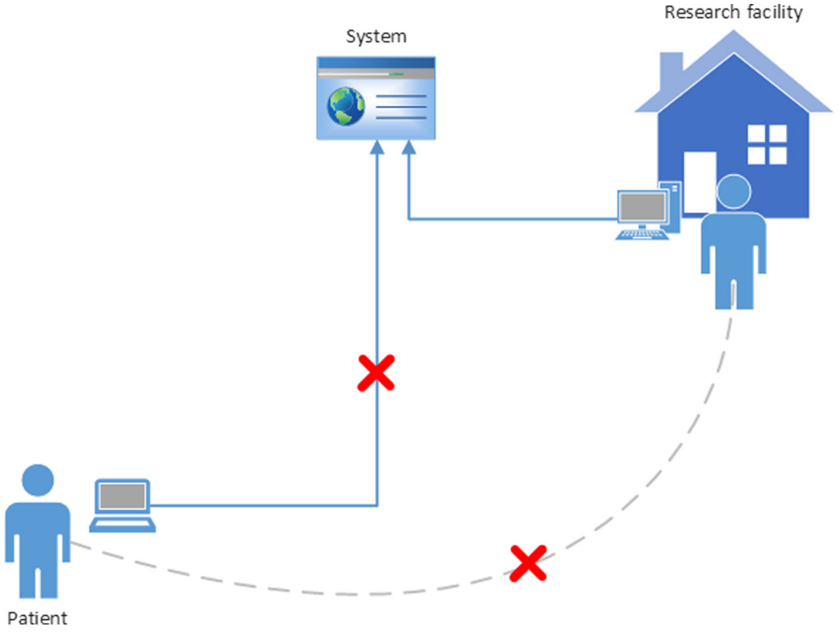


physicians or members of the medical team. Often, data are created, edited, and accessed without the knowledge or the consent from the patients. Such peculiarities happen in all the three presented scenarios. As a consequence, the process of disclosure of data is not as evident as in other domains. For example, in on-line banking users are informed, when first they are about to disclose their data to the system, how the system will handled the current and future data. But regardless how patient's personal data reach the system, regulations, like the General Data Protection Regulation, are in place to protect a patient's right to be informed.

On transparency and related work

In Health Information Technology, transparency has been regarded together with openness about policies and processes in [17, 37]. The authors say: "*there should be openness and transparency about policies, procedures, and technologies that directly affect individuals and/or their individually identifiable health information*" and "*clear and accessible policies and procedures help maintain the trust of participants*". Transparency has been considered a predisposition to increase responsibility and therefore presented

Fig. 3 Clinical research system



with *accountability* as "*critical to helping society manage the privacy risks that accumulate from expeditious progress in communication, storage, and search technology*" [9]. Transparency has been also defined as the property *to be informative* towards the patient in [31]. Transparency has also been discussed as *a mean to enhance and promote privacy*: medical data systems provide transparency by allowing users *to audit* the operations run on data considered sensitive [33].

Ray and Wimalasiri defend that transparency in medical systems has two dimensions: *to give access* to Electronic Health Records and *to disclose* how the system works [29]. They present a use case which rates poorly in transparency "due to the *lack of visible privacy policies* and details on the personal information that will be stored". Tang and Lansky have a similar opinion, they mention that an optimal medical systems must be *transparent in terms of information sources and information access* [36].

All the considered papers in medical systems see transparency related to the act of *informing users* and *making policies and processes openly available*. This appears to be the interpretation of "transparency" in the Health Information Technology. However, there is basically no further development and no standard solution that makes a medical system compliant to it.

Instead, transparency has been discussed in cloud computing. Transparency has been inspected with relation to privacy and accountability from the perspective of end-users by Berthold et al. in [3]. Transparency Enhancing Tools (see [7] and [13] for a survey) have been developed *to inform* users about how data are handled. In this sense, transparency intends to *simplify the understanding of privacy policies*, an interpretation that reminds usability; to help *check for possible violations of the privacy policy*, which recall auditability; and to allow the user *to keep track of the personal data and its disclosures*, which we think refers to verifiability. Hansen [12] advocate that users should have "*a way of knowing what personal data is available in the system and who can access it*". According to the author, transparency is about "*letting the users feel in control of the technology*", for example by simplifying the presentation of privacy policies and the explanation of user's privacy rights. This is another proposition that suggest some sort of usability.

Transparency has been also studied as a quality in software engineering for organisations. Leite and Cappelli study transparency from an organisational view and present a graph of qualities (or soft goals) that relate to the notion of transparency [4, 21]. They construct the graph by combining the terms associated with transparency in the literature. By doing that, they find out four main qualities that provide a notion on how transparency would be satisfied in software products: *usability*, *auditability*, *accessibility* and *informativeness*.

