PhD-FSTC-2018-75
The Faculty of Sciences, Technology and Communication

DISSERTATION

Defence held on 28/11/2018 in Luxembourg

to obtain the degree of

DOCTEUR DE L'UNIVERSITÉ DU LUXEMBOURG

EN INFORMATIQUE

by

Dayana PIERINA BRUSTOLIN SPAGNUELO
Born on 20 August 1989 in Florianópolis, Brazil

DEFINING, MEASURING, AND ENABLING TRANSPARENCY FOR ELECTRONIC MEDICAL SYSTEMS

Dissertation defence committee

Dr Peter Y. A. RYAN, dissertation supervisor
Professor, Université du Luxembourg

Dr Paulo ESTEVES-VERÍSSIMO, Chairman
Professor, Université du Luxembourg

Dr Gabriele LENZINI, Vice-chairman
Senior Research Scientist, Université du Luxembourg

Dr Simone FISCHER-HÜBNER
Professor, Karlstad University

Dr Jean Everson MARTINA
Senior Lecturer and Researcher, Universidade Federal de Santa Catarina

UNIVERSITY OF LUXEMBOURG

DOCTORAL THESIS

Defining, Measuring, and Enabling Transparency for Electronic Medical Systems

Author:
Dayana P. B. SPAGNUELO

Supervisor:
Prof. Dr. Peter Y. A. RYAN
Daily advisor:
Dr. Gabriele LENZINI

A thesis submitted in fulfilment of the requirements
for the degree of Doctor of Philosophy

in the

Applied Security and Information Assurance Group
SnT - Interdisciplinary Centre for Security, Reliability and Trust

November 28, 2018

Declaration of Authorship

I, Dayana P. B. SPAGNUELO, declare that this thesis titled, “Defining, Measuring, and Enabling Transparency for Electronic Medical Systems” and the work presented in it are my own. I confirm that:

- This work was done wholly or mainly while in candidature for a research degree at this University.
- Where any part of this thesis has previously been submitted for a degree or any other qualification at this University or any other institution, this has been clearly stated.
- Where I have consulted the published work of others, this is always clearly attributed.
- Where I have quoted from the work of others, the source is always given. With the exception of such quotations, this thesis is entirely my own work.
- I have acknowledged all main sources of help.
- Where the thesis is based on work done by myself jointly with others, I have made clear exactly what was done by others and what I have contributed myself.

Signed: Dayana P.B. Spagnuelo

Date: November 28, 2018

Abstract

Dayana P. B. SPAGNUELO

Defining, Measuring, and Enabling Transparency for Electronic Medical Systems

Transparency is a novel concept in the context of Information and Communication Technology (ICT). It has arisen from regulations as a data protection principle, and it is now being studied to encompass the peculiarities of digital information. Transparency, however, is not the first security concept to be borrowed from regulations; privacy once emerged from discussions on individual's rights.

Privacy began to be vigorously debated in 1890, when Warren and Brandeis analysed legal cases for which penalties were applied on the basis of defamation, infringement of copyrights, and violation of confidence [244]. The authors defended that those cases were, in fact, built upon a broader principle called *privacy*. But privacy was only given a structured definition almost one century later, in 1960, when Prosser examined cases produced after Warren and Brandeis' work [176], classifying violation of privacy into four different torts; it took twenty years more before the concept was thoroughly studied for its functions in ICT. Guidelines by the OECD outlined principles to support the discussion of privacy as a technical requirement [56]. Proceeded by international standards for a privacy framework (ISO/IEC 29100), which translated the former legal concepts into information security terms, such as data minimisation, accuracy, and accountability.

Transparency has a younger, but comparable history; the current General Data Protection Regulation (GDPR) defines it as a principle which requires "that any information and communication relating to the processing of those personal data be easily accessible and easy to understand [..]". However, other related and more abstract concepts preceded it. In the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Privacy Rule demands to document privacy policies and procedures and to notify individuals of uses of their health information. Former European Directives, i.e., 95/46/EC and 2011/24/EU, establish "the right for individuals to have access to their personal data concerning their health [..] also in the context of cross-border healthcare". The same did the Freedom of Information Act (FOIA) of 1966, instituting that any person has a right to obtain from agencies information regarding their records. These and other similar requests refer to the transversal quality called *transparency*.

Similarly to what happened with privacy, transparency was also the subject of guidelines that clarify its interpretation in ICT [10]. However, no framework or standard has been defined yet that translates transparency into a technical property. This translation is the goal of our work.

This thesis is dedicated to debate existing interpretations for transparency, to establish requirements and measurement procedures for it, and to study solutions that can help systems adhere to the transparency principle from a technical perspective. Our work constitutes an initial step towards the definition of a framework that helps accomplish meaningful transparency in the context of Electronic Medical Systems.

Acknowledgements

Four years of PhD studies have passed, and there is so much to be thankful for. First of all, I would like to express my gratitude to Professor Peter Y. A. Ryan, who took me into his group, APSIA, where I received all the support to conduct my research. Professor Ryan was also a big enabler of this project, for times providing insightful feedback and contributing to valuable discussions regarding my research. In his group I also had the opportunity to meet bright researchers, who soon became close friends; to my dear *Apsians* my warmest regards.

I could not even start discussing the merits of this research without mentioning Dr. Gabriele Lenzini, who accepted the challenging role of being my daily advisor. Gabriele taught me so much about science, from critical reasoning to argumentation, and scientific writing techniques. He pushed my boundaries and made sure I was always improving my ways, but he was also there to give me words of encouragement in times I needed so. Gabriele is a true *mentor* to me. Today I am proud to say that he helped me become the researcher I am. Gabriele, I am genuinely grateful for all your dedication, it was an honour working with you.

I would also like to thank Dr. Cesare Bartolini, who collaborated to my research, and also for times guided me through my saga; Prof. Dr. Paulo Esteves-Veríssimo, who dedicated time to evaluate my progress over these years; Prof. Dr. Simone Fischer-Hübner, and Dr. Jean Martina, who were kind enough to accept being members of my dissertation committee. I appreciate all the effort you invested.

This research project was also made possible with the support received from the Luxembourg National Research Fund (FNR), through the AFR project grant 7842804 – Transparent Yet Private Access to Medical Data (TYPAMED). I must also acknowledge the support received from the Doctoral Programme in Computer Science and Computer Engineering (DP-CSCE) and the Interdisciplinary Centre for Security, Reliability and Trust (SnT) in multiple occasions.

Finally, I would like to thank all the love and support received from my family. I am grateful to my mother, Iraci Brustolin, and my sister, Diane Spagnuelo, who fought so much to become who they are. They taught me by example how to be a stronger woman, and inspired me with their sweetness and generosity towards others. You will always be my role models. Also, to my husband and life partner, Cezar Signori, who accepted joining me abroad in pursuit of my degree. And who has never doubt me, even when I did so. Thank you for being so supportive. This accomplishment is also yours.

Contents

List of Figures

List of Tables

List of Abbreviations

BTG	Break-the-Glass
CNF	Conjunctive Normal Form
DAC	Discretionary Access Control
DNF	Disjunctive Normal Form
EAL	Evaluation Assurance Levels
EHRs	Electronic Health Records
FOIA	Freedom of Information Act
GDPR	General Data Protection Regulation
HCI	Human-Computer Interaction
HIPAA	Health Insurance Portability and Accountability Act
Health IT	Health Information Technology
ICT	Information and Communication Technology
MDE	Model-Driven Engineering
NFR	Non-Functional Requirement
RE	Requirements Engineering
SDLC	Systems Development Life Cycle
SDM	German Standard Data Protection Model
SE	Searchable Encryption
SSE	Symmetric Searchable Encryption
TEAL	Transparency Evaluation Assurance Levels
TET	Transparency Enhancing Tool
UML	Unified Modeling Language
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
WP29	Article 29 Data Protection Working Party

In memory of Benitto Romano Spagnuelo Tripicchio.
"Para siempre estarás."

Chapter 1

Introduction

Transparency is a concept invoked to implement people's right to have control over their data [205]. It has been defined as "the possibility to access information and evidences revealed through a process of disclosure" [237]. It has been presented as the "practice to inform users and make policies and processes openly available" [124] and as the "predisposition to increase responsibility and accountability" [75].

The recently approved General Data Protection Regulation (GDPR)[1] describes transparency as one of the main principles in processing of personal data. It states that data controllers shall "provide any information [..] relating to processing to the data subject in a concise, transparent, intelligible and easily accessible form" and that they shall "facilitate the exercise of data subject rights" (Article 12.1 and 12.2).

Transparency is also a principle that can be embraced to promote honesty and therefore trustworthiness [126]. Transparency can also be a strategic element in business, especially when applied in distributed data management systems, such as cloud computing, electronic banking, or medical data-sharing. Personal data are an asset [201, 202] and data controllers may suffer from the mistrust of data subjects (e.g., users, clients, patients) who, aware of the risks of potential exposure of personal information [101], can be reluctant to consent with the processing of their data. Transparency here can help build and preserve trust: providers that offer detailed information about their policies and practices, express them in a clear and readable manner, and have easily-accessible documents and records of processing operations will also have a better chance of gaining their client's trust and stay in business. For all these reasons transparency is considered a pro-ethical principle believed to promote accountability, improve service quality, empower people by giving them choices and right to demand better services, and foster social innovation and economic growth [99, 166].

In the domain of medical data systems, transparency is a desirable quality. Electronic Health Records (EHRs) carry very sensitive data about a patient and are subject to exceptional protection measures[2]. Even though transparency is not meant to provide such measures, it promotes having clear privacy policies, and the availability of means for patients to verify that the system is taking or has taken the necessary precautions to protect their data.

1.1 Medical Data Systems

It is true that to some extent transparency may be accomplished outside the domain of Information Technology. A conversation between a physician (or some other

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

[2] *Ibid.*, Art. 9.

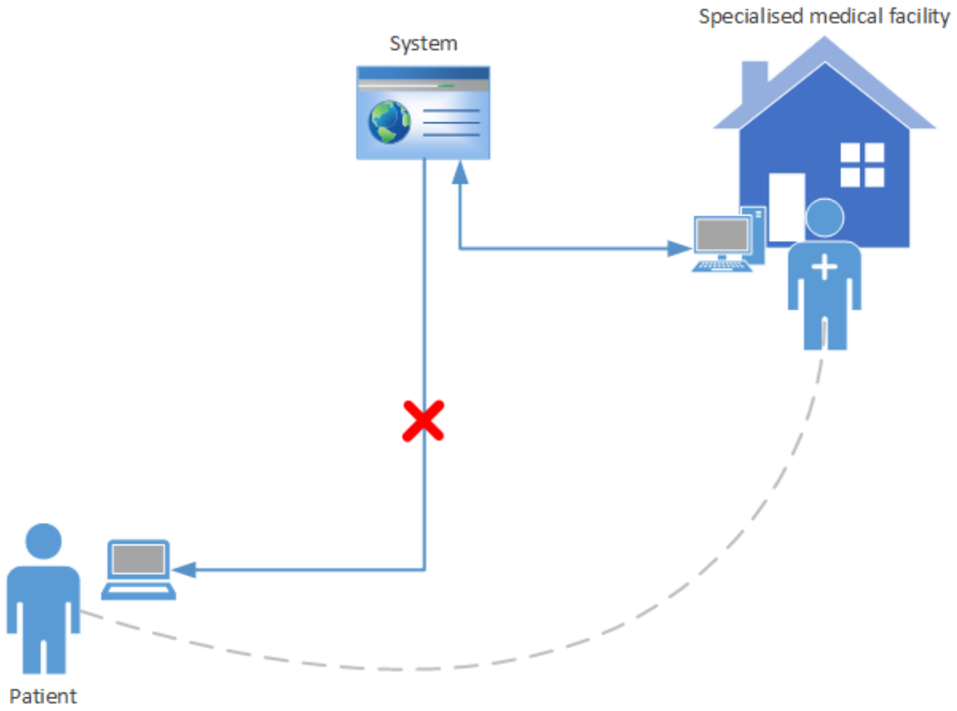


FIGURE 1.1: Hospital information system.

member of a medical team) and their patient can be sufficiently revealing about how personal data are handled. Nevertheless, in this work, we assume that there is, or can be, a channel for the patient to directly access 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 GDPR.

We base our understanding of the information flow in modern medical processes, with respect to five specific systems: i) the *Visual Electronic Patient Record* (VEPR) of the São João Hospital, Portugal, a centralised data management system that collects clinical reports from various hospital departments and makes them accessible to authorised health professionals; ii) 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; iii) 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; iv) the *Shared Care Dossier* (myDSP), the Luxembourgish EHRs system, which connects patients and caregivers; v) the *Microsoft HealthVault*, an online platform for storing personal health information. In what follows we describe and classify them according to the level of access the patients have to their data.

No access

The Visual Electronic Patient Record system (VEPR) (see Figure 1.1) foresees no interaction between the patients and the system [43]. In the usual scenario, the patient goes to the specialised medical facility and is treated by the physician who, in turn, accesses the system to retrieve the patient's health history.

The clinical research data system of the NCER-PD (see Figure 1.2) aims to aid the management of medical information about patients participating in long-term clinic

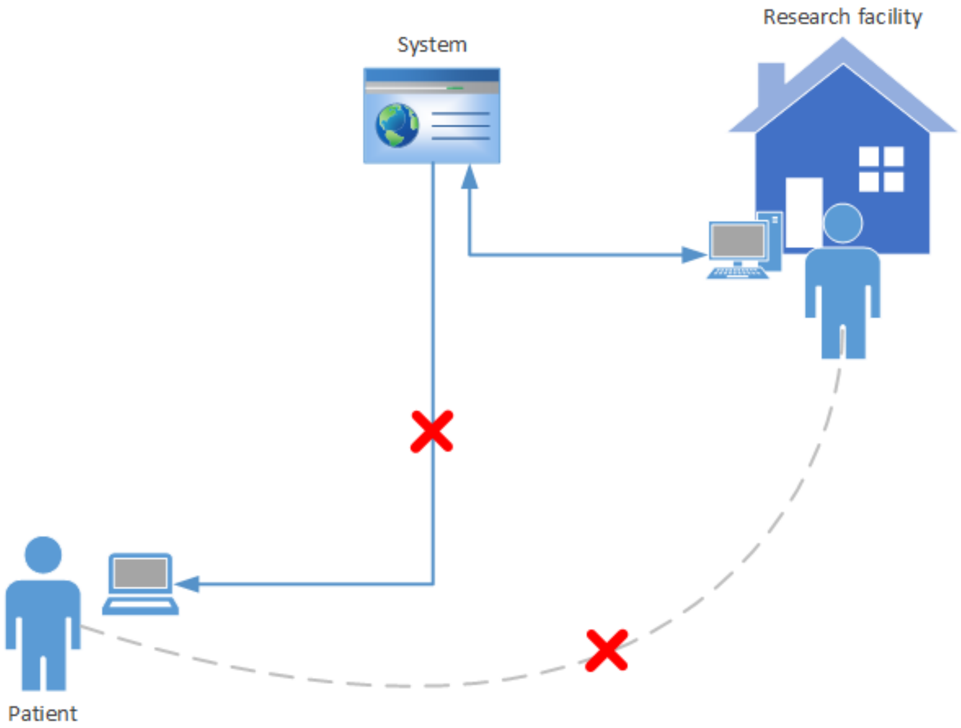


FIGURE 1.2: Clinical research system.

research. In the current implementation, the patients can neither access the system, or contact the researchers and the medical team that handle their data. The patients entrust their data to be used in clinical research with the goal of studying a specific disease.

Limited access

The Brazilian telemedicine system[3] (STT/SC) (see Figure 1.3) foresees an interaction between patients and the system. However, this interaction is limited to the access to medical examinations with no contact with specialised physicians. Patients only have contact with nurses and the technical team that handle medical equipment in their regional medical facility.

Full access

The Shared Care Dossier[4] (Dossier de Soins Partagé – myDSP, in the original language) is an online service provided by the Luxembourgish eHealth platform (see Figure 1.4). It stores several types of health-related information from the patients. These pieces of information can be provided by the patients, by a trusted health care professional, or by medical institutions, such as laboratories. In myDSP, the patients are in full control of who has access to their data, and what information can be shared with healthcare professionals.

Finally, Microsoft HealthVault[5] is an online platform that allows users to gather, store and share health information (see Figure 1.5). The information in HealthVault

[3] https://telemedicina.saude.sc.gov.br/rctm/.
[4] https://www.esante.lu/portal/fr/.
[5] https://www.healthvault.com/lu/en.