There have been also a few attempts to define transparency more rigorously. Two definitions stand out for their clarity. The first, states that transparency is "the state when every party in the target group possesses perfect knowledge, [..] i.e., when no party in the target group could learn any information (in Shannon's sense) about the observable of interest" [3]. This definition defines a measure of transparency in information theoretical sense; however, at least in the domain addressed here where patients are the end users, *perfect* knowledge as referred in [3] is hardly measurable in which it depends on subjective abilities of individuals to acquire knowledge. A second definition separates transparency in two categories: ex ante and ex post transparency. Ex ante transparency, we quote, "*enables the anticipation of consequences before data are actually disclosed*". Ex post transparency, "*offers information about any consequences if data already have been revealed*" (FIDIS deliverable D7.12 [8]).

This definition fits better the concept of transparency that has been advocated for Health Information Technology. It is simple and yet flexible enough to comprise the intuition one has about what transparency should be. We adopt it in this paper with minor modifications:

Definition 1 (**Transparency in ICT healthcare**) *Ex-ante transparency* enables the patient to anticipate what will happen to his/her medical and personal data. *Ex-post transparency* enables the patient to be informed or get informed about what happened to his/her medical and personal data.

Since in medical systems it is not always evident when a piece of information is disclosed —medical data is created and manipulated by the medical team, sometimes without the knowledge of the patient— Definition 1 interprets disclosure as the act of giving in custody or giving access to the data. This happens whenever the data is shared with another doctor or medical institution, for example.

Related properties

The works we cited in Section "Introduction" and in Section "On transparency and related work" present several interpretations of transparency. What emerges is that transparency is accompanied by the following properties: openness, availability, auditability, verifiability, empowerment, usability and privacy. We have emphasised these words or the phrases that refer to these properties, and the reader may want to review the sections at this point.

Although these terms are often invoked to describe transparency, there is no agreement on how they relate with transparency. Is transparency a collective name for them? Or is it a synonymous for some of them? Or is it instead a new property itself that is only qualified better by those concepts?

We answer to these questions by discussing what these properties mean in the domain of Health Information Technology and how they relate with transparency. Despite conceived for Health Information Technology, the correlations between the concepts that we present remain valid even outside this application domain. The resulting taxonomy (see Fig. 4) not only clarifies better what transparency is, but also led us to have a neat list of requirements for transparency in medical data systems (see Section "Requirements for transparency").

Empowerment The "authority or power given to someone to do something" [28]. In medical systems, empowerment has been discussed in terms of giving individuals power to take appropriate action in regard to personal data and privacy issues [12]; giving patients control over their health information [30]; and "[to] allow patients to grant access to specific portions of their health data" [32]. Because empowerment is about giving patients the power to control their data rather than helping them understanding what happened or will happen to their data, it does not define transparency. Instead, it can be seen as complementary to transparency for it gives individuals the right to react to the information provided by a transparent system.

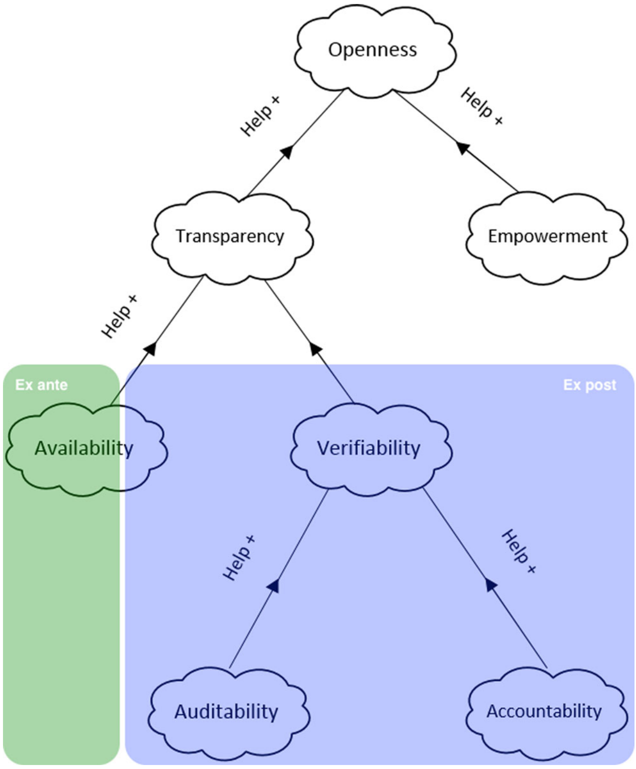


Fig. 4 How other properties that relate with transparency help define ex post or ex ante transparency