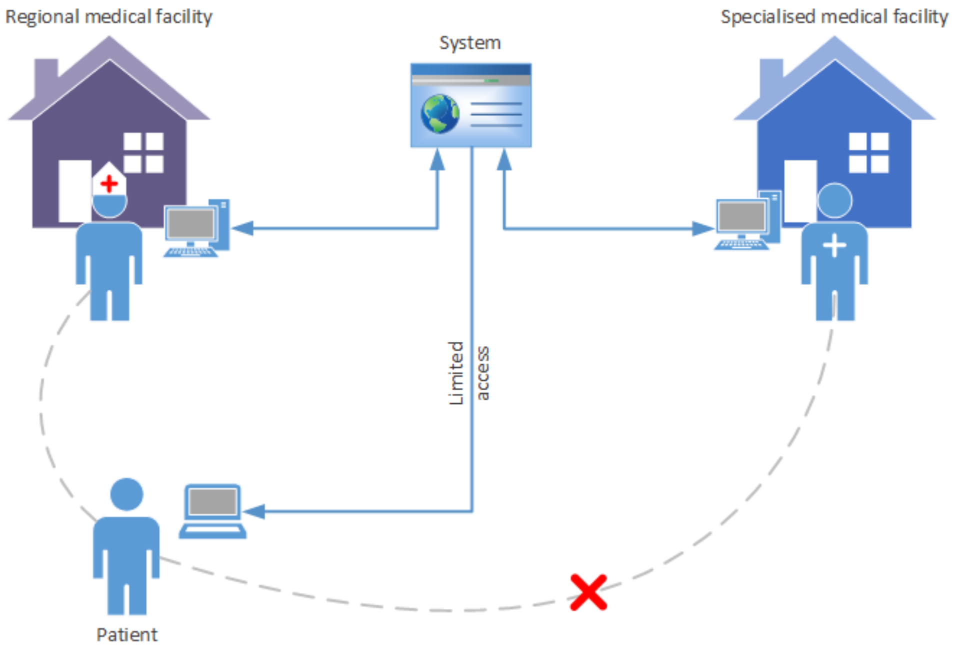


FIGURE 1.3: Telemedicine system.

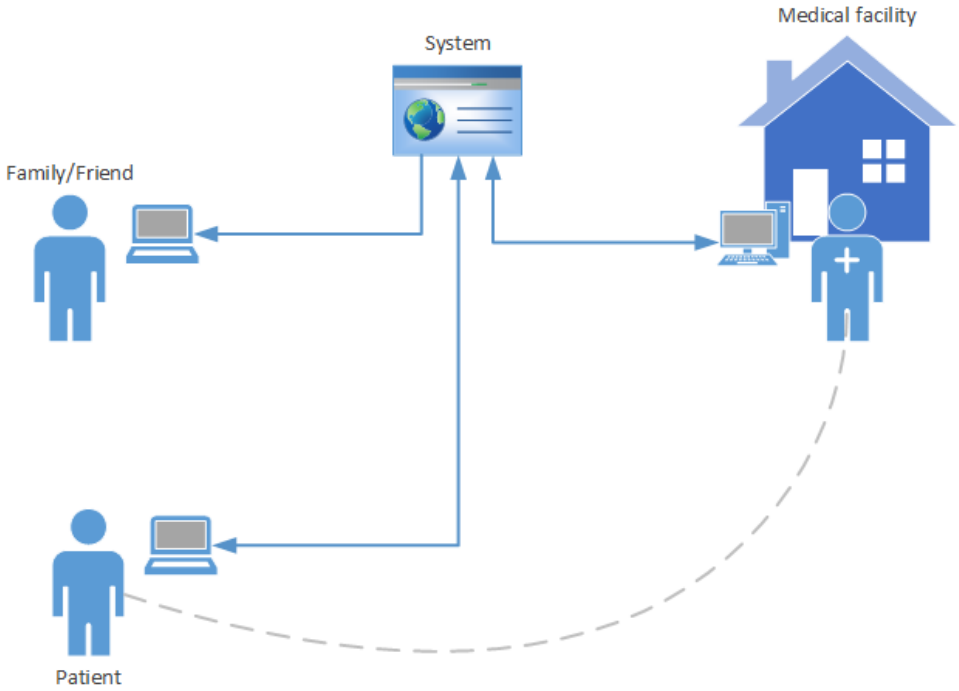


FIGURE 1.4: Electronic Health Record system.

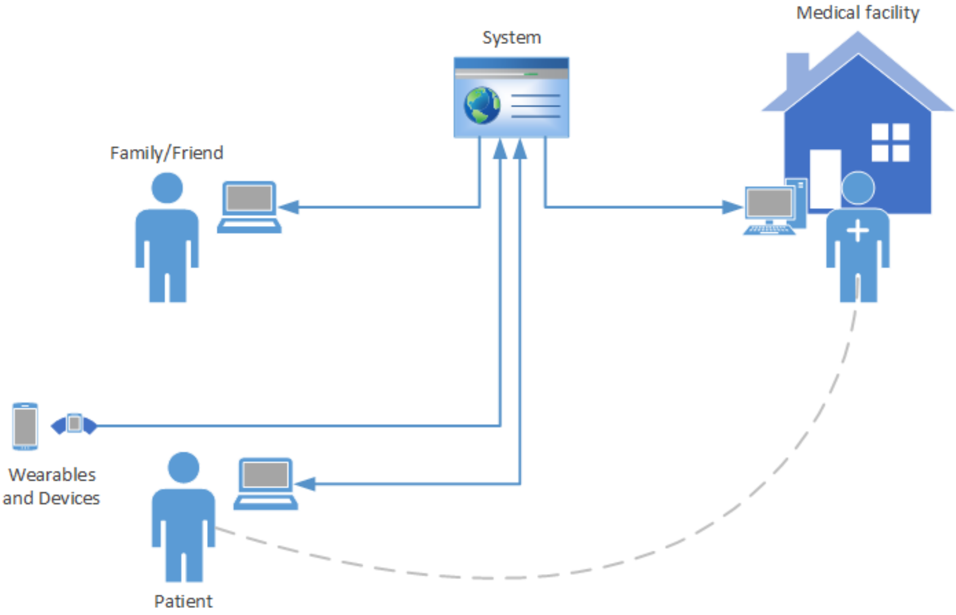


FIGURE 1.5: Patient-centred system.

can be provided by the user, an external mobile or web applications whenever authorised by the user, or by specific compatible health devices, such as blood pressure monitors, weight scales, and others. Microsoft HealthVault is patient-centred: it allows the patients to choose who can have access, edit, or act as a custodian of their data.

Overview. A peculiarity of the medical domain is that the content produced about patients is often not created by the patients themselves but by other subjects, such as physicians or healthcare professionals. Commonly, data is created, edited, and accessed without the knowledge or the consent from the patients. Such peculiarities can be observed in the medical data systems previously mentioned. As a consequence, the process of disclosure of data is not as evident as in other domains. For example, in online banking, users are typically informed of how the system will handle their current and future personal information when they are about to disclose their data to the system. With medical systems sometimes there is not even a precise moment when the data disclosure occurs, as it depends on when a patient visits the hospital or schedules an examination.

Another particularity of the medical domain is that the availability of health information is often related to the safety of the patients. Even though end users have the right to control the access and usage to personal data held by service providers, exercising this right in the medical domain may endanger patients' lives. Hence, solutions available in other domains may not be immediately suitable for medical systems. It is important to consider solutions that enable doctors and the medical team to access patient's data in case of emergency. This is often referred to in the literature as Break-the-Glass (BTG) [64]. However, regardless of how a patient's data reaches the system or how it is used, regulations, like the GDPR, are in place to protect patients' right to be informed.

1.2 Transparency in the recent literature

Despite not being fully explored in the context of medical data systems, there are some works which investigate transparency in other domains and are of paramount importance to our understanding of this property. We designate this section to the presentation and acknowledgement of these works. We also explore them further throughout this thesis and, where applicable, we contextualize them and explain how they contributed to inspire several stages of our research.

The Cloud Accountability Project[6] (A4Cloud for short) is a European Commission's Seventh Framework awarded project for increasing trust in cloud-based IT services. Several works related to this project explore the use of accountability tools, which is advocated to contribute to the governance of cloud activities by providing transparency and policy enforcement. In particular, two works executed for A4Cloud deserve to be highlighted here. The first, by Berthold *et al.* [19], focuses on the relationship between privacy, accountability and transparency. The properties are defined formally, in terms of information theoretic quantities, such as the Shannon entropy, and based on that the authors discuss the conceptual conflicts between them. The second, authored by Fischer-Hübner *et al.* [67], presents transparency in terms of data processing and classifies it into two categories: one that enables the anticipation of consequences before disclosure of data; and another that offers information about consequences if data has been already disclosed. This work proposes usability requirements to be considered when implementing transparency and presents a few transparency enhancing tools designed to meet these requirements.

Both works contribute significantly to the understanding of transparency and its relationship with other relevant properties. Apart from these works, a few other technical reports and deliverables from A4Cloud also assisted us in the clarification of transparency's meaning in the context of medical data systems.

Also relevant to our research are two works authored by Cappelli [31] and Leite [135], explore transparency in the context of software engineering. The authors qualify transparency as a Non-Functional Requirement (NFR). As such, they advocate that once implemented transparency should be spread across different parts of a software, and should not affect their behaviour. The authors further explore transparency in the context of a NFR framework by modelling it in a graph of concepts and other NFR which are suggested as composing and contributing to the realisation of transparency. Both works shed light on how such a property, which cannot be objectively said to be implemented in software, could be evaluated in a less objective notion of satisfaction.

Finally, another work deserves to be highlighted here for its relevance to the state of the art of transparency studies. The recent work authored by Meis and Heisel [149] presents a thorough requirements engineering analysis of the privacy goal of intervenability, a property said to be strongly coupled with transparency. Intervenability is a property that allows for end-users empowerment by giving them control over how the processing of their data is done. In this sense, transparency relates to it because it informs the end-users on the processing of data and exception accesses to data (both subject of intervention from the end-users), and should also inform about the existence of intervenability tools available in a system. The authors present a detailed taxonomy (see Figure 1.6) which clarifies the hierarchy amongst their requirements and the relationship between the two properties.

[6] http://www.cloudaccountability.eu/.

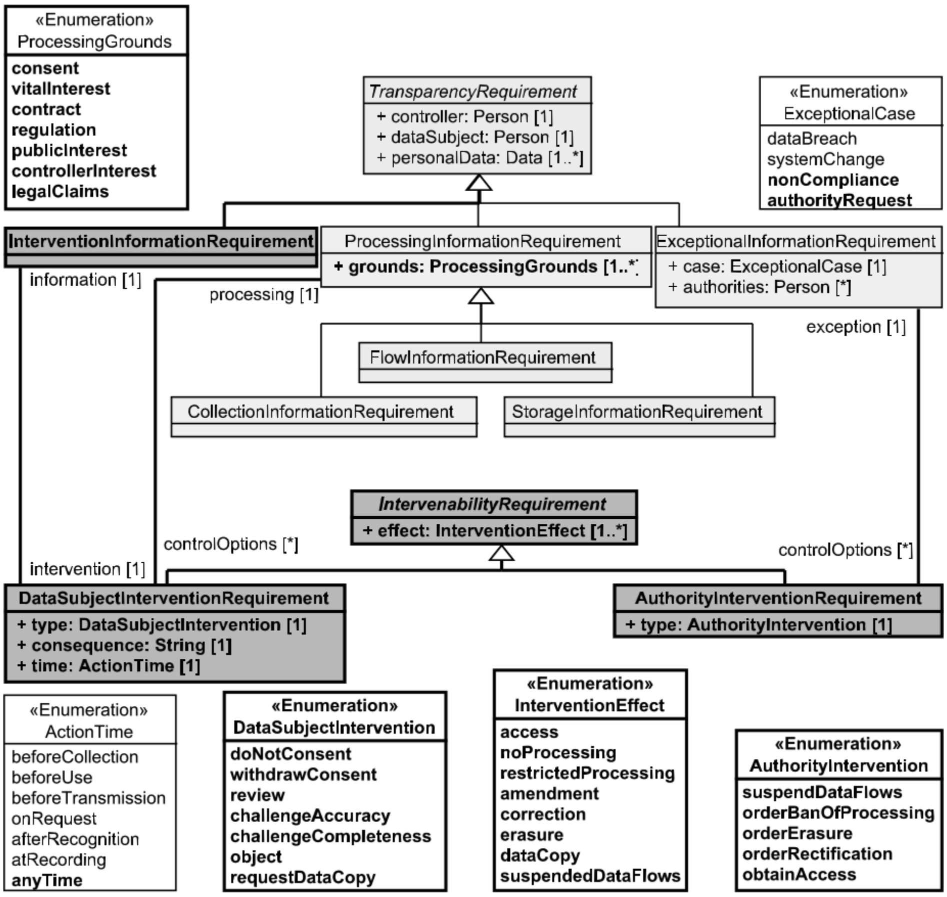


FIGURE 1.6: Transparency and Intervenability taxonomy proposed by Meis and Hiesel (image taken from [149]).

Meis and Heisel also propose a computer-aided method to support a privacy analysis of any given software based on its functional requirements. As intervenability and transparency are considered as privacy goals, this method also comprises an analysis of those. In other words, this method would identify the need for transparency and intervenability for any functional requirement of a system that foresees processing of data.

Our work and the work carried out by Meis and Heisel are related. However, we do not see them as conflicting, nor contradicting, rather our work agrees with the perspective presented by these authors. Nonetheless, our work distinguishes from [149] (and other work by the same authors) for we focus on transparency applied in the medical data systems context. This allowed us to deepen in the subject and to do a comprehensive analysis of transparency. Which in turn led to the study of its different aspects, the proposal of means to evaluate it in a system, and the analysis and modelling of transparency enhancing tools that are meant to be applied in that domain.

1.3 Goal and research questions

Transparency is a quality considered desirable in medical data systems to defend patients' right to data protection. However, beyond the demands of the legal framework and despite the discussions about the benefits of having transparency implemented in Health Information Technology (Health IT) (e.g., [75, 83, 139, 193, 205]), 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 is our research goal:

Research goal. *To provide a formal operational definition for transparency and to design solutions to achieve it in medical data systems.*

By clarifying the meaning of transparency in the medical domain, and providing an operational definition for it, we can help accomplish meaningful transparency in medical systems. The results of this research can be interpreted as a framework to guide the implementation of *transparency-by-design*. To achieve this goal we have structured our research around the following open questions:

1.3.1 How can transparency be defined in medical data systems and how does it relate to other security properties?

Even though transparency is not a new term, it has been discussed for a while with different meanings. In order to provide an operational definition for it in medical systems, we first have to study its different existing interpretations. What is an adequate understanding of transparency in the context of medical systems? How does transparency relate to other known properties? Is transparency part of, or composed by other known properties? Does transparency conflict with, or compromise any of those?

1.3.2 How can transparency be assessed in a system?

Transparency is not a clear requirement. Its several interpretations already suggest that it is instead a multi-faceted subjective property. Finding or proposing an adequate interpretation that considers the peculiarities of the medical domain is not enough if there are no ways of telling whether a given system is indeed transparent. With transparency being a complex property, how can one decide if it is being realised in a system? Are there objective ways of assessing how transparent a system is?

1.3.3 How can transparency be realised in a privacy-friendly manner?

Since transparency is a property related to the disclosure of information, intuitively one would think that transparency can weaken or compromise people's right for data privacy, if not correctly implemented. Transparency is a principle intended to promote trust; it should not come at the expense of privacy. It is essential to understand whether transparency can become a hindrance to privacy, and where it does, how to realise it in a privacy-friendly way.

1.3.4 Can transparency be achieved with the existing tools?

The interest in transparency has grown in the past few years, and the number of Transparency Enhancing Tools (TETs) proposed in the literature reflects this fact. From a purely technical point of view, one could compare these tools and reason about the aspects of transparency which are implemented and well explored, and the ones in need of more investigation. However, are those tools suitable and sufficient to accomplish transparency in the medical data systems domain? Can they help achieve compliance with the GDPR provisions?

1.4 Thesis overview

Each chapter and appendix in this thesis explores topics related to the questions previously presented. An overview of contents is show in Table 1.1. In the following, we summarise the content of the chapters and highlight our contributions.

	Question 1.3.1	Question 1.3.2	Question 1.3.3	Question 1.3.4
Chapter 2	x		x	
Chapter 3	x			
Chapter 4		x		
Chapter 5			x	
Chapter 6				x

TABLE 1.1: Content overview. Chapters and the research questions they help answer.

Chapter 2: On Transparency and related properties. In this chapter, we explore the existing interpretations for transparency and its relationship with other known properties. This chapter contributes to answering the open question 1.3.1. To do so, we first perform a literature review about the primary security concerns in the medical domain, where we find out how transparency is debated in the domain, with which meaning, and with relation to which other properties. We later propose a definition of transparency, describe the most relevant properties linked to it, and suggest a taxonomy that represents how these properties contribute to each other. This chapter also starts discussing the relationship between transparency and privacy, contributing to answer the open question 1.3.3.

This chapter is based on two academic contributions: a literature review presented in a technical report [222]; and a journal article [223] that summarises our definition of transparency and positions it in a taxonomy of related properties.

Chapter 3: Transparency requirements. In this chapter, we expand the definition of transparency by establishing requirements that help realise it in a medical system. This chapter explores more technically the open question 1.3.1. In here we describe our requirements gathering methodology and present an extensive list of software requirements with their categories.

This chapter is based on two scientific contributions: a conference article [221] and a scientific journal which extends it [223].

Chapter 4: Metrics for Transparency. In this chapter, we present a set of metrics proposed to help assess how transparent a system is. This chapter presents discussions that answer the open question 1.3.2. In here we explain our methodology when selecting and defining metrics and mathematical formulations for quantifying transparency. We also justify and reason about their suitability. Later we propose a guide on how to properly apply those metrics, and how to conduct a full evaluation of transparency.

The content presented this chapter is adapted from the results published in a workshop [217] and a conference article [218]. Another manuscript was inspired by the results of this collaboration [219]; it was submitted to the Journal of Computers & Security, and it is currently under review.

Chapter 5: Private verification of access logs. In this chapter, we propose a tool for verifying if access logs comply with a given access control policy. This work contributes to answering the open question 1.3.3 by exploring searchable encryption schemes and reasoning on how they can be applied to achieve a privacy-friendly transparency. In here we first review the state-of-the-art on searchable encryption, we then propose a theoretical policy verifier. Later, we give insights into its feasibility based on algorithmic complexity and security considerations on the scheme.

This chapter is based on the work in collaboration with Thaís Bardini Idalino (University of Ottawa) and Dr. Jean Everson Martina (Universidade Federal de Santa Catarina). The content presented here was published in a workshop article [106].

Chapter 6: Accomplishing Transparency in Medical Systems. In this chapter, we systematically review what solutions, among the current Transparency Enhancing Technologies, can help accomplish transparency in agreement with our technical requirements and Articles we elicited from the General Data Protection Regulation. This work contributes to answering the open question 1.3.4; we reason on the current Transparency Enhancing Tools (TETs) and discuss the aspects of transparency which still need to be better explored from a technical perspective.

This chapter is based on the work realised in collaboration with Dr. Ana Margarida Leite de Almeida Ferreira (CINTESIS - University of Porto) and Dr. Gabriele Lenzini (SnT - University of Luxembourg). The result of this collaboration was published in a conference article and was awarded *Best Paper* at the 5th International Conference on Information Systems Security and Privacy [220].

Chapter 7: Concluding remarks. In this chapter, we present considerations taken in conclusion to this research project. We revisit our goal and questions and discuss how this thesis addresses them. We also present some future works and open problems which remain to be explored.

Appendix A: Transparency measurement procedure. This appendix describes in details how to compute each metric described in chapter 4. The description is given in a series of table, formatted according to the indications in the ISO/IEC 27004 standard.

Appendix B: Evaluation of Microsoft HealthVault. This appendix exemplifies the evaluation process we propose in chapter 4: we show, step by step, how to calculate the metrics to assess the quality of transparency on the Microsoft HealthVault. Lacking any comparative analysis, this assessment exercise is not meant to suggest any judgement on the quality of transparency and on the legal compliance of that particular service, but instead, it serves as an example of how to apply the metrics to a real system and of how to visualise the result.

Appendix C: Transparency Enhancing Tools in the context of the GDPR. This appendix expands the results of the work described in chapter 6: it presents a comprehensive table with the correlations between the TETs and each article from the GDPR we identify as transparency-related.

1.5 Scientific contributions

Below we list the scientific contributions arising from the execution of this research project.

Publications as main author

1. Dayana. Spagnuelo and Gabriele Lenzini. *Security on medical data sharing (a literature review)*. http://hdl.handle.net/10993/23241. Mar. 2015

2. Dayana Spagnuelo and Gabriele Lenzini. "Patient-Centred Transparency Requirements for Medical Data Sharing Systems". In: *New Advances in Information Systems and Technologies*. Ed. by Álvaro Rocha et al. Cham: Springer International Publishing, 2016, pp. 1073–1083. ISBN: 978-3-319-31232-3. DOI: 10.1007/978-3-319-31232-3_102

3. Dayana Spagnuelo and Gabriele Lenzini. "Transparent Medical Data Systems". In: *Journal of Medical Systems* 41.1 (2016), p. 8. ISSN: 1573-689X. DOI: 10.1007/s10916-016-0653-8

4. Dayana Spagnuelo, Cesare Bartolini, and Gabriele Lenzini. "Metrics for Transparency". In: *Data Privacy Management and Security Assurance: 11th International Workshop, DPM 2016 and 5th Int. Workshop, QASA 2016, Heraklion, Crete, Greece, September 26-27, 2016, Proceedings*. Cham: Springer International Publishing, 2016, pp. 3–18. ISBN: 978-3-319-47072-6. DOI: 10.1007/978-3-319-47072-6_1

5. Dayana Spagnuelo, Cesare Bartolini, and Gabriele Lenzini. "Modelling Metrics for Transparency in Medical Systems". In: *International Conference on Trust and Privacy in Digital Business*. Springer. 2017, pp. 81–95

6. Dayana Spagnuelo, Cesare Bartolini, and Gabriele Lenzini. “Qualifying and Measuring Transparency (A Medical Data System Use Case)”. In: *Computers & Security* (2018). **Under review; Submitted in August 2018**.

7. Dayana Spagnuelo, Ana Ferreira, and Gabriele Lenzini. “Accomplishing Transparency within the General Data Protection Regulation”. In: *5th International Conference on Information Systems Security and Privacy*. **To appear**. 2018

Publications as co-author

8. Thaís Bardini Idalino, Dayana Spagnuelo, and Jean Everson Martina. “Private Verification of Access on Medical Data: An Initial Study”. In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2017, pp. 86–103

Chapter 2

On Transparency and related properties

Medical records (e.g., test results and health reports) are about patients. Hospitals and healthcare institutions generate them after a patient's visit. Today they are digitized, stored electronically, and accessed remotely by professionals.

European directives suggest that patients should access these records too. Besides, they say, patients should have control over these data and be informed if and when their records are shared and how secure they are. These requirements are difficult to be met.

From a patient's perspective, the viewpoint of this work, it may be easier to address at least one of such requirements: to inform patients about how secure their data are. This is a property usually referred as *transparency*, but a clear meaning of the word is still missing.

This chapter is dedicated to clarify the meaning of transparency. In here we survey the literature in medical data sharing and discuss what are the main security concerns in it. In doing so, we investigate whether transparency is debated in this domain, in relation to which other properties, and which meaning and role are given to it. The findings of this task are described in section 2.1. Moreover, we explore the existing transparency definitions in other domains, and discuss how they fit in the medical data systems domain in section 2.2. Finally, we identify the concepts that relate to transparency and review them in the context of Health Information Technology (Health IT). This exercise is presented in section 2.3, it help us clarifying the role of transparency in modern medical data systems.

2.1 Transparency and security in Medical Systems

According to [63] transparency ought to be regarded as an additional feature that qualifies security. So, security can be said to be transparent when is intelligible to human user. It opposes an opaque security, which holds technically but without the user's being aware of it. Thus, transparency is a socio-technical security property.

Transparency, is not a new term. It has been proposed in relation to Transparency Enhancing Tools (TETs) [113]. These are usually browser extensions that read out web server's privacy policies and inform users concisely, for instance, that a web server records the user's whereabouts and may sell the user's data to third parties. TETs have been discussed in relation to electronic health records [63], but no concrete solution has been proposed. Transparency in the medical domain is still an unfulfilled requirement.

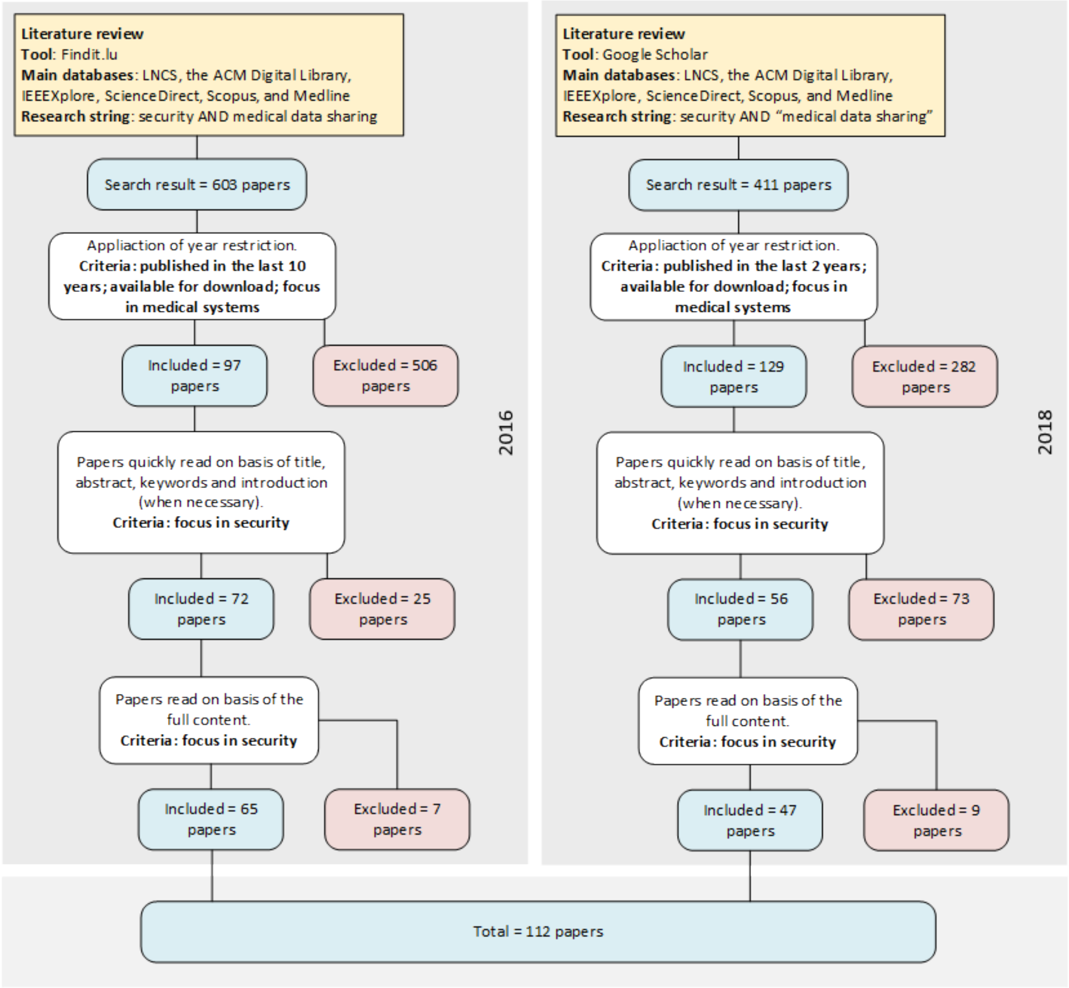

Literature review
Tool: Findit.lu
Main databases: LNCS, the ACM Digital Library, IEEEXplore, ScienceDirect, Scopus, and Medline
Research string: security AND medical data sharing
Search result = 603 papers
Appliaction of year restriction.
Criteria: published in the last 10 years; available for download; focus in medical systems
Included = 97 papers
Excluded = 506 papers
Papers quickly read on basis of title, abstract, keywords and introduction (when necessary).
Criteria: focus in security
Included = 72 papers
Excluded = 25 papers
Papers read on basis of the full content.
Criteria: focus in security
Included = 65 papers
Excluded = 7 papers
2016
Literature review
Tool: Google Scholar
Main databases: LNCS, the ACM Digital Library, IEEEXplore, ScienceDirect, Scopus, and Medline
Research string: security AND "medical data sharing"
Search result = 411 papers
Appliaction of year restriction.
Criteria: published in the last 2 years; available for download; focus in medical systems
Included = 129 papers
Excluded = 282 papers
Papers quickly read on basis of title, abstract, keywords and introduction (when necessary).
Criteria: focus in security
Included = 56 papers
Excluded = 73 papers
Papers read on basis of the full content.
Criteria: focus in security
Included = 47 papers
Excluded = 9 papers
2018
Total = 112 papers

FIGURE 2.1: Methodology diagram.

2.1.1 Methodology and tools

To find out whether transparency was debated in the medical data systems domain, we browsed the state of the art querying for "Security" and "Medical Data Sharing", and we looked for papers containing them in the title, in the abstract, in the list of keywords, and in the entire body. We chose "Security" because it is a general term: we expect that a paper that addresses more precise security properties will also mention "security" somewhere its text. We chose "Medical Data Sharing" to refine our domain to papers that discuss sharing medical data.

The literature review was conducted in two stages. Initially we executed a systematic review in 2016, it included all works published in the previous 10 years. In 2018, we again searched for works in that area, but only reviewed papers from the last 2 years. The results of the two reviews were later appended. An overview of our methodology is presented in Figure 2.1.

To conduct our literature review we searched for papers via "Findit.lu"[1] and Google Scholar[2]. The first is the largest library portal in Luxembourg, and it is entirely dedicated on searching for electronic contents. The second is the popular search engine from Google dedicated to the scholarly literature. Both index a large

[1] www.findit.lu.

[2] https://scholar.google.lu/.

number of important scientific digital libraries such as, among many others, LNCS, the ACM Digital Library, IEEEXplore, ScienceDirect, Scopus, and Medline. Browsing papers through the two engines ensures we diversify as much as possible our sources.

First, we queried without constraints on the year of publication. We got as many as 1014 articles (603 from the first stage, and 411 from the second), too many for us to be able to read or scan them all. Thus, we restricted the focus to the last 12 years, from 2006 to now. Excluding the repeated results and the papers not available for download, and the works that only mentioned medical systems as example, our pool shrank down to a total of 226 papers (97 from the first stage, and 129 from the second). We read the abstract and skimmed through the content of all of them. It turned out that 98 papers were about medical data sharing but with no focus on "security": the word appeared to be mentioned but the concept is not discussed. We read the remaining papers more carefully, again looking for papers focused on security. After this task, we were left with a pool of 112 papers (65 from the first stage, and 47 from the second). At this stage, we judged the number of paper selected sufficient to understand whether transparency was discussed in the medical domain. We did not conduct a snowballing search.

We organized our findings around one question: *"what particular security property the paper is about?"*. To answer this question helped us to classify the papers depending on the property, or properties, they debate. It also helps us to understand whether transparency is considered as a security requirement and, if it is, in relation to which other property.

2.1.2 Findings

Answering our main question, and so looking into what security properties our pool of papers is about, lead us to identify nine main security categories, each concerning policies, tools, or techniques meant to guarantee, preserve, or enforce a specific property. The nine categories are the following:

1. *Privacy* – providing anonymity to the data owners or empowering them to define who can operate on the data;

2. *User authentication* – enhancing the way in which users are authenticated electronically;

3. *Access control* – concerning better ways to define who can access medical data and in what circumstances;

4. *Data authenticity* – solutions to prove that data origin is authentic, and that it is coming from the source as claimed;

5. *Data Integrity* – solutions to guarantee and prove that the data has not been manipulated or tampered with;

6. *Confidentiality* – preventing data disclosure to non-authorized third-parties;

7. *Auditability* – helping data owners to retrieve information clarifying how their data is being used;

8. *Accountability* – helping data owners to hold someone or some entity responsible in case of data misuse;

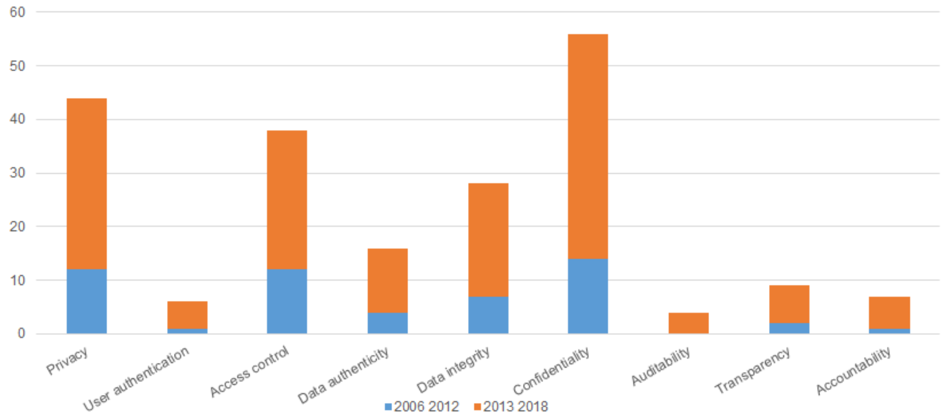


FIGURE 2.2: Number of papers published per category from 2006 to now. We distinguished the first from the second 6 years.

9. *Transparency* – informing and clarifying about security policies and processes.

Most of the surveyed papers argue about data confidentiality (see Figure 2.2). This property is invoked in relation to protect the data transmitted in open channels, such as the internet, or stored in open data bases, such as the cloud. One comment is mandatory: in the pool "confidentiality" there are 56 papers, namely [1, 2, 5, 6, 9, 11, 14, 20, 29, 33, 36–38, 50, 55, 59, 65, 91–94, 96, 100, 102, 105, 115, 118, 123, 134, 136, 140, 142, 144, 146, 148, 155, 161, 165, 182, 184, 189, 190, 195, 197, 200, 204, 207, 208, 211, 224, 232, 234, 240, 242, 253, 255]. Some of those were, per keywords, first gathered under "privacy". A closer look revealed that they are using the term inappropriately since their concern is mainly about encrypting data. But, encryption *per se* is insufficient to guarantee that the user's personal and sensitive information remains private during the whole data life cycle; more sophisticated techniques have to be in place for privacy to be protected. Thus, we decided to re-classify those works as being about confidentiality, adding those up to the ones already in that category.

Confidentiality is constantly discuss together with data integrity and data authenticity. That is because encryption is the technique that is more often adopted to enforce confidentiality in medical systems and the same technique is also proposed for data authenticity and integrity. In a total of 28 papers about data integrity (i.e., [5, 11, 14, 20, 36, 41, 50, 54, 55, 59, 84, 91, 94, 124, 131, 136, 140, 141, 144, 148, 158, 161, 189, 197, 200, 224, 232, 240]) only 7 works do not discuss confidentiality. We observed a very similar scenario with the category data authenticity. Only 5 works do not discuss confidentiality, out of 16 papers discussing data authenticity (i.e., [11, 14, 29, 41, 50, 54, 84, 131, 136, 140, 158, 161, 189, 197, 200, 240]). Also, almost all works that examine data authenticity explicitly discuss data integrity too, with exception of only one work (i.e., [29]).