Openness "The concept of openness [..] refers to a kind of transparency which is the opposite of secrecy and most often this transparency is seen in terms of access to information especially within organisation, institutions or societies" [27]. The Open Source Initiative (OSI), who educates in methods for software development, reminds that open source is about disclosing source and allowing others to modify and derive other works [26]. By rephrasing the concept in medical data systems, we understand that openness is about allowing patient to know what a process does and how it does it, and giving them the permission to change it. This notion of openness comprises the transparency as we defined it; in addition, calls for empowering a patient, in our case, to modify his/her data. Figure 4 represents openness as the father node of transparency and of empowerment: both children help defining openness.

Accountability, auditability and verifiability Accountability is "the fact or condition of being accountable; responsibility" [28]. In the medical domain it has been defined as "a concept that lets us monitor a person's use of information and hold that person accountable if he or she misuses the data" [9].

Auditability is defined as "an official inspection of an organisation's accounts, typically by an independent body" (derived from the definition of "audit" [28]). But in medical systems it has being regarded as an informal procedure made by the patients to indicate how sensitive data was used [33]. In this sense it can be also interpreted as "the ability to examine carefully for accuracy with the intent of verification" [21]. Auditability and accountability are often associated with the concept of *verifiability*.

Verifiability is "[being] able to be checked or demonstrated to be true, accurate, or justified" (from the definition of "verifiable" in [28]), or "the quality of being tested (verified or falsified) by experiment or observation" [21]. In computer security, verifiability is a property that includes auditability. Universal verifiability, for instance, states that anyone (thus, not only auditors) should be able to verify that the system's run satisfies a given property [18] but, assuming a patient-centred focus where there are no entities but the patient and the system, auditability and verifiability become undistinguishable. We talk in this sense of verifiability/auditability. Figure 4, for sake of generality, pictures verifiability and auditability as distinct nodes helping transparency: they both enable patients be informed about what happened to their records (see the ex post interpretation in Definition 1).

Accountability ensures that who has misbehaved will be identified [19]. Berthold et al. links accountability and transparency by stating that accountability is being transparent about the occurrence of privacy breaches. In Fig. 4, accountability is a brother node of auditability, both are ex post properties, and help specifying verifiability.

Availability Finally, transparency is constantly regarded as being informative towards the patients on the usage and disclosure of their personal and medical data [31], on the policies [12], and procedures [37]. These definitions closely relate to the concept of availability, which can be defined as*"the quality of being able to be used or obtained"* [28] or *"the quality of being at hand when needed"* [21]. In our context, availability helps ex ante transparency as it provides a way for patients to obtain information on the intentions of the systems in regard to their data. It also helps ex post transparency when it makes available information on what happened to the patient's data. Availability thus helps defining transparency.

Usability and privacy There is a huge amount of works about these two properties, so we focus on what is most relevant for the scope of this paper.

The ISO 9241-11 defines usability as "the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use" [16]. Despite desirable for transparency (see Sections "Introduction" and "On transparency and related work"), we think that a system can be transparent even without reaching the quality required by usability. But, usability improves transparency in the sense to help users reaching their goal more effectively, efficiently, satisfactorily. In this understanding, usability appears to be an attribute of transparency. It is not shown in Fig. 4, but we consider usability in our requirements.

A similar argument holds for (information) privacy. Privacy is preserved when sensitive information is not leaked by unauthorised entities. Interpreted as confidentiality, privacy seems to conflict with transparency [27]. Instead, as pointed out in [3], privacy and transparency can be realised without friction. In particular, helping a patient anticipate what will happen or informing him/her about what has happened about his/her data can be done without leaking sensitive information about other patients. In this interpretation, privacy becomes a principle of minimal disclosure applied to transparency; when called for, it improves the quality of transparency. As we did for usability, we do not include privacy in Fig. 4, but define for it subsidiary requirements.