After confidentiality, the second and third most discussed security properties are privacy and access control. We found out that 45 works discuss privacy (the correct interpretation of this term) [3, 7, 34, 39, 54, 75, 77, 84, 88, 90, 96, 97, 100, 102, 112, 120, 124, 127, 133, 137, 138, 143, 145, 161, 163, 165, 178–181, 187, 193, 196–198, 204, 207, 208, 211, 213, 214, 224, 233, 242, 246], and that 38 papers discuss access control [2, 3, 5, 6, 20, 23, 34, 58, 74, 93, 111, 112, 114, 132, 140, 141, 144–146, 161, 180, 181, 191, 193, 196, 197, 213, 215, 226, 230, 231, 240, 243, 246, 251–253, 255].

User authentication seems not a major concerns as it is present only in 6 papers [5, 36, 50, 88, 121, 146]. We do not have enough data to justify this lack of interest in authentication, but we can speculate on it. An hypothesis we have is that most of the works give for granted that medical data are accessed only by professionals and that they are considered trustworthy. Similarly, we claim that the lack of interest in user authentication may indicate that there is not yet a widespread concern about opening the access of the health data to patients. This is, indeed, a requirement that only very recently has been debated and brought to the attention of the society. If concrete actions to open up access to patients were taken into consideration, it would, we expect, raise more attention about identification and authentication. Indeed the works which discuss such a feature have identification and authentication as their main requirement (e.g., see [62]). A similar speculation, i.e., that the patient-centred approach is not yet under the bull's-eye in medical data security, concerns also the last three properties, transparency – the one of interest for our work, auditability and accountability. Auditability is subject of discussion of only 4 papers [141, 164, 197, 252]. Accountability is subject of discussion of 7 papers [65, 75, 100, 124, 197, 233, 251]. While transparency is mentioned only in 9 papers [65, 75, 100, 124, 127, 157, 193, 208, 233].

Transparency has been regarded as openness about policies and processes in [124, 157, 233]. 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*" [124], "*clear and accessible policies and procedures help maintain the trust of participants*" [233], and point out "*the need for transparent data stewardship practices, [..] as well as transparency about the transfer or sharing of any data*" [157]. Transparency has been considered a predisposition to increase responsibility and therefore presented with *accountability* as "*critical to helping society manage the privacy risks that accumulate from expeditious progress in communication, storage, and search technology*" [75], and "*increases the accountability and transparency of the HRI system, thus, improving its trustworthiness with all parties involved*" [65]. Transparency has been also defined as the the property *to be informative* towards the patient in [193]: the authors denounce the lack of transparency for "*[the] patient is not automatically aware which professionals or entities are processing her EHR and for what purposes. [The] patient is not aware of all disclosures of the content of her EHR*".

Most recent works regard transparency as a major issue, and a critical requirement for the success of systems [100, 127]. Henze et al. propose the concept of *transparency by design*. They advocate there should be documentation on data usage from the design and implementation of a service in order to improve transparency. We highlight here: "*individual concerns mainly result from the fact that there is no control or at least transparency over the access to this data*", "*[the] lack of precise, up-to-date information about the data processing again leads to uncertainty and non-transparency for the users*" [100]. Kostkova et al. point out that *transparency* and *openness* are paramount for regaining public trust; they defend that transparency implies "*public understanding of benefits and risks of data sharing, [..] strong disclosure, and notification mechanism informing public about potential [privacy] violations*" [127].

2.1.3 Discussion

Our review has an obvious limitation: it considers papers that matched only two key-phrases, "security" and "medical data sharing". However, "security" is a generic terms under which we were able to find papers discussing more specific properties and requirements. "Medical data sharing" is our target, so this choice is justified. Still one could question why we did not searched for synonyms, and whether, in not doing so, we missed some important papers. Our searching on the whole body of the

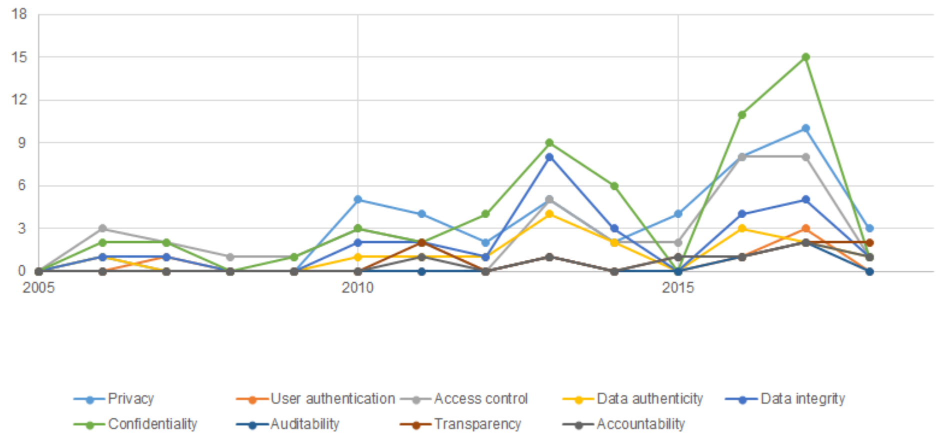


FIGURE 2.3: Number of papers per year per category.

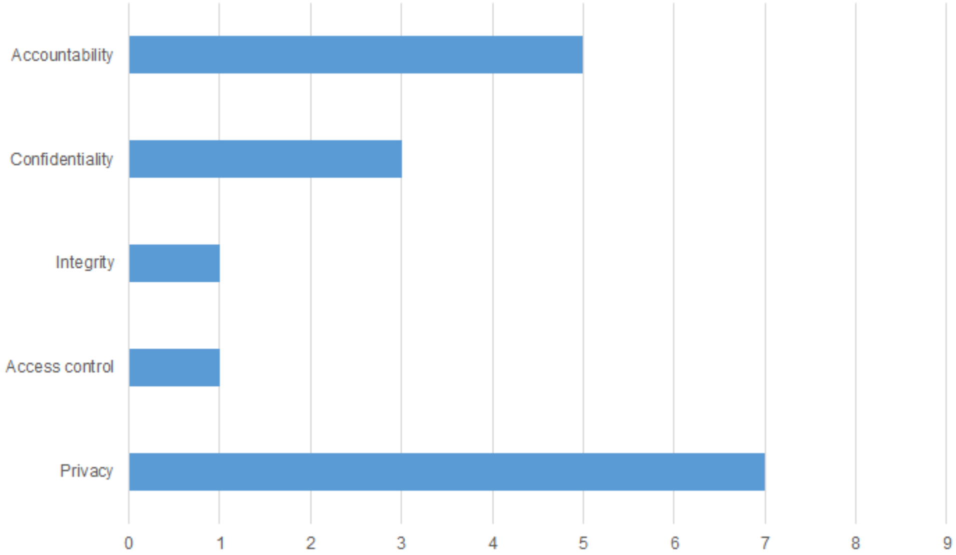


FIGURE 2.4: Properties related to Transparency and the number of papers in which they appear.

paper, however, was sufficient to catch works about electronic health records, biomedical data, health care information systems, health-grid. Therefore, we judged the choice of our key-phrases sufficiently good for our scope.

This survey, organized around the works published in the last 12 years, shows that confidentiality and privacy are the major concerns in security for medical data (see also Figure 2.3). Privacy is also the property that seems to be mostly related to transparency, as it is discussed in almost every work concerning transparency (see Figure 2.4). This comes with no surprise.

About transparency, the survey shows that this requirement has just began to be addressed; all the considered papers see transparency related to inform users and make policies and processes openly available. This seems to be the interpretation of “transparency” in the medical domain, a meaning which matches what we propose. However, there is no formalization of it and no standard solution that makes a medical system compliant to it.

Although we already had some hint of it, after having looked at the recent growth of interest as this survey reports, it is evident that there is still little attention from the security community towards auditability, accountability, transparency, and user authentication, at least in relation to medical data systems. We did not searched into the literature of auditability, for example, and checked for use cases on medical data (e.g., as in [49]). Auditability, accountability and transparency are essential wherever humans need to be informed about practices in sharing sensitive personal data. No solution exists to comply with current EU regulations on this. Our first impression is that both categories are relatively understudied in the medical sectors. We expect a growth in attention to these properties as the idea of user empowerment will get more popular.

User authentication seems suspiciously undervalued in the papers we surveyed. It is hard, from the data we have, to infer why. It may be that there are already good-enough authentication solutions to which medical systems can resort to. But, if we have to attempt another explanation, we are keen to suppose that current medical data are accessed mainly by professionals and that these roles are assumed to be trustworthy. Authentication is therefore implemented by simple login and password. Similarly as what we claimed while discussing transparency, if the EU directive suggesting to let users access their medical data should take off, we expect the problem of user authentication to became a pillar for the working of other several security features, and to foster a renewed interest.

2.2 Transparency definition

Apart from the works emerged from our systematic review (see section 2.1), three other works deserve to be commented for bringing up relevant discussions on transparency in the medical domain (i.e., [186, 205, 229]). Transparency is presented by Seneviratne and Kagal 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 [205].

Ray and Wimalasiri defend that transparency in medical systems has two dimensions: *to give access* to Electronic Health Records (EHRs) and *to disclose* how the systems works [186]. 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* [229].

All the considered papers in medical systems see transparency related to the act of *informing users* and *making policies and processes openly available*. This seems to be the interpretation of "transparency" in the Health IT. 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 [19]. TETs (see [63] and [98] for a survey) have been developed *to inform* users about how data are handled. In this sense, transparency is intended 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 [95] 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 [31, 135]. 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" [19]. 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 [19] is hardly measurable in which it depends on subjective abilities of individuals to acquire knowledge. A second definition that 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 [67]).

This definition fits better the concept of transparency that has been advocated for Health IT. 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 Health IT)**.** ***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 is not always clear when a data 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.

2.3 Related properties

The works we cited in section 2.1 and in section 2.2 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 where those properties emerge, and the reader may want to review the sections at this point.

Although these terms are often invoked to describe transparency, there is not an agreement on how they relate with transparency. Is transparency a collective name for these other properties? Is it a synonymous for some of them? Is it instead a property itself that is only qualified better by those concepts?

And how precisely those terms help qualifying transparency? These questions are unanswered.

We answer to these questions by discussing what these properties mean in the domain of Health IT and how they relate with transparency. Despite conceived for Health IT, the correlations between the concepts that we present remain valid even outside this application domain. The resulting taxonomy (see Figure 2.5) 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 chapter 3).

Empowerment. Empowerment is a concept that appears to be closely related to transparency. According to Oxford Dictionaries empowerment is the "authority or power given to someone to do something" [175]. In medical systems, empowerment has been discussed in terms of giving individuals power to take appropriate action with regard to personal data and privacy issues [95]; giving patients control over their health information [192]; and "[to] allow patients to grant access to specific portions of their health data" [203]. Empowerment has been discussed with the name of intervenability, as a means to give users the power to decide on the processing of their data [149]. 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, we see it as complementary to transparency for it gives individuals the right to react to the information provided by a transparent system.

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 organization, institutions or societies" [173]. The Open Source Initiative (OSI), who educate in methods for software development, reminds that open source is about disclosing source and allowing others to modify and derive other works [169]. 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 2.5 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" [175]. 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" [75].

Auditability is defined as "an official inspection of an organization's accounts, typically by an independent body" (derived from the definition of "audit" [175]). But in medical systems it has being regarded as an informal procedure made by the patients to indicate how sensitive data was used [205]. In this sense it can be also interpreted as "the ability to examine carefully for accuracy with the intent of verification" [135]. 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 [175]), or "the quality of being tested (verified or falsified) by experiment or observation" [135]. 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 [128] 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 2.5, 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 [130]. Berthold *et al.* link accountability and transparency by stating that accountability is being transparent about the occurrence of privacy breaches. In Figure 2.5, accountability is a brother node of auditability, both are an 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 [193], on the policies [95], and procedures [233]. These definitions closely relate to the concept of availability, which can be defined as*"the quality of being able to be used or obtained"* [175] or *"the quality of being at hand when needed"* [135]. 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 our work.

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" [108]. Despite desirable for transparency (see section 2.1 and section 2.2), 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 (a perspective also shared by [67]). Usability is not shown in Figure 2.5, but we will consider it 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 [173]. Instead, as pointed out in [19], privacy and transparency can be conceptually realised without friction. These properties do not conflict if the data that transparency intends to reveal is not the same data which privacy intends to protect. 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. However, the realisation of these two properties in a practical tool is far from trivial. Some of the technical challenges involving the implementation of privacy-preserving TETs are presented in [67], and are also further discussed in this thesis, in chapter 5. As we did for usability, we do not include privacy in Figure 2.5, but define for it subsidiary requirements.

Table 2.1 summarises and rephrases the properties that help defining transparency which are adapted to the Health IT domain. Figure 2.5 shows how they relate

Property	**Definition in Health IT**
Accountability	Enables the patients 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 EHRs.
Verifiability/Auditability	Enables the patient to verify what happened to his/her medical and personal data;

TABLE 2.1: Properties that relate with Transparency and their definition in relation to Health IT.

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

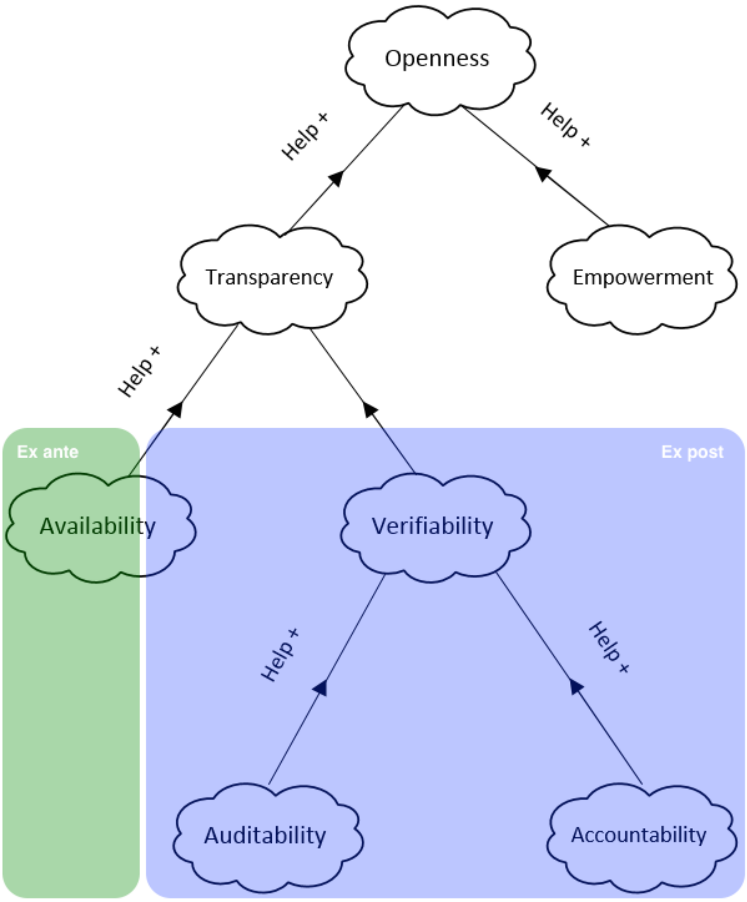


FIGURE 2.5: How other properties that relate with Transparency help defining ex post or ex ante Transparency.

Chapter 3

Transparency requirements

Instead of interviewing engineers of medical systems and lawyers expert in regulations (a task which was beyond our possibilities), to establish requirements for transparency we started from the existing literature. By reviewing works in other domains for similar requirements, we collected existing requirements potentially applicable in health care. After having searched our sources for what engineers discuss about medical systems and understood their concerns about transparency, we critically discussed, systematically selected, and completed a preliminary requirement list, before delivering our list of final requirements.

3.1 Requirements establishment

To compose our final list of requirements we proceeded in six steps (see Figure 3.1):

1. *Definition of sources*, where we review the literature in other domains searching for potentially applicable-to-transparency requirements, and where we collect papers that discuss technical features in medical systems that directly or indirectly address transparency;

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 categorize our preliminary list of requirements according to whether they provide information or mechanisms, to whether they concern privacy, accountability, or other security properties, and to whether they are ex ante or ex post;

4. *Refinement*, where we review the requirements questioning their relevance in the healthcare domain;

5. *Grouping/rewriting*, where we group similar requirements, rewrite and restyle them;

6. *Revision*, where we review our requirements on the light of the two openness properties: transparency, and empowerment.

The following sections describe the six steps in details.