Table 1 summarises and rephrases the properties that help defining transparency which are adapted to the Health Information Technology domain. Figure 4 shows how they relate with transparency. Nodes are properties, and edges are positive relationship between nodes, in which the lower node helps constructing the concept of the higher node. It is important to note that we do not infer how much each

Table 1 Properties that relate with transparency and their definition in relation to Health Information Technology

Property	Definition in Health Information Technology
Accountability	Enables the patient to monitor the use of his/her medical and personal data, and to hold a person accountable in case of its misuse;
Availability	Enables the patient to obtain and use information related to his/her medical and personal data when needed;
Empowerment	To give a patient authority and power to control his/her medical and personal data;
Openness	The absence of secrecy and concealment from patients of any information on policies and practices affecting their Electronic Health Records.
Verifiability / Auditability	Enables the patient to verify what happened to his/her medical and personal data;

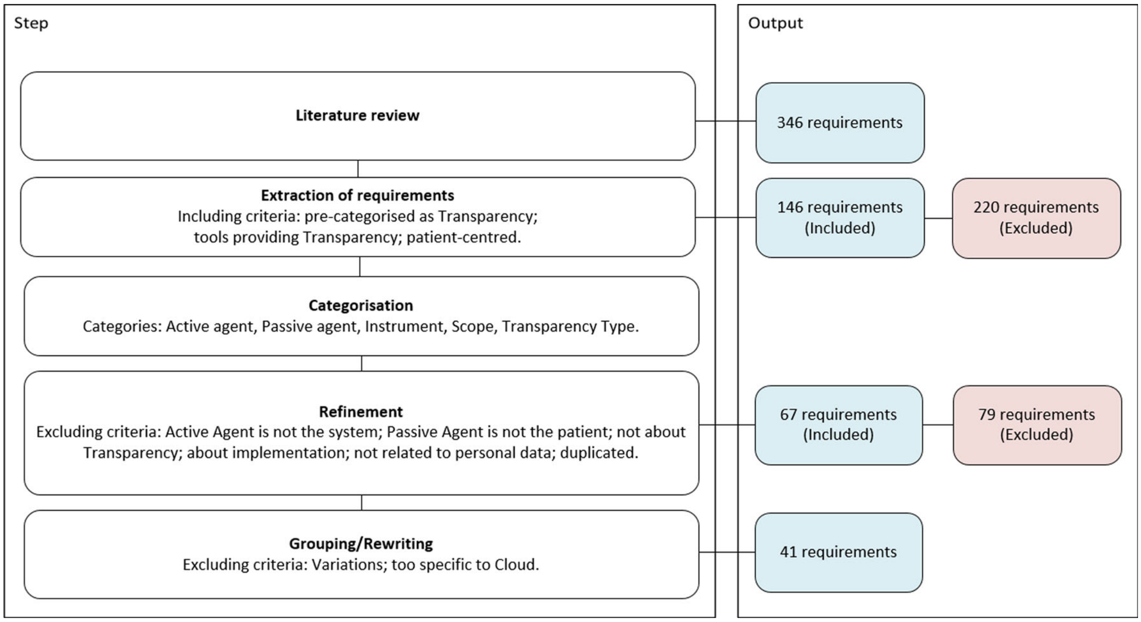

Step
Literature review
Extraction of requirements
Including criteria: pre-categorised as Transparency; tools providing Transparency; patient-centred.
Categorisation
Categories: Active agent, Passive agent, Instrument, Scope, Transparency Type.
Refinement
Excluding criteria: Active Agent is not the system; Passive Agent is not the patient; not about Transparency; about implementation; not related to personal data; duplicated.
Grouping/Rewriting
Excluding criteria: Variations; too specific to Cloud.
Output
346 requirements
146 requirements (Included)
220 requirements (Excluded)
67 requirements (Included)
79 requirements (Excluded)
41 requirements

Fig. 5 Our elicitation process' 5 steps (*left*); No. requirements retained/rejected (*right*)

quality helps, nor if they are enough for constructing the others.

Requirements for transparency

In [35] we give a full report about finding a definition for transparency and proposing a set of requirements that fit the peculiarities of medical systems as those we mentioned in Section "Medical data systems". Such a contribution was missing with regard to the medical domain. What we found about transparency in other domain was completed with what we found about desired functional features for medical systems that, despite not directly related to transparency, we judged contributing to define the notion of a transparent system. Thus, we created a novel list of requirements. In the following we synthetically comment on the steps that we have been following to list a comprehensive set of requirements, but to know all the detail one should refer to [35].

Elicitation process

We proceeded in five steps (see Fig. 5): (1) *literature review*, where we browse the literature in other domains searching for potentially applicable-to-transparency requirements (i.e., [5, 23]), and where we collect papers that discuss technical features in medical systems that directly or indirectly are about transparency (i.e., [1, 2, 11, 15, 30, 33]); (2) *extraction of requirements*, where we define the criteria to select/compose transparency requirements in preparation to have a preliminary list; (3) *categorisation*, where we categorise our preliminary list of requirements according to the actors involved in realising transparency (active agent) or benefiting from transparency (passive agent), to whether they provide information or tools (instrument), to which security properties they concern (scope), and to whether they are ex ante or ex post (transparency type); (4) *refinement*, where we review the requirements questioning their relevance in Health Information Technology; (5) *rewriting*, where we rewrite, restyle, and present our final list of requirements.