3.1.1 Definition of sources

Our sources are papers and projects that mention transparency as a goal or as a subject of research, as well as papers and projects about medical data security. In addition to the works we found while exploring transparency and its related properties

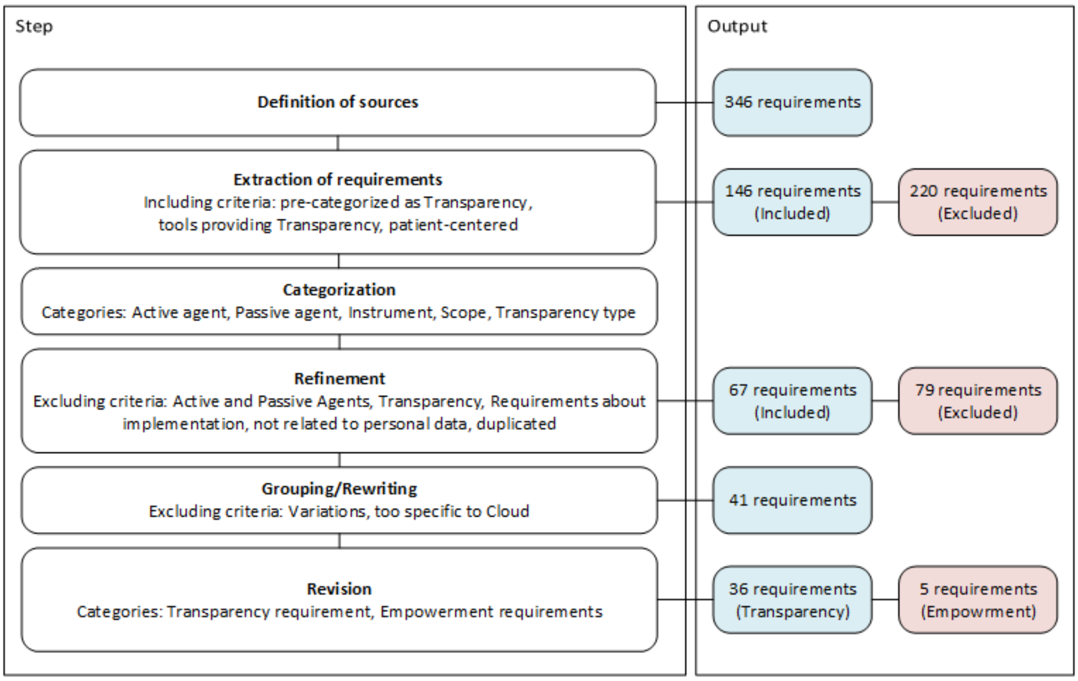

Step
Output
Definition of sources
346 requirements
Extraction of requirements
Including criteria: pre-categorized as Transparency, tools providing Transparency, patient-centered
146 requirements (Included)
220 requirements (Excluded)
Categorization
Categories: Active agent, Passive agent, Instrument, Scope, Transparency type
Refinement
Excluding criteria: Active and Passive Agents, Transparency, Requirements about implementation, not related to personal data, duplicated
67 requirements (Included)
79 requirements (Excluded)
Grouping/Rewriting
Excluding criteria: Variations, too specific to Cloud
41 requirements
Revision
Categories: Transparency requirement, Empowerment requirements
36 requirements (Transparency)
5 requirements (Empowrment)

FIGURE 3.1: Our second phase's 6 steps (left); No. requirements retained/rejected (right).

(see chapter 2), we selected others by searching for "transparency" and "privacy" to find works discussing transparency but not necessarily in healthcare, and others more by searching for "security," "privacy", and "medical data", to find articles in healthcare that discuss properties linked to transparency. The choice of keywords is justified by the findings presented in section 2.1: *privacy* seems to be the property that most relates to transparency. Because of that, from such generic keywords we expected to find works in healthcare discussing solutions that provide some level of transparency according to the definition elected here (see Definition 1) without addressing it directly. We also searched through papers cited in articles that survey the topic [183, 203].

We have found several publications on transparency, the majority belonging to the EU project A4Cloud (`www.a4cloud.eu`). Two deliverables of this project [44, 153] comment 346 requirements for accountability. They are listed after several interviews with professionals, among which data protection experts. We decided to use this project's deliverables as our main source, since the requirements that they provide form a superset of potentially interesting requirements. To this, we added six papers (i.e., [4, 17, 89, 103, 192, 205]), discussing technical features for medical systems that match our definition of transparency.

3.1.2 Extraction of requirements

Because we had both a list of already well stated requirements for cloud computing and six scientific articles discussing security in medical data sharing systems, we set two different criteria for extracting requirements:

1. To select from the list of requirements those that were already tagged *transparency*: this because the requirements coming from the A4Cloud project where already labelled using combinations of accountability attributes, among which "transparency".

2. To identify sentences describing operations that patients are able to do, or are allowed to do, or have the right to do, as well as tasks executed by the medical system that concern a patient's records and affect the patient's right over them (e.g., break the glass and delegation of access rights).

By applying the first criterion we sieved a total of 126 requirements. The second criterion is meant to discern mainly patient-centred requirements. Words such as *can*, *should*, *might*, and *must* helped us spot key sentences. We extracted additional 20 requirements for a total of 146 requirements, written according to the RFC2119 to indicate the requirement levels.

3.1.3 Categorisation

The requirements resulting from the previous step have been classified according to six attributes that remind the syntactic categories used in the description of a requirement: "The [*Active Agent*] must/should/may provide a [*Passive Agent*] with an [*Instrument*] for a [*Scope*]". *Agents* are data providers, medical systems, consumers, data owners, the patients or a data broker. *Instrument* are pieces of information or mechanisms that realize the "being transparent" in respect to a *Scope*, for instance compliance to policies, accountability, auditability. A further attribute, *Transparency Type*, specifies the requirement be ex ante, ex post, or other.

3.1.4 Refinement

We refined the set of requirements by removing:

1. *Requirements where the Active Agent is not "data provider"*, since data provider is (the subject managing) the medical data sharing system, the role we intend to let provide transparency;

2. *Requirements where the Passive Agent is not the consumer*, since we are interested in requirements about data providers (medical systems) and data consumers (patients), excluding requirements about other roles not relevant or uncommon in the medical domain, such as data brokers;

3. *Requirements that are not about ex ante or ex post transparency*;

4. *Requirements about implementation*; and

5. *Requirements that are not about personal data*.

We adopted the terminology suggested by the A4Cloud to define the Cloud provider and the EHR systems as *provider* and users or patients as *consumer*. Here we considered the requirements that were not explicit about the agents, allowing the interpretation the that the provider is the Active agent and the consumer is the Passive agent. We also removed duplicates. We had duplicates since the two lists considered as source are not independent, and because some of the concerns expressed in medical data sharing works are in common. This step reduced the pool of 146 requirements to 67 requirements (53 from A4Cloud and 14 from healthcare literature).

3.1.5 Regrouping/Rewriting

We clustered the requirements according to our categorization. We did so to discover requirements that are in fact variations of the same concept expressed with slightly different words; in this case, we merged those variants into one new requirement. In this process we also identified and excluded requirements that were meaningless in healthcare, mainly because tailored specifically to cloud computing. Finally, we removed requirements that were mere specializations of others, leaving only those most general; they implicitly embrace the special cases. After this step we were let with an initial list of 41 requirements.

3.1.6 Revision

After having concluded the definition of our transparency taxonomy we reviewed our requirements and classified them accordingly. At this point we abandon the categories presented in subsection 3.1.3, which was formulated with the goal of aiding in the manipulation of numerous requirements. Our taxonomy is much more fitting to the presentation of the requirements studied here.

One of the consequences of this revision is the reclassification of 5 requirements. Because transparency and empowerment are strongly coupled properties, in our initial list of requirements some empowerment requirements were included. Five of these were not captured by the previous stages of our requirements establishment process. They were initially classified by us as related to transparency, and reclassified at this stage. Our final list is composed by 36 transparency requirements.

3.2 Transparency requirements for Medical Systems

Tables 3.2, 3.3, 3.4 and 3.5 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 3.2, 3.3, 3.4 together compose ex ante and ex post transparency as depicted in Figure 2.5.

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

TABLE 3.1: Category codes: attribute (left) and Value (right).

As requirement identifier, we gave a numerical code inspired by the Dewey Decimal Classification [168]. It relies on the attributes: *type*, the transparency type; *property*, the property in the taxonomy the requirement relates to; and *instrument*, what is being provided to the patient. Table 3.1 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 property, and the units represents the instrument. Requirements in the same class are distinguished by adding decimal ciphers to the code.

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.[1]	Ex post	Information
221.5	S must inform P if and when data is gathered, inferred or aggregated.	Ex post	Information

TABLE 3.2: Availability requirements (S =medical system; P =patient).

3.2.1 Availability requirements

Availability requirements are mainly regarded in terms of providing information, and serve both transparency types. However, they mostly contribute to the ex ante notion. We present the availability requirements in Table 3.2.

Availability contributes to the notion of ex ante transparency because EHRs 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.

[1] According to GDPR Article 33, notification must be provided within 72 hours after having become aware of the incident.

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
211.8	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 3.3: Verifiability/auditability requirements (S =medical system; P =patient).

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

TABLE 3.4: Accountability 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 3.5: Empowerment requirements (S =medical system; P =patient).

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

TABLE 3.6: Quality requirements (S =medical system; P =patient).

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

3.2.2 Verifiability requirements

Verifiability contributes only to the notion of ex post transparency, and is composed by requirements providing information and mechanisms (see Table 3.3 and Table 3.4). 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.

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.

3.2.3 Empowerment requirements

Table 3.5 shows requirements that were initially classified as related to transparency, and later, in our *revision* step, were assigned to empowerment. These requirements 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. This is a viewpoint we share with the presented by Meis and Heisel in [149]. In that work, the authors explore aspects of empowerment (under the name of intervenability), addressing aspects such as the right to data portability, the right to be forgotten, and the right to object. We refrain from exploring further the property of empowerment.

3.2.4 Quality requirements

As presented in section 2.3, we found in the literature properties that help improving the quality of transparency, those are referred as quality requirements [238]. We list three of such requirements in Table 3.6.

Usability and privacy emerged while we browsed the literature for definitions of transparency, they were presented and discussed in section 2.3. 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. A similar reasoning is also defended in [149] with regard to intervenability. For these reasons we decided to included it as a desired quality.

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

3.3 Discussion

It is generally difficult to have a complete list of requirements and our is not an exception. We know, for instance, that we overlooked technical requirements regarding *how* to implement transparency. We did so intentionally, since we aimed to identify the non-functional rather than the technical features supporting transparency as a property. But even if we have restricted the discussion to non-functional requirements it is unrealistic claiming we are complete; yet at the best of our efforts we believe we did not missed any important requirement.

One can question that, while selecting our sources, we did not searched broadly enough. We searched for "transparency", "security" and "privacy", which we think are very general terms. In the General Data Protection Regulation (GDPR), transparency is frequently related to security properties meant to give the users feedback on their private data. So, for instance, even though we overlooked *accountability* or/and *auditability*, being them more specific than security and privacy, we indeed harvested works on those topics too. And, as we comment in chapter 2, in medical systems, *privacy* is the property more likely to be related to with transparency solutions.

One could also question that the best way to achieve completeness is to discuss with engineers working with medical systems and with health care professionals. We did not, for instance, organised group studies, or interviews, or workshops with medical professionals because we did not have the resources for this kind of activities. However, even interviewing health care professional has its own limitation: professionals although using medical systems may not be familiar, or just have a non-professional understanding of terms like privacy, security, and transparency; moreover there is no assurance that a population of specialist's answers can lead to complete set of requirements. We instead chose to rely on previous studies (A4Cloud), who in their turn had the resources to organise workshops with different stakeholders. The original list of 346 requirements that we "borrowed" from A4Cloud did emerge from a workshop. Where precisely those professional figures were asked for requirements also about transparency in the context of cloud computing. Moreover, we also extracted requirements from works debating patient-centric desirable features on medical systems.

Besides, to build a list as complete as possible, we decided to add three quality requirements to our pool, exploring human aspects (usability), transversal security aspects (preserving privacy), and fairness aspects (knowledge of existence). They all capture better the spirit of transparency. We have thus indirect reason to believe that we have not missed much.

A similar argument gives us some guarantee about the relevance of our selection of requirements. However, although we chose carefully our sources, we cannot verify the relevance only by looking at the data we have. But, at least, if relevance is intended with respect to our definition of transparency (see chapter 2), we have some insurance because of our methodology: its selective and its integrative steps were conceived to be compliant with that definition. However, if relevance is intended with respect to regulations, our methodology may not be sufficient to give full guarantee: it only gives best compliance with what we have found in the literature. Reaching legal compliance is a very difficult task in general, usually reached by compliance to standards; there are no standard yet for transparency. Even the GDPR, which promotes transparency as one of its driving principle for data protections, is not clear on the matter and, as far as we know, there is an alive discussion about how to be compliant to it. Our requirements constitute a reasoned first proposal that should be followed by discussions with health care specialists, patient associations and, regulators.

Chapter 4

Metrics for Transparency

The legislation on data protection in the European Union (GDPR) places emphasis on ensuring high quality of data processing service. It proposes principles intended to serve individuals and to guarantee that their personal information is processed "lawfully, fairly and in a transparent manner."[1]. In particular, transparency is not only regarded as essential for data processing, it is also a way for service providers to build and preserve trust. Providers that are transparent on their data privacy policies and practices, express them in a clear and readable manner, and have easily-accessible documents and histories of processing operations can have a better chance to gain and maintain their client's trust and stay in business.

But how can transparency be modelled and implemented, and how to measure the amount of transparency that a system guarantees? And, as a consequence, what degree of presumption of compliance to the GDPR's principle does a service ensure?

Although the GDPR does not give any precise and detailed definition of transparency, its Recital 39 explains that "transparency requires that any information and communication relating to the processing of those personal data be easily accessible and easy to understand, and that clear and plain language be used", and that "natural persons should be made aware of risks, rules, safeguards and rights in relation to the processing of personal data and how to exercise their rights in relation to such processing."[2]. Such statements do qualify transparency somehow but, purposely, GDPR's descriptions are meant to concern heterogeneous perspectives and thus are stated to leave room for interpretation. The means to adhere to the principle of transparency thus can vary depending on *e.g.*, the type of service, the data being processed, and the class of individuals whose personal data it processes. All those means can hardly be understood unless the principle is clearly and operationally defined.

A step in this direction has been attempted by the EU Article 29 Data Protection Working Party (WP29). In April 2018, it has published a document about practical guidance and interpretative assistance on the new obligation of transparency[3]. The document comments on the GDPR's articles that refer to the principle (Art. 12, 13, 14, 15-22, and 34) and highlights what categories of information must be provided to data subjects, in which manner and by using which tools. It also explains on what qualities, called elements in the document, should the provided information and communication satisfy (e.g., conciseness, intelligibility, easy accessibility, free of charge).

[1] GDPR, Article 5.1(a).

[2] *Ibid.* (39)

[3] Article 29 Working Party - Guidelines on transparency under Regulation 2016/679, WP260 rev.01, 11 April 2018.

These guidelines are certainly helpful but yet they do not indicate a best practice that one can follow to implement the principle; no tool-kit has been proposed that can help verify the quality of transparency of a data service.

This chapter presents a viable way to achieve this goal by following a Requirements Engineering (RE) approach. Here we present a well-defined methodology that guides us to identify a list of ten fundamental functions whose role is the evaluation of transparency. We also discuss what aspects of the non-functional requirements they are expected to measure and how operatively one can apply them, focusing on what evidence one needs to collect and how to be able to calculate the output values. Finally, we present a way of interpreting the output obtained when applying these metrics. The interpretation is based on Evaluation Assurance Levels (EAL) [42], it considers the quality factors of transparency to define 4 Transparency-EALs. To exemplify the evaluation process we show, step by step, how to calculate the metrics to assess transparency on the Microsoft HealthVault. Lacking any comparative analysis, this assessment exercise is not meant to suggest any judgement on the quality of transparency and on the legal compliance of that particular service, but rather it serves as an example of how to apply the metrics on a real system and of how to visualize of the result. Two appendices aid the understanding of this process: Appendix A describes in details how to compute each metric, the description is given in a series of tables, formatted according to the indications in the ISO/IEC 27004 standard; and Appendix B presents the results of the evaluation of Microsoft's system.

4.1 Related works

Transparency is a multi-faceted non-functional property. It has been defined in terms of *availability*, *auditability*, *accountability* and *verifiability* (see chapter 2). Availability is the property of ensuring that users are able to obtain and use, whenever they need it, information about the processing of their personal data; auditability is the property that allows users to audit what happened to their personal data; accountability enables users to monitor the usage of their data and hold a person accountable in case of misuse[4]. Auditability and accountability are specialization of verifiability, which in turn ensures that it is possible to check whether specific propositions hold on a system's execution.

The multi-faceted structure that characterizes transparency makes modelling and measuring it a challenging task. Conventional modelling and measuring approaches are not suited to represent its peculiarities, while *ad-hoc* methodologies proposed to model transparency (e.g., see [45, 149]) focus only on specific related properties (e.g., empowerment, accountability), serve only certain domains (e.g., cloud computing), or cover the problem only partially (e.g., modelling but not measuring).

To approach the problem systematically, one could express transparency in terms of Non-Functional Requirements (NFRs), then looking for "non-functional" metrics [122]. Unfortunately not all NFRs can be expressed in terms that allow them to be easily measured [79, 228]; if this practice has to be followed, it requires a dedicated discussion. For this task, one could refer to the IEEE Standard 10601-1998 [107], which defines a methodology for defining metrics in general, and then follow the suggestions in [117] to reason about the validity ("What Do They Measure and How Do We Know?") of a set of metrics.

[4] Under the GDPR, the data controller is legally accountable; nevertheless accountability aims to identify actual responsibilities e.g., after the violation of a privacy policy.

In the context of NFR measurement and assessment, another standard of relevance is the ISO/IEC 27004 [109]. It has been conceived to define how to fulfil requirements for information security management systems, but it has been built with broad approaches and concepts so it can be applied to different organizations and contexts. In here we refer to these standards to propose a methodology to measure how much a system fulfils requirements for transparency.