List of requirements

Tables 2, 3, 4 and 5 present 41 requirements. While the first three tables present the Transparency requirements separated by qualities (availability, verifiability/auditability, and accountability), the latter one presents Empowerment requirements. These requirements do not help qualifying transparency, but are being presented here because they complement the discussion about transparency and its relation with other properties. In what concerns Definition 1 the requirements presented in Tables 2, 3, 4 together compose ex ante and ex post transparency as depicted in Fig. 4.

As requirement identifier, we gave a numerical code inspired by the Dewey Decimal Classification [25]. It relies on the attributes: *type*, the transparency type; *quality*, the quality of the taxonomy the requirement relates to; and *instrument*, what is being provided to the patient. Table 6 lists the codes of our attributes. Each code is a three digits number in which the hundreds represents the transparency type, the tens represents the quality, and the units represents the instrument. Requirements in the same class are distinguished by adding decimal ciphers to the code.

Table 2 Availability requirements. (*S* = medical system; *P* = patient)

Req.	Specification	Type	Instrument
111.1	*S* must provide *P* with real time information on physical data storage and data storage location of different types of data.	Ex ante	Information
111.2	*S* must inform *P* on how data are stored and who has access to them.	Ex ante	Information
111.3	*S* must inform *P* from whom it purchases services, and about any conflict of interest towards data.	Ex ante	Information
111.4	*S*, in case of using services from third parties, must inform *P* about the existence of sub-providers, where they are located and whether they comply with the legal requirements of the country of *P*.	Ex ante	Information
111.5	*S* must inform *P* how it is assured that data are not accessed without authorisation.	Ex ante	Information
111.6	*S* should make available a document that describes the adopted mechanisms for securing data against data loss as well as data privacy vulnerabilities.	Ex ante	Information
111.7	*S* should make available a document that describes the procedures and mechanisms planned in cases of security breaches on *P*'s data.	Ex ante	Information
111.8	*S* should make available the technical documentation on how data are handled, how they are stored, and what are the procedures for accessing them.	Ex ante	Information
111.9	*P* must be made aware of the consequences of their possible choices in an unbiased manner.	Ex ante	Information
111.10	*S* must inform *P* about who is responsible for handling owned data.	Ex ante	Information
111.11	*S* must inform *P* about storage in other countries and compliance issues related to this storage with respect to laws and regulations of both the other country and their own country.	Ex ante	Information
111.12	*S* should inform *P* about the use of specific security mechanisms.	Ex ante	Information
111.13	*S* must inform *P* on how to protect data or how data are protected.	Ex ante	Information
111.14	In case of using services from third parties, *S* must inform *P* on the responsibilities of the different parties involved in the agreement.	Ex ante	Information
111.15	*S* must inform *P* about who has the authority to investigate any policy compliance.	Ex ante	Information
111.16	*S* must provide *P* with evidence of data collection practices.	Ex ante	Information
111.17	*S* must make available a document explaining the procedures for leaving the service and taking the data out from the service.	Ex ante	Information
111.18	*S* must make available a document that describes the ownership of the data.	Ex ante	Information
111.19	*S* must provide *P* with disclosure of policies, regulations or terms regarding data sharing, processing and the use of data.	Ex ante	Information
111.20	*S* must provide *P* with evidence of separating personal from meta data.	Ex ante	Information
112.1	*S* must provide *P* with mechanisms for accessing personal data.	Ex ante	Mechanisms
211.1	*S*, in case of security breaches, must inform *P* on what happened, why it happened, what the procedures *S* is taking to correct the problem and when services will be resumed as normal.	Ex post	Information
211.2	*S* must inform *P* when the authorities access personal data.	Ex post	Information
211.3	*S* must notify *P* in case the policy is overridden (break the glass).	Ex post	Information
211.4	*S* must provide *P* with timely notification on security breaches.	Ex post	Information
211.5	*S* must inform *P* if and when data is gathered, inferred or aggregated.	Ex post	Information

Availability requirements

Availability requirements, mainly regarded in terms of providing information, serve both transparency types but mostly they contribute to the ex ante notion. We present the availability requirements in Table 2.