Except those works and documents about metrics in general, little can be found on measures for transparency. In software design for control applications, metrics for transparency have been indeed discussed but in relation with net based algorithm. In a transparent algorithm "it is easy and clear to see what the controller does in the moment and what it will do in the next steps" [72]. Such notions and the relative metrics are very much customized measure the net traffic in terms of signal in input and outputs, and are hardly applicable in our context of services for data protection.

A possible quest for metrics for transparency may look at the factors that have been proposed to qualify transparency. For instance Sullivan *et al.* [227], while studying requirements for trust and other *trust-terms*, describe transparency as an attribute that requires the *observability* of several types of *data* concerning the users. In our work, these trust-terms correspond to the attribute *instrument* (see chapter 3). No metric is discussed but it indicates the terms to be considered when defining a criterion to measure transparency.

Metrics for transparency exist in eGovernment [241], where transparency is discussed as a means of assessing accountability and qualified for efficiency, effectiveness and accessibility of the volume of information that public administrators provide to users. Such concepts provide valid suggestions for metrics, despite none of them is expressed formally.

There are also other relevant works on the properties composing transparency. Accountability, for example, has been systematically analysed [73] proposing a Unified Modeling Language (UML) meta-model for defining metrics. This model helps reasoning on complex properties, structuring them into more basic ones whose metrics are simpler to define. Though designed with the purpose of measuring accountability, the model is not strictly tailored for it and can be generalised for other properties. In comparison with other works proposing approaches to express requirements based on Model-Driven Engineering (MDE) techniques (e.g., [15, 51]), the one presented in [73] seems to be the most fit to model transparency. We refer this model here.

4.2 Methodology

The process of defining metrics was conducted in two steps. Initially transparency was decomposed into elements that describe what attributes a quality implementation should present. Based on those, fine-grained metrics were defined. This step was conducted based on the methodology presented in the IEEE standard 1061 [107]. Later, by reviewing the meta-model proposed in [73] for transparency, we validated those previous metrics and enriched them giving a more solid justification grounded on a MDE approach. The two methodologies have their peculiarities, but have proven to be compatible.

The process followed by the IEEE standard first operates at a higher level, requiring to identify the quality *factors* and quality *sub-factors* that contribute to establishing transparency. The second phase consists in assigning metrics for those more fine-grained qualities. The standard also suggests five steps that should be followed to define software metrics: 1. establish requirements, 2. identify metrics, 3. implement the metrics, 4. analyse them, and finally 5. validate them.

The MDE approach proposed in [73] focuses on how to establish requirements and identify metrics, corresponding to steps 1 and 2 of the standard. The various facets of transparency are represented in a meta-model (see Figure 4.2 and Figure 4.3), where properties are divided into smaller and less abstract elements. The meta-model is completed by evidences, i.e., the elements a user can observe in a system, and that confirm the proper implementation of the property in study. Metrics are then designed to measure the evidences, hence the importance of this part of the meta-model.

In general, both methodologies propose three main activities to be performed when defining metrics: 1. partitioning transparency into less abstract elements; 2. selecting attributes that contribute in establishing those elements; 3. defining metrics for those attributes. In the following, we describe how these activities were conducted.

4.2.1 Partitioning transparency

Transparency is a multi-faceted concept, and assigning it a metric directly would end up in a very coarse assessment. Instead, following the suggestion of the two methodologies, we first identify the elements that contribute to establishing transparency. In line with the IEEE standard, we call those elements factors. The search for factors that help defining transparency does not present any difficulty. As stated in chapter 3, implementing transparency means providing information and mechanisms. These are the *instruments* required to achieve transparency. Partitioning those factors even further required a review of the literature on software qualities and NFRs [31, 40, 135, 241]. Four major sub-factors appear relevant: accessibility, informativeness, understandability, and validity. The first three refine both factors, whereas the last one refines exclusively the “providing mechanisms” factor.

Accessibility, here in the sense of “being easy to obtain”, is a quality that refers to both categories of instruments. Since the instrument expresses the act of providing something, it must be easy for a user to obtain it, regardless of whether its source is information or mechanisms. *Informativeness* concerns the ability of conveying a good quality of information, and helps understanding the excellence of any piece of information provided (including the ones provided through the use of a mechanism). *Understandability* represents the ability of “achieving a comprehensible meaning”, exploring the linguistic quality of an instrument. *Validity*, here in the sense of “being precise and producing the correct result”, is linked with the provision of mechanisms, and defines how sound the mechanism is in doing its job. Figure 4.1 summarises the selected factors and sub-factors.

For the sake of simplicity, transparency is discussed and modelled with regard to five requirements, specifically the ones shown in the excerpt contained in Table 4.1. Even though this set may seem small, the requirements were carefully selected. Examples of each type of information-based and mechanism-based requirements, and the relevant characteristic for selecting metrics, are shown. The first three requirements demonstrate how to attain to the transparency sub-property of *availability* by providing *information* (111.10, 111.13 and 211.3), while the last two entail a *mechanism* for the transparency sub-properties of *auditability* (222.1) and *accountability* (232.1) respectively.

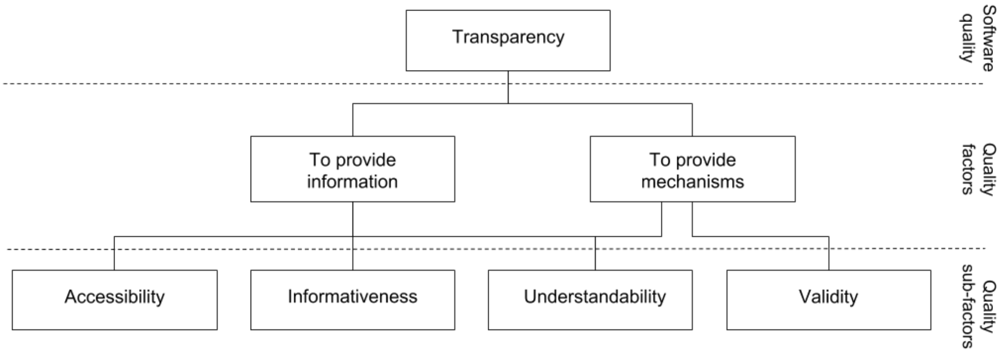


FIGURE 4.1: Transparency and its factors and sub-factors.

ID	Description
111.10	*S* must inform *P* about who is responsible for handling owned data.
111.13	*S* must inform *P* on how to protect data or how data are protected.
211.3	*S* must notify *P* in case the policy is overridden (break the glass).
222.1	*S* must provide *P* with audit mechanisms.
232.1	*S* must provide *P* with accountability mechanisms.

TABLE 4.1: Excerpt from the Transparency requirements.

The meta-model in the MDE approach correlates several elements: *Property*, *BaseProperty* and *CompoundProperty*, which are the objects under study; *Goal*, the high-level description of the property; *Entity*, the subject responsible for realising the property; *Action*, representing what is executed by, or has an effect on, the entity; *Evidence* and *EvidenceProcessing*, the tangible and observable elements of the property; *Criterion*, a constraint to what should be measured; and *Metric*, *BaseMetric* and *CompoundMetric*, representing a quantitative assessment to measure the property.

In the meta-model, the process responsible for collecting and processing the evidence is as important as the evidence itself. Hence, another evidence is proposed in association with each process to explain how it works. We slightly adapt this in our work. We accept that a requirement may be implemented in several different ways, depending on the business model of each system. However, regardless of the actual implementation, the bottom line is that the user must be able to observe the evidence in the system. This approach is alike to the software engineering technique of black-box testing, whose purpose is to test a piece of software in the absence of any knowledge of its internal structure, and based solely on the observation of its inputs and outputs [16]. Since this approach was not completely aligned to what is defined in the original meta-model, we slightly adapted it. This is referred throughout this paper as the "black-box approach" and is further explained in section 4.2.1.

Another adjustment we did is regarding elements *Goal* and *Criterion*. We do not adopt a goal nor a criterion at this point to leave the possibility of exploring all the possible facets of transparency. These elements may be modelled at a later stage, in order to select a portion of transparency requirements needed in order to achieve a goal, or to constrain the measurement to a specific context (e.g., relevant regulations, or standards).

In the following, we present how the elements proposed in the original meta-model are interpreted and adapted to transparency in medical systems. Figure 4.2

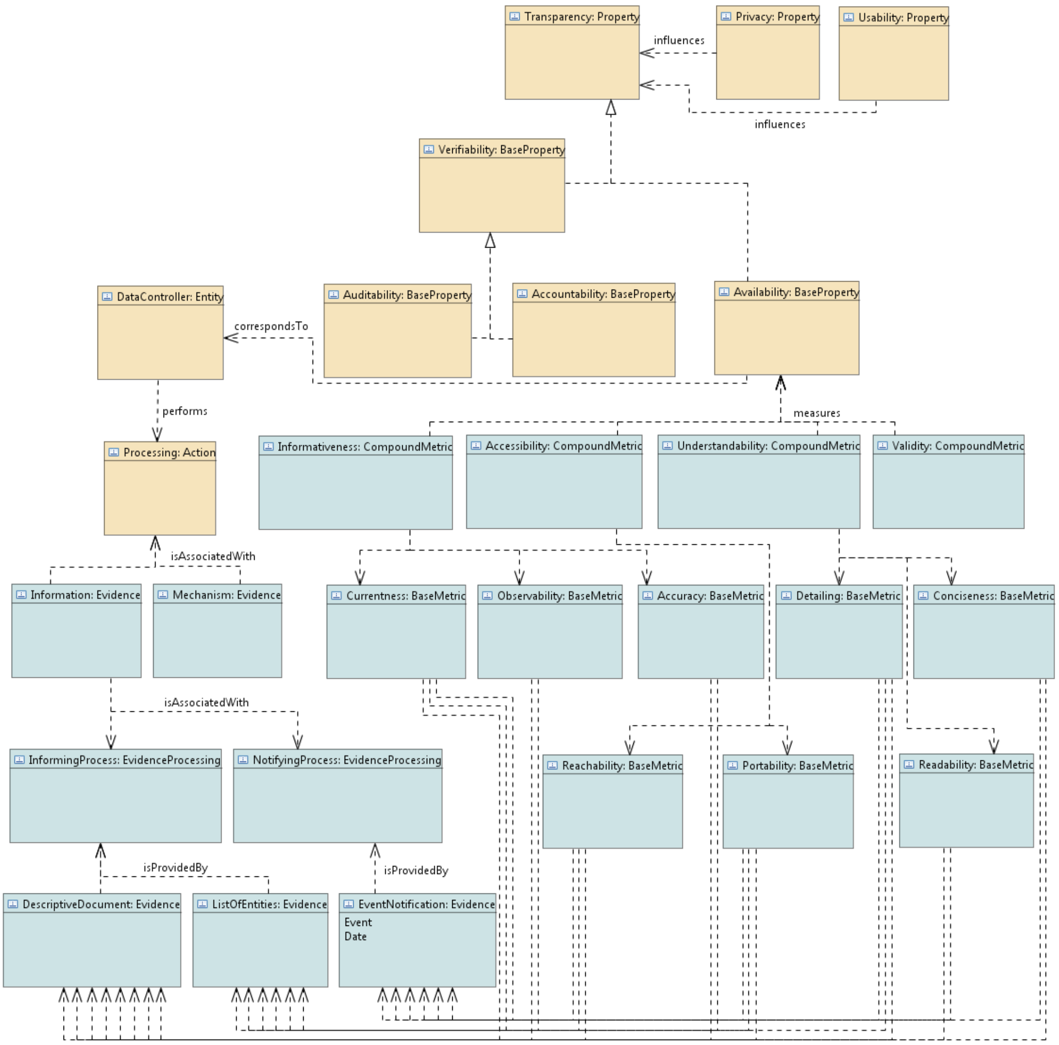


FIGURE 4.2: Model of availability requirements.

shows the model for availability. However, since the requirements are all information-based and were selected in a way to represent every possible evidence, the model can also generically be used as a basis for the model of any other information-based requirement. Similarly, Figure 4.3 contains the model for auditability, but as these requirements are highly representative for the mechanism-based family, and all evidence is represented therein, therefore any other mechanism-based requirements can be modelled in a similar way. Elements in yellow are common to the two models.

Properties

The central component of these models is the *Property* that is being described, specifically *Transparency*. Its composing sub-properties are *Availability*, *Auditability*, *Accountability* and *Verifiability*, and are represented by classes inherited from *BaseProperty*.

In addition to transparency, two other properties are presented in this model: *Privacy* and *Usability*. They have been introduced as secondary properties that need to be considered in order to provide a fair transparency, as they might influence it.

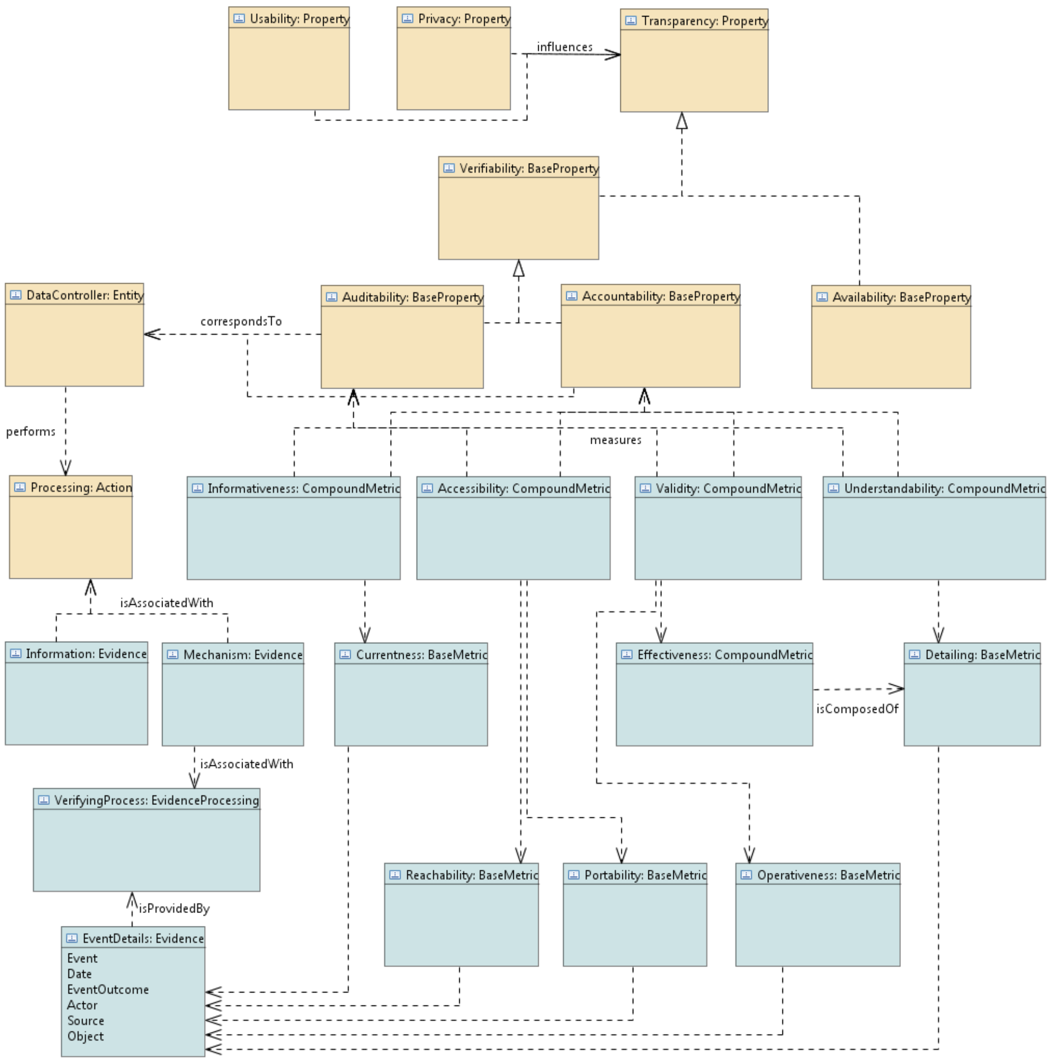


FIGURE 4.3: Model of auditability and accountability requirements.

However, even in a condition of very low privacy and usability, the system may not fail to be transparent (see chapter 2). The two properties are, therefore, not analysed in the perspective of defining transparency metrics.

Entity and Action

The actuation on the properties rests on the *Entity* element. An entity also performs, or is affected by, an *Action* that happens over a period of time. As transparency aims at sharing knowledge with users about how a system processes their personal data, and the system is managed by a data controller, *DataController* and *Processing* components are used. Here, *data controller* may be interpreted as the *Controller* in the GDPR.

Evidences and Evidence processing

The characteristics of each requirement are represented by the *Evidence*, which captures the elements a user can observe with respect to the property of interest. Transparency is a high-level concept, difficult to observe and measure. However, whenever the requirements for transparency 111.10, 111.13, and 211.3 are properly implemented, the users must have access to pieces of information regarding the processing of their personal data. In other words, a sufficient amount of information provided to the user serves as a possible indicator that a system is actually transparent. Consequently, in the first model we present (see Figure 4.2), the *Information* class is the evidence associated with the *Processing* action. The same holds for the transparency mechanisms. A system that complies with 222.1 and 232.1 must give users access to some sort of mechanism to verify how their data have been processed. In the second model (see Figure 4.3), this is represented by the evidence class *Mechanism*, and by the associated evidence processing class *VerifyingProcess*.

The *EvidenceProcessing* class brings into the model the fact that the evidence, although associated with the action performed by the entity, is not produced by it. In the first model, *Information* is evidence of the fact that the *Action* of data processing is undergoing, but it is generated by other processes, which are solely responsible for informing and notifying the user. These processes are represented by the *InformingProcess* and *NotifyingProcess* classes.

According to the black-box approach described previously, the analysis is centred on the evidence itself, rather than on the process that collects the evidence. For example, in the requirement 111.10, "*S* must inform *P* about who is responsible for handling owned data", the important aspect is that users are informed about the entity responsible for handling their data. It does not matter if the data controller displays a list in the system highlighting who is responsible, or if it sends to the users an e-mail with the name of the person in charge of their data. Therefore, the focus of the analysis is on how well this information is able to satisfy the requirement. The association *isProvidedBy* between the *EvidenceProcessing* and *Evidence* elements emphasises this, describing in more detail what type of information is provided by each process.

Requirement 111.10 is about providing information to the users. A simple list of the people responsible for data processing should be enough for this requirement to be fulfilled. Requirement 111.13 demands that the user be informed about the protection of data. It is impossible to abstractly specify how this information looks like, but in any case it needs to describe the policies of the data controller, so it will be in the format of a descriptive document. Finally, requirement 211.3 asks for notification whenever an extraordinary event (e.g., "break the glass") happens. As it does not specify any further details, a simple notification about the occurrence of the event and the date when it happened is enough to fulfil this requirement. The *ListOfEntities*, *DescriptiveDocument* and *EventNotification* components represent the evidences in those requirements.

To further discuss the *Evidence* and *EvidenceProcessing* elements presented in the second model, we first need to clarify the interpretation of auditability and accountability we adopt here. In the domain of medical systems, auditability and accountability are commonly interpreted as properties about access control (e.g., [71, 125, 235]). As such, they allow the users to monitor how and by whom their data has been accessed, used, and modified[5]. The concepts of "access", "usage" and "modification" are interpreted in this work as the basic actions for persistent storage: CRUD (create, read, update and delete). In the following, auditability and accountability will be regarded as mechanisms with respect to those actions.

As each requirement may be implemented in several different ways, depending on the business model of the system implementing it, the analysis is based on the evidence they produce (the black-box approach). The question, then, is how the evidence of auditability and accountability mechanisms should be structured.

RFC 3881 [147] defines the format and minimum attributes that need to be captured in order to provide auditability and accountability for health systems. This document describes the data to be collected for four different events, including events and actions that happen to patient's data. It states that the system should document "what was done, by whom, using which resources, from what access points, and to whose medical data". On this basis, the mechanism's output should contain the following event details, as abstracted in the evidence class *EventDetails* in Figure 4.3: description of the action performed; time of the event; whether the event was successful or not; who performed the action; where the action was performed (user interface, application, etc.); the data that suffered the actions.

4.2.2 Selecting quality attributes

Building on top of previous NFR literature, we search for suitable qualities that define the elements previously identified and presented. As an assistance for this task, we first build a questionnaire whose goal is to clarify how to decide when a quality is to be considered satisfied.

The questionnaire that we used to find out how to assess whether or not each quality is satisfied is reported in Table 4.2. We defined the questions on the basis of the definitions and descriptions found while exploring the literature. To maintain a high level of granularity, where necessary, questions are partitioned into sub-questions.

Quality	**Question**	**Sub-question**
Accessibility	1. Is the system making the instrument available?	1.1. Is the system providing an instrument that can be used whenever needed?
	2. Is the system providing portable information?	2.1. Is the system providing information that can be used in different environments?
		2.2. Is the system providing information that can be extracted in different formats?
		2.3. Is the system providing information that can be accessed through different means?
Informativ.	3. Is the system providing accurate information?	3.1. Is the system providing consistent and flawless information?
	4. Is the system providing up-to-date information?	4.1. Is the system providing timely information?

[5] The interpretation adopted here also seems to be the one followed by ISO/TS 18308:2004 [110], in particular section 5.4.6.

	5. Is the information consistent to what the user experiences?	5.1. Is the system providing information that can be observed in the system by the user?
	6. Is the system providing unbiased information?	
Understand.	7. Is the system providing the minimum possible information for the understanding of the matter? 8. Is the system providing enough details on the information for the understanding of the matter? 9. Is the system helping the user to understand the information provided?	
	10. Is the system providing clear and neat information?	10.1. Is the system providing information using the terminology appropriate to the area? 10.2. Is the system providing information that does not use jargon?
Validity	11. Is the system providing correct and precise mechanism?	11.1. Is the system providing ways to verify a mechanism? 11.2. Is the system providing mechanisms that can be tested by experiment or observation? 11.3. Is the system providing a mechanism that reaches the goal for which it has been provided? 11.4. Is the system providing the source code of the mechanism?

TABLE 4.2: Qualities questionnaire. The questions in grey cells have led to metrics

4.2.3 Defining metrics

Not all of the questions correspond to some metric. Questions whose answer may vary depending on the user's perceptions or that are context dependent, such as question 6 and 10, have been disregarded. Instead, questions that admit objective answers (the grey boxes in Table 4.2) have been assigned metrics to measure the corresponding factors and sub-factors. As a consequence, the metrics we propose here are based on quantitative analysis.

One may advocate that qualitative analysis have the advantage of capturing nuances of human perceptions, and allowing for dynamic settings. And as such, may be perceived as a natural choice for the medical domain. However, qualitative analysis have the advantage of providing reliable and objective measurements. Thus

Compound	Metric	Description
Accessibility	Reachability	How easy it is for a user to reach an information or mechanism.
	Portability	How easy it is to transfer and use an information or mechanism in different systems.
Informativ.	Observability	How much of the information provided can be observed by the user in the real process of the system.
	Accuracy	How consistent and correct the information provided is.
	Currentness	How up-to-date the information or the result provided by a mechanism is.
Understand.	Conciseness	How straightforward is the information.
	Detailing	Whether the information is detailed enough for the general understanding of its subject.
	Readability	How easy it is for a user to read and understand a text.
Validity	Effectiveness	How satisfactory the mechanism provided is.
	Operativeness	Whether the mechanism functions and produces an appropriate effect.

TABLE 4.3: Metrics for information-based requirements.

enabling software engineers to have an objective assessment of the quality of transparency in early stages of development, and accommodating for *transparency-by-design*. The metrics are discussed in details in the following.

The original model classifies metrics into two types: *CompoundMetric* and *BaseMetric*. The first models metrics that are defined in terms of other metrics, while the second actually uses the evidences for the calculations. As discussed previously, when measuring the quality of transparency implementations, there are four factors that need to be taken into account: *Accessibility*, *Informativeness*, *Understandability* and *Validity* [217]. The four factors are represented as compound metrics in this work. Whenever the data controller declares to have provided some kind of information to the users (including through the use of a mechanism), that information is expected to have the following features: 1. users must be able to easily obtain it (accessibility); 2. it conveys the precise knowledge (informativeness); 3. it is expressed in a comprehensible meaning (understandability). Mechanisms provided to the users should also 4. be precise and provide correct results (validity).

Ten metrics (represented in both models) were defined to measure the quality of information-based and mechanism-based requirements. *Reachability* and *Portability* refer to the accessibility of the evidence. Observability, *Accuracy* and *Currentness* are related to the informativeness of the evidence. *Conciseness*, *Detailing* and *Readability* concern the understandability of the evidence. Finally, *Effectiveness* and *Operativeness* relate to the validity of the evidence. These metrics, and a short description for each, are summarised in Table 4.3.

By highlighting the specific pieces of evidence that are used to model transparency and its sub-properties, it is possible to refine the metrics and define which ones are suitable to be applied to each type of evidence. In particular, *Observability* and *Accuracy*, as metrics intended to observe and compare statements about the process and intentions of the data controller against its actual practice, are not suitable for measuring notification of events. That is because events are considered as extraordinary occurrences, such as overriding an access control policy, or a security breach. Since they are unexpected, the user might not find any further information (apart from the mere notification) to observe and compare them against. *Conciseness* and *Readability* are also not suitable for application to all kinds of information, as these metrics operate on a piece of information in the form of a text made up of sentences. As such, evidence in other forms, e.g., a list, might not be evaluated using those metrics. Conversely, metrics such as *Portability* and *Currentness* are shown to be suitable for measuring the results of a given mechanism, even though they were originally thought for information-based requirements.

4.3 Metrics

4.3.1 Reachability

This metric measures how easy it is for a user to reach a given instrument, if reachable at all. To measure the reachability $\mathcal{R}c$, we first define N_{int} as the number of interactions the user needs to perform to reach the desired instrument. An interaction is considered as any action the user must perform, such as typing, clicking, tapping, sliding, etc. Reachability applies to any sort of information or mechanism the system provides, and we define its metric as follows:

$$\mathcal{R}c = \begin{cases} 1, & \text{if } 0 \leq N_{\text{int}} \leq k \\ e^{(1-\frac{N_{\text{int}}}{k})}, & \text{if } N_{\text{int}} > k \end{cases} \tag{4.1}$$

Here k is the maximum number of interactions that is considered acceptable for reaching the instrument. Equation (4.1) reaches the maximum value 1, whenever the number of interactions needed is less or equal than the deemed acceptable. From that point on, the degradation is exponential in the number of interactions. This metric has been updated from the one originally presented in our previous work. The changes we propose here are so that reachability scores the maximum grade 1 for any number of interactions smaller or equal than the considered as acceptable.

As many possible implementation for transparency mechanisms are acceptable, it may not be trivial to identify when a mechanism is reached. In this work, we suggest a mechanism is considered in place whenever users can reach its output, even if a tool or plug-in is not visible to them. As such, the reachability of the mechanism is measured considering the number of interactions until its output is reached.

4.3.2 Portability

This metric measures how easy it is for an information to be transferred and used in different systems. To measure portability, we reused the popular classification provided by the 5 star open data [18], which is a scheme for rating the degree of structuredness of data on the web. It is a model that uses an incremental scale from 1 to 5. To measure how portable an information is, we need to verify whether the properties described in each scale are implemented. We adapted the scale and normalised it to our context as shown in Equation (4.2).

$$\mathcal{P} = \begin{cases} 0, & \text{if no information available} \\ 0.2, & \text{if available in any open format} \\ 0.4, & \text{if available as a structured data} \\ 0.6, & \text{if available in a non-proprietary format} \\ 0.8, & \text{if uses URI} \\ 1, & \text{if based on linked data} \end{cases} \tag{4.2}$$

This metric can also be applied to transparency mechanisms, by considering the mechanism's output. It measures to which extent the mechanism provides information that could be easily used in other systems.

4.3.3 Observability

This metric measures how much of the information provided can be observed by the user in the real process of the system. Observability is a metric derived from our previous Accuracy metric. In here we split it in two metrics: observability that captures the amount of information that can be even observed in a system, and accuracy which now tests only the observable information for its consistency and correctness. This modification makes the transparency evaluation more fine-grained. To measure observability, we must first define what is considered a statement. Statements are going to depend on the nature of the information, but we suggest that at least claims and affirmations about what the system is or does should be considered. A representation of the system's process (for example, a model such as a business diagram) might also be considered, as it may help in the assessment of observability.

Each statement should be linked to some part of the process the user can observe. If it is not possible to link the statement, either because it is not present, or because it is dubious, then the information should not be considered observable. The result is the proportion of linked statements. If LS is the number of statements that can be linked to some parts of the process, and NLS is the number of statements which do not correspond to a specific part of the process, then observability $\mathcal{O}b$ can be expressed as shown in Equation (4.3).

$$\mathcal{O}b = \frac{LS}{LS + NLS} \tag{4.3}$$

4.3.4 Accuracy

This metric measures how consistent and correct the information provided is. Accuracy builds on top of the observability metric. To measure it, we must consider only the observable statements identified for that purpose.

Each observable statement should accurately describe some part of the system's process. If the statement contains information that is either incorrect, or that is dubious because it is inconsistent to what the user experiences, then the information should not be considered accurate. The result is the proportion of accurate statements. In particular, if LS is the number of observable statements, and ALS is the number of statements which accurately describe a specific part of the process, then accuracy $\mathcal{A}c$ can be expressed as shown in Equation (4.4).

$$\mathcal{A}c = \frac{ALS}{LS} \tag{4.4}$$

4.3.5 Currentness

Currentness depends on the time that passes between something happening in the system and the system providing information about it. More specifically, if t is the amount of time that the system has taken to inform about the change, and t_{max} is the amount of time that represents the maximum acceptable delay (i.e., the ideal time) for updating that piece of information, then currentness is measured as shown in Equation (4.5).

$$\mathcal{C}u = \begin{cases} 1, & \text{if } t \leq t_{max} \\ 2^{-\left\lceil \frac{t-t_{max}}{t_{max}} \right\rceil}, & \text{if } t > t_{max} \end{cases} \tag{4.5}$$

In other words, anything that takes less time than what would be deemed an acceptable delay for that information has $\mathcal{C}u = 1$.

It should be noted that while some pieces of information should be updated in a matter of minutes or hours (e.g., information on security breaches), for others a longer time would be acceptable (e.g., results of a research with patients). The maximum acceptable delay t_{max} is highly dependent on the nature of the system and the type of information that must be updated, and must be carefully chosen for each case. Likewise, the acceptable delay should be the same for similar services offering the same information. A poorly chosen delay will result in inaccurate currentness values.

The ceiling function in the exponential simplifies the metric by providing discrete values. Let us consider an example in which a piece of information is extremely relevant, for instance because it concerns a security breach, and the maximum acceptable delay is defined as one minute ($t_{max} = 1$). If the system takes one hour ($t = 60$) to update the information, then the currentness is $\mathcal{C}u = 2^{-59} \simeq 0$. On the other hand, if the acceptable delay in providing an information is 30 minutes, then this can be used as the time unit, and the currentness is $\mathcal{C}u = 2^{-\left\lceil \frac{60-30}{30} \right\rceil} = 2^{-1} = 0.5$. This metric has been updated from the one originally presented in [217]. In here, we adapt the variable names for more suitable ones, and we apply the ceiling function to distinguish between information provided under the maximum acceptable time delay t_{max}, and information provided in the time range $t_{max} \leq t < 2t_{max}$. The present version of the currentness metric produces a smaller grade for the second case.

This metric can also be applied to transparency mechanisms, by considering the mechanism's output. It measures how up-to-date the information provided by the mechanism is.

4.3.6 Conciseness

The conciseness metric measures how straightforward an information is. We measure the conciseness of an information in terms of the average number of words per sentence. The scales of this metric are based on recommendations for the English language. While [47] suggests that the average length of sentences should be between 15 and 20, it is stated in [85] that an average of 5 to 8 words per sentence can be read by people with moderate learning disabilities, and that by using common words it is possible to help all users to understand a sentence with around 25 words. For this reason, we use a Gaussian curve $N(\mu, \sigma^2)$, with a mean $\mu = 20$ and a standard deviation $\sigma = 5$, as expressed in Equation (4.6). However, we normalise this function so that its maximum value is one. The resulting formula for measuring the conciseness is shown in Equation (4.7). Here ASL denotes the average number of words per sentence, and it is calculated as N_W / N_S, where N_W is the total number of words, and N_S is the total number of sentences.

$$N(\mu, \sigma^2) = \frac{e^{-\frac{1}{2\sigma^2}(x-\mu)^2}}{\sigma\sqrt{2\pi}} \tag{4.6}$$

$$\mathcal{C}o = \sigma\sqrt{2\pi}N(\mu, \sigma^2) = e^{-\frac{1}{50}(ASL-20)^2} \tag{4.7}$$

We understand that conciseness is not only about short sentences, and that semantics analysis should be considered too. What is presented here, however, is an easy-to-calculate approximation for syntactic straightforwardness.

4.3.7 Detailing

This metric describes a strategy for measuring whether an information provided is detailed enough for the general understanding of its subject. Detailing is measured by checking if the main crucial details are present in an information that the system provides. The crucial details will vary from information to information, but we suggest that, at least, basic questions should be answered, such as: what? who? why? when? to whom? which? and so on. The information provided has to be cross-checked with the questions, and the result is a matrix of details provided versus important details. The metric $\mathcal{D}$ is the proportion of important details provided.

The detailing matrix should be constructed in such a way that only the questions pertinent to a given piece of information are counted towards the proportion. For example, assuming the system must inform the users on how their data are stored and who has access to them, questions like “why [is the data accessed]?” and “when [was the data stored]?” are not pertinent.

If n_I is the number of pieces of information provided, and m_Q is the total number of detailing questions, the detailing matrix has a size of $n_I \times m_Q$. For each piece of information $i = 1 \ldots n_I$, there will be a number P_i^D of questions pertinent to the detailing metric, and a number $NP_i^D = m_Q - P_i^D$ of non-pertinent questions. The non-pertinent questions are not relevant and therefore do not count towards the metric. On the other hand, the pertinent questions can be partitioned into a number d_i of questions for which the details are provided, and a number u_i of questions for which details are not provided, such that $d_i + u_i = P_i^D$. Under these premises, the detailing metrics $\mathcal{D}$ can be expressed as shown in Equation (4.8).

$$\mathcal{D} = \frac{\sum_{i=1}^{n_I} d_i}{\sum_{i=1}^{n_I} P_i^D} = 1 - \frac{\sum_{i=1}^{n_I} u_i}{\sum_{i=1}^{n_I} P_i^D} \tag{4.8}$$

A highly-detailed system ($\mathcal{D} = 1$) will possibly answer all pertinent questions for each piece of information.