Availability contributes to the notion of ex ante transparency because Electronic Health Records are normally created and manipulated by medical teams, and so patients are not automatically aware of what data the system has on them, how data are handled and by whom are accessed. Without this pieces of information patients are not able to anticipate what is going to happen to their data.

Availability in ex post includes requirements (like requirements 211.1-4) that inform patients about events that

Table 3 Verifiability/auditability requirements. (*S* = medical system; *P* = patient)

Req.	Specification	Type	Instrument
221.1	*S* must provide *P* with evidence that policies, regulations and practices have been applied correctly.	Ex post	Information
221.2	*S* must provide *P* with evidence of the recovery from security attacks.	Ex post	Information
221.3	*S* must provide evidence of compliance with respect to extraterritorial legislative regimes.	Ex post	Information
221.4	*S* must provide evidence that the data is being maintained in the correct way.	Ex post	Information
221.5	*S* must provide *P* with evidence regarding permissions history for auditing purposes.	Ex post	Information
221.6	*S* must provide detailed information on the data collected about *P*, and what information *S* has implicitly derived from disclosed data.	Ex post	Information
221.7	*S* must provide *P* with evidence that revoked consent has been executed.	Ex post	Information
221.8	*S* must provide *P* with evidence of security breaches.	Ex post	Information
222.1	*S* must provide *P* with audit mechanisms.	Ex post	Mechanisms

Table 4 Accountability requirements. (*S* = medical system; *P* = patient)

Req.	Specification	Type	Instrument
232.1	*S* must provide *P* with accountability mechanisms.	Ex post	Mechanisms

may endanger their data, like security breaches. The goal of these requirements is to inform the patients so that they are able to understand the impact of the event on their data, but not necessarily to find and blame the responsible for the event.

Verifiability requirements

Verifiability contributes only to the notion of ex post transparency, and is composed by requirements providing information and mechanisms. The first ones allow the patients to check by observation the way in which data have been handled, and whether they have been handled in compliance to policies and regulations. The second ones allow them to check by experimentation what happened to their data. Verifiability requirements are presented in Tables 3 and 4.

Because we define ex post transparency as a way to inform the patients about what happened to their personal data, ex post is mostly composed by verifiability requirements.

Empowerment requirements

Empowerment requirements (see Table 5) should not be confused with ex ante transparency requirements. In a sense, to provide ways for patients to control their personal data also helps them to anticipate what will happen to it. But these requirements bring more than just anticipation. Empowerment requirements directly address the problem of ownership of the data by allowing the patients to react to the information provided by a transparent system, and to control the usage of their data.

Quality requirements

As presented in Section "Related properties", we found in the literature properties that help improving the quality of transparency, those are referred as quality requirements [20]. We list three of such requirements in Table 7.

Usability and privacy emerged while we browsed the literature for definitions of transparency, they were presented and discussed in Section "Related properties". Existence emerged from the requirements elicitation process and is justified by the fact that a system cannot be considered truly transparent if its users are not informed about the transparency functionalities existent.

Table 5 Empowerment requirements. (S = medical system; P = patient)

Req.	Specification	Type	Instrument
042.1	S must provide P with data sharing mechanisms.	–	Mechanisms
042.2	S must provide P with mechanisms allowing the revocation of access rights.	–	Mechanisms
042.3	S must provide P with mechanisms for the administration of access rights.	–	Mechanisms
042.4	S must provide P with mechanisms for amending and correcting personal data.	–	Mechanisms
042.5	S must provide P with mechanisms that allow to express binding privacy policies regarding the disclosure of data to third parties.	–	Mechanisms

Table 6 Category codes: attribute (left) and Value (right)

Attribute		Value
Type	Ex ante	100
	Ex post	200
	Not transparency	000
Property	Availability	10
	Verifiability/ Auditability	20
	Accountability	30
	Empowerment	40
Instrument	Information	1
	Mechanisms	2

The three requirements can potentially be applied over the 41 identified requirements. If we do so, we obtain 41×4 requirements (for each original version we add three modalities). We can even give an ID to them if we assume modality being a fourth attribute.

For instance, requirement 232.1 - "S must provide P with accountability mechanisms" have three other modalities: 1232.1 - "[S must inform P that there are] accountability mechanisms"; 2232.1 - "S must provide P with [usable] accountability mechanisms"; 3232.1 - "S must provide P with accountability mechanisms [that do not disclose other private information]".

Discussion and conclusion

We have discussed transparency as a property of relevance in Health Information Technology, and we have elicited several requirements that suggest how to realise it in medical data systems.

We cannot claim to have included all possible concepts that one may find be linked to transparency. For instance, Leite and Cappelli in [21] categorise transparency in terms of more concepts than those we consider here, but they refer to the broader context of business processes. However, at least in the domain of medical data systems availability,

Table 7 Quality requirements. (S = medical system; P = patient)

Req.	Specification	Quality
1000	S shall inform the P about the existence of transparency tools.	Existence
2000	S shall comply with a requirement in an understandable and usable way.	Usability
3000	S shall comply with a requirement without harming data privacy.	Privacy

verifiability/auditability, and accountability are the properties that we have found to contribute the most to a precise understanding of transparency.

The requirements that we present here describe how to realise this understanding of transparency. Presenting transparency in this way, we believe, should facilitate its implementation.

We also studied transparency in respect to other properties, namely empowerment, usability and privacy.

Empowerment, which is about giving patients control on his/her Electronic Health Records, emerged to be a complementary property to transparency. Together, transparency and empowerment help realise openness, a concept that we argued include transparency. We gave also requirements for empowerment. The implementation of them will make medical systems fully patient-oriented, although implementing them may require big architectural and regulatory changes in the current Health Information Technology.

Usability and privacy do not directly contribute to the notion of transparency, but enhance its quality. Their requirements are desirable but not mandatory. Implementing a private and usable transparency brings some challenges and we leave the task of understanding how to implement such properties together for future work.

We also intend to develop, as future work, a complete set of metric to assess, given a system, up to which level it complies with our requirement. This can be a measure of the quality of transparency for medical data systems. Preliminary results on this matter are reported in [34].

Acknowledgments Spagnuelo's research is supported by FNR/AFR project 7842804 TYPAMED.

References

1. AL Faresi, A., Wijesekera, D., and Moidu, K., A comprehensive privacy-aware authorization framework founded on HIPAA privacy rules. In: Proceedings of the 1st ACM International Health Informatics Symposium, pp. 637–646. ACM, 2010.
2. Benaloh, J., Chase, M., Horvitz, E., and Lauter, K., Patient controlled encryption: Ensuring privacy of electronic medical records. In: Proceedings of the 2009 ACM Workshop on Cloud Computing Security, CCSW '09, pp. 103–114. ACM, 2009.
3. Berthold, S., Fischer-Hübner, S., Martucci, L., and Pulls, T., Crime and punishment in the cloud - accountability, transparency, and privacy. In: Pre-Proceedings of International Workshop on Trustworthiness, Accountability and Forensics in the Cloud in conjunction with the 7th IFIP WG 11.11 International Conference on Trust Management, 2013.
4. Cappelli, C.: Uma abordagem para transparência em processos organizacionais utilizando aspectos. Ph.D. thesis, PUC-Rio, 2009.
5. Cruzes, D., and Jaatun, M.: D:b-2.4 requirements report deliverable, 2014.
6. EU: Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation). http://ec.europa.eu/justice/data-protection/reform/index_en.htm, 2012.
7. Ferreira, A., and Lenzini, G., Can transparency enhancing tools support patient's accessing electronic health records? In: Proceedings of the 3rd World Conference on Information Systems and Technologies, 2015.
8. Fischer-Hübner, S., Angulo, J., and Pulls, T., How can cloud users be supported in deciding on, tracking and controlling how their data are used? In: Privacy and Identity Management for Emerging Services and Technologies, IFIP Advances in Information and Communication Technology, Vol. 421, pp. 77–92. Berlin Heidelberg: Springer, 2014.
9. Gajanayake, R., Iannella, R., and Sahama, T., Sharing with care: an information accountability perspective. *Intern. Comput. IEEE* 15(4):31–38, 2011.
10. Goodman, K. W., Berner, E. S., Dente, M. A., Kaplan, B., Koppel, R., Rucker, D., Sands, D. Z., Winkelstein, P., and et al., Challenges in ethics, safety, best practices, and oversight regarding HIT vendors, their customers, and patients: a report of an AMIA special task force. *J. Amer. Med. Inf. Assoc.* 18(1):77–81, 2011.
11. Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N., and Müller, G., Aspects of privacy for electronic health records. *Int. J. Med. Inf.* 80(2):e26–e31, 2011. Special Issue: Security in Health Information Systems.
12. Hansen, M., Marrying transparency tools with user-controlled identity management. In: The Future of Identity in the Information Society, Vol. 262, pp. 199–220. US: Springer, 2008.
13. Hedbom, H., A survey on transparency tools for enhancing privacy. In: The Future of Identity in the Information Society, IFIP Advances in Information and Communication Technology, Vol. 298, pp. 67–82. Berlin Heidelberg: Springer, 2009.
14. Henke, N., Kelsey, T., and Whately, H., Transparency — the most powerful driver of health care improvement? *Health Int.* 64–73, 2011.
15. Hu, J., Chen, H., and Hou, T., A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations. *Comput. Standards Interf.* 32:274–280, 2010.
16. International Organization for Standardization: ISO 9241-11:1998 Ergonomic requirements for office work with visual display terminals (VDTs) (2000). Part 11: Guidance on usability.
17. Kim, K., McGraw, D., Mamo, L., and Ohno-Machado, L., Development of a privacy and security policy framework for a multistate comparative effectiveness research network. *Med. Care* 51:S66–S72, 2013.
18. Kremer, S., Ryan, M., and Smyth, B., Computer Security – ESORICS 2010: 15th European Symposium on Research in Computer Security, Athens, Greece, September 20-22, 2010. In: Proceedings, chap. Election Verifiability in Electronic Voting Protocols, pp. 389–404. Berlin, Heidelberg: Berlin Heidelberg, 2010.
19. Ku̇sters, R., Truderung, T., and Vogt, A., Accountability: definition and relationship to verifiability. In: Proceedings of the 17th ACM Conference on Computer and Communications Security, CCS 2010, Chicago, Illinois, USA, October 4-8, 2010, pp. 526–535: ACM, 2010.
20. van Lamsweerde, A. *Requirements Engineering: From System Goals to UML Models to Software Specifications*: Wiley, 2009.
21. Leite, J. C. S.d.P., and Cappelli, C., Software transparency. *Bus. Inf. Syst. Eng.* 2:127–139, 2010.
22. Liebovitz, D., Meaningful EHR attributes for an era of accountability, transparency, shared decision making, and value assessment. *J. Legal Med.* 34(1):43–53, 2013.
23. Moe, N.: D:b-2.1 workshop 1 results (requirements), 2013.

24. Office for Civil Right of the Department of Health and Human Services, USA: Privacy, Security, and Electronic Health Records (2015).
25. Online Computer Library Center, Inc.: Dewey decimal classification. https://www.oclc.org/dewey/features/summaries.en.html. Last accessed in May 2016.
26. Open Source Initiative: The Open Source Definition. https://opensource.org/. Last accessed in May 2016.
27. Peters, M., The idea of openness: Open education and education for openness. In: Peters, M., Besley, T., Gibbons, A., Žarnić, B., and Ghiraldelli, P. (Eds.) The Encyclopaedia of Educational Philosophy and Theory, 2010.
28. Press, O.U.: Oxford Dictionaries. http://www.oxforddictionaries.com/. Last accessed in May 2016.
29. Ray, P., and Wimalasiri, J., The need for technical solutions for maintaining the privacy of EHR. In: Engineering in Medicine and Biology Society, 2006. EMBS'06. 28th Annual International Conference of the IEEE, pp. 4686–4689: IEEE, 2006.
30. Rostad, L., An initial model and a discussion of access control in patient controlled health records. In: Proceedings of the 3rd International Conference on Availability, Reliability and Security, pp. 935–942, 2008.
31. Ruotsalainen, P., Blobel, B., Nykänen, P., Seppälä, A., and Sorvari, H.: Framework model and principles for trusted information sharing in pervasive health, 2011.
32. Señor, I., and Fernández-Alemán, J., Security and privacy in electronic health records: a systematic literature review. *J. Biomed. Inf.* 46(3):541–562, 2013.
33. Seneviratne, O., and Kagal, L., Enabling privacy through transparency. In: Proceedings of the 12th Annual International Conference on Privacy, Security and Trust, pp. 121–128, 2014.
34. Spagnuelo, D., Bartolini, C., and Lenzini, G., Metrics for Transparency. In: Proceedings of Data Privacy Management and Security Assurance: 11th International Workshop, DPM 2016 and 5th International Workshop, QASA 2016, pp. 3–18, 2016.
35. Spagnuelo, D., and Lenzini, G., Patient-centred transparency requirements for medical data sharing systems. In: New Advances in Information Systems and Technologies, pp. 1073–1083: Springer, 2016.
36. Tang, P. C., and Lansky, D., The missing link: bridging the patient–provider health information gap. *Health Affairs* 24(5):1290–1295, 2005.
37. Thorogood, A., and Zawati, M. H., International guidelines for privacy in genomic biobanking (or the unexpected virtue of pluralism). *J. Law Med. Ethics* 43(4):690–702, 2015.
38. Turilli, M., and Floridi, L., The ethics of information transparency. *Ethics Inf. Technol.* 11(2):105–112, 2009.