4.3.8 Readability

This metric measures how easy it is for a user to read and understand a specific text. There are several well-established formulas available for this purpose. Each formula has its advantages and there are no general recommendations or standards stating which one should be used in each case. To select the formula, we searched the literature to understand how to measure readability in the medical domain (the domain used for our requirements). The most used formulas are the Flesch-Kincaid grade level (FKGL), the Simple Measure Of Gobbledygook (SMOG), and the Flesch

Reading Ease (FRES) [57, 86, 119, 254]. FKGL and FRES are variants of the same method, and both use the average sentence length and the average word length as an input. SMOG is calculated using the number of long words (three syllables or more). We chose to use FRES for being the only one that provides the results in easiness grades.

As already introduced in *conciseness* metric, the average sentence length is measured as $ASL = N_W / N_S$, where N_W is the total number of words and N_S is the total number of sentences. Similarly, the average number of syllables per word is $ASW = N_{SY} / N_W$, where N_{SY} is the total number of syllables. The *FRES* can be expressed as shown in Equation (4.9). In theory, the higher boundary of the *FRES* is 121.22, which is achieved by applying it to a sentence with one word of one syllable, like "yes" or "no". There is no theoretical lower boundary, but by applying the formula to long sentences with long words it is possible to reach huge negative scores. However, such extremes are non-realistic in the documentation of a system. The common interpretation of *FRES* considers scores from 0 to 100 only [70]. As a measure of the readability metric $\mathcal{R}$, we consider the bounded and normalised *FRES*, as shown in Equation (4.10).

$$FRES = 206.835 - (1.015 \times ASL) - (84.6 \times ASW) \tag{4.9}$$

$$\mathcal{R} = \begin{cases} 0, & \text{if } FRES < 0 \\ \frac{FRES}{100}, & \text{if } 0 \leq FRES \leq 100 \\ 1, & \text{if } FRES > 100 \end{cases} \tag{4.10}$$

4.3.9 Effectiveness

This metric measures how satisfactory the mechanism provided is. By decomposing the mechanism into evidences, effectiveness can be defined in terms of the mechanism's output. This metric partly overlaps with the previously-defined *Detailing* metric. In other words, a mechanism is effective if the output it provides contains enough details to understand whether and by whom the personal data has been accessed and used (i.e., the goal of the mechanisms in requirements 222.1 and 232.1). As a consequence, in the model *Effectiveness* is a compound metric element by the *Detailing* base metric.

The strategy is very similar to the one presented in Equation (4.8). Effectiveness is measured by checking whether the goal of the mechanism is being reached. The goal varies according to the requirements, but similarly we suggest that the output of the mechanism addresses at least basic questions, such as: what? who? why? when? If n_I is the number of pieces of information provided as the output, and m_Q is the total number of questions, the effectiveness matrix has a size of $n_I \times m_Q$. For each piece of information $i = 1 \ldots n_I$, there will be a number P_i^E of questions pertinent to the effectiveness metric, and a number $NP_i^E = m_Q - P_i^E$ of non-pertinent questions. The pertinent questions can be partitioned into a number e_i of questions whose goal is reached, and a number v_i of questions whose goal is not reached, such that $e_i + v_i = P_i^E$. Under these premises, the efficiency metric $\mathcal{E}$ can be expressed as shown in Equation (4.11).

$$\mathcal{E} = \frac{\sum_{i=1}^{n_I} e_i}{\sum_{i=1}^{n_I} P_i^E} = 1 - \frac{\sum_{i=1}^{n_I} v_i}{\sum_{i=1}^{n_I} P_i^E} \tag{4.11}$$

Even though detailing and effectiveness are calculated similarly, the two metrics are differentiated because they give different insights about the quality of a transparency instrument. That happens because the transparency mechanisms we consider in this work intend to provide non-textual information to end users, i.e., data. If data provided by a mechanism is detailed enough for the understanding of a given subject, this is an indicative that the mechanism is adequately accomplishing its purpose. In this case, the same reasoning applied in detailing metric can be applied in support to determine a mechanisms' effectiveness. On the other hand, for textual information this reasoning does not hold. The fact that information is detailed is not sufficient to determine its effectiveness with regard to the understanding of a subject. Matters such as reading ease have to be regarded as well.

4.3.10 Operativeness

Something is said to be operative if it is functioning and "producing an appropriate effect"[6]. This metric proposes a strategy for defining whether or not a mechanism is operative. It is inspired by the black-box tests of the audit type [212] and uses the technique of equivalence partitioning [160]. It consists in partitioning the input domain of a mechanism into equivalence classes, in such a way that it is reasonable to assume that testing a value in a given class is equivalent to testing any other value in the same class. In this context, the equivalence classes are based on the actions executed in the system that a mechanism should process, and the test consists on executing these actions and observing the output to verify if they were processed by the mechanism.

For requirements 222.1 and 232.1, a reasonable set of equivalence classes can be the CRUD actions. This set of equivalence classes can be expressed as $E = C \cup R \cup U \cup D$, the union of all possible actions, where C contains create actions, R contains read actions, and so on. To measure operativeness, a sub-set of actions $A = \{a_0, a_1, \ldots, a_{k-1}\} : (A \subseteq E)$ containing at least one action of each equivalence class (i.e., $(A \cap C \neq \emptyset) \wedge (A \cap R \neq \emptyset) \wedge (A \cap U \neq \emptyset) \wedge (A \cap D \neq \emptyset)$) must be selected and tested. The test consists in verifying if the actions were correctly processed and reported in the mechanism's output. If one action is not reported, or it is not possible to verify (e.g., deceptive or inconsistent information provided as output), the entire test fails. In particular, if the set of actions A contains k actions, and the number of actions that can be verified is represented by n, the operativeness $\mathcal{O}_A$ can be expressed as shown in Equation (4.12). The notation of this metric was slightly adapted from the originally presented in our previous work.

$$\mathcal{O}_A = \lfloor n/k \rfloor \tag{4.12}$$

The operativeness metric presents a strategy to rationally reason about a mechanism's functioning, without delving into subjective aspects, such as whether or not the mechanism's output conveys satisfactory knowledge. This metric is conservative, meaning that it considers that one counter-example is enough to show that a mechanism is not properly functioning (this is represented by the floor function in Equation (4.12)). A result of 1 can be interpreted as an indication that the mechanism has performed as expected, supporting and inspiring a sense of confidence. Nevertheless, it must be noted that the operativeness of a mechanism is always measured

[6] Definition extracted from the Merriam-Webster Dictionary.

with regard to one specific set of actions (here represented by A). The metric is therefore, always accompanied by the set of actions tested, lest the result be meaningless and the test not be replicable. Each equivalence class should be measured, so it is necessary to select at least one action from each of those. If it is not possible to select one action from a particular class, it means that it is not possible to verify that class, and the test should be considered unsuccessful. The metric is flexible and allows the evaluator to decide how to couple the actions into classes, so it is possible to decide on the granularity of the test. The most suitable equivalence classes and granularity strictly depend on the peculiarities of the system implementing the mechanism. Discussing what classes can be the most appropriate for a specific system is outside the scope of this work.

4.4 Measurement

The measurement methodology presented here is based on the process of monitoring, measurement, analysis and evaluation proposed in ISO/IEC 27004 standard [109]. This standard is intended to assist organisations in the evaluation of an information security management system for the fulfilment of requirements defined in another document of the series (ISO/IEC 27000). However, all the documents in the series are produced to be broadly applicable. In here we consider the steps that can be reused in the context of medical data, and adapt the process to measure the transparency of systems handling such data.

The following subsections reflect the three parts of the measurement process depicted in Figure 4.4. They are composed by processes suggested in the original standard. We explicitly mention in the text where significant alterations were made.

4.4.1 Definition of goals

Before starting the analysis of a system, the goals of the measurement must be defined. This process is represented by the first lane of the *Measurement* pool in Figure 4.4. This task should not be done unilaterally by the requirements analyst (whether internal or external). The administrator of the system under analysis should also be duly notified and, whenever appropriate, included in the definition of goals. This task should be executed to ensure the fairness of the measurement activities. We refer to the interested parts (the analysis team and the system administrator) as the stakeholders.

Prior to the analysis itself, the ISO/IEC 27004 standard suggests to identify the data collection and analysis tools. In our context, we suggest this task should be realised in two steps. First, the stakeholders should select the transparency requirements to be analysed. The measurement procedure we propose is flexible, and can accommodate any combination of requirements. It does not mandate all requirements to be measured at the same time.

After selecting the requirements to be measured, the second step of identifying data collection and analysis tools is to determine the metrics suitable for measuring each of those requirements. To this end, the transparency models depicted in Figure 4.2 and Figure 4.3 can be used. The association between the classes extending *BaseMetric* and the ones extending *Evidence* show which metrics are suitable to measure a given requirement. For instance, whenever a metric is associated with an evidence of the type *information*, this metric is suitable for measuring information-based requirements. This is also synthesised in Table 4.4.

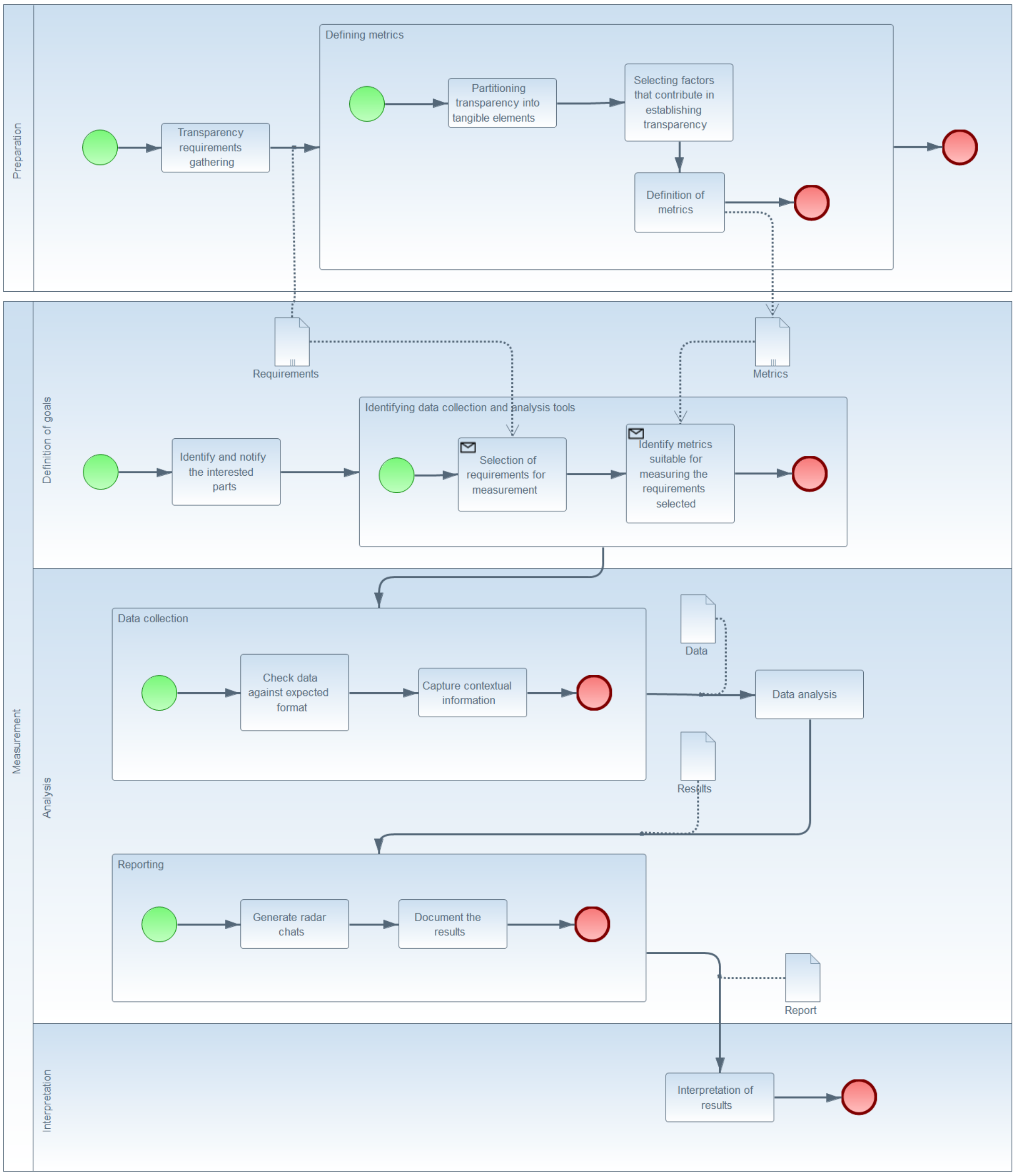

Preparation
Defining metrics
Transparency requirements gathering
Partitioning transparency into tangible elements
Selecting factors that contribute in establishing transparency
Definition of metrics
Measurement
Definition of goals
Requirements
Metrics
Identifying data collection and analysis tools
Identify and notify the interested parts
Selection of requirements for measurement
Identify metrics suitable for measuring the requirements selected
Analysis
Data collection
Check data against expected format
Capture contextual information
Data
Data analysis
Results
Reporting
Generate radar chats
Document the results
Report
Interpretation
Interpretation of results

FIGURE 4.4: BPMN representation of the measurement process.

Quality	**Metric**	**Information-based req.**	**Mechanism-based req.**
Accessibility	Reachability	✓	
	Portability	✓	✓
Informativeness	Observability	✓	
	Accuracy	✓	
	Currentness	✓	✓
Understandability	Conciseness	✓	
	Detailing	✓	
	Readability	✓	
Validity	Effectiveness		✓
	Operativeness		✓

TABLE 4.4: Metrics and the types of requirements they are suitable for measuring.

4.4.2 Analysis

The analysis procedure (represented by the second lane of the *Measurement* pool in Figure 4.4) starts with the data collection. For each requirement selected, it is necessary to collect the appropriate evidence (information, or the output of a mechanism). But the analysis of these evidences can only proceed if they are present in the system, in a specific format. For example, to measure readability, information presented in a textual form (natural language structured in periods and sentences) is needed. Other types of information cannot be measured by that metric. The expected formats were described throughout section 4.3, and are concisely presented in Appendix A.

In addition to the collection of the evidences, some metrics require further contextual information to be captured as well. Reachability, for example, requires the measurer to capture the amount of interactions the user needs to perform in order to find an information or mechanism's output. The contextual information needed for each metric has also been discussed in section 4.3, and it is similarly presented in Appendix A.

After completing both sub-processes of the data collection (checking data against expected formats, and capturing contextual information), the stakeholders have all the data needed for the data analysis itself.

The data analysis process represents the application of the suitable metrics to the data collected regarding each of the selected requirements. At this stage, the measurer should apply the mathematical formulæ as specified in the previous section. This procedure will generate several results that should be reported in a structured way.

Each requirement measured in the system will result in a set of grades. Although normalised and aligned on the same ranges, the metrics proposed are heterogeneous and cannot easily be combined into a mathematical expression that can clearly measure transparency as a whole. Instead, we adopt a benchmarking strategy, where each of the proposed metrics serves to assess the performance of one or more of the factors that determine the transparency quality. The benchmark can be represented as a radar chart (as shown throughout Appendix B).

Finally, a document containing all the results should be generated. In this document, all requirements should be presented accompanied by their respective radar charts. In order to avoid ambiguity it is necessary to specify whenever a metric could not be applied (e.g., for lack of access, or incompatible data formats). This clarifies the difference between metrics that grade the minimum from metrics that could not be measured. Whenever a metric (e.g., operativeness) requires additional information for its interpretation, this information should be presented together with the radar chart. Additionally, two general radar charts can be appended to summarise the transparency measurement of the system. One chart should display the average of grades achieved by metrics applied to information-based requirements, while the other displays the same for mechanism-based ones. An example of reporting document can be found in Appendix B.

4.4.3 Interpretation

The result of transparency evaluation should be interpreted similarly to a performance benchmarking, in which several transparency quality factors and sub-factors are tested and evaluated in a system. These factors can be later used to compare different systems, provided the evaluation is done with regard to the same set of requirements and with the auxiliary metric parameters for all systems.

The transparency benchmark can also serve in support to *assurance levels*, similar to the Evaluation Assurance Levels (EAL) proposed in the Common Criteria standard [42]. The standard supports an objective evaluation of the security requirements implementation. Each evaluation is conducted in a system with regard to a specific set of requirements called the *security target*. The standard defines 7 levels of confidence. At each level, the rigour of tests realized in the system is increased, providing a greater assurance that the requirements are in fact reliably implemented. However, these levels do not measure how secure the system is, they rather state the level of tests executed.

In our context, EAL can be adapted to represent how thorough a system has been tested with regard to transparency. If the set of transparency requirements selected for evaluation (see subsection 4.4.1) represents the target, the level of assurance can be defined with regard to the metrics used to evaluate them. In here we propose 4 Transparency Evaluation Assurance Levels (TEAL), based on the quality factors identified in section 4.2.

TEAL1 is applicable when confidence that the information and mechanisms referred to in the target requirements exist in the system is desired. **Accessibility** metrics should be applied, as they test whether information (or mechanisms' output) provided to the end user can be obtained, and used;

TEAL2 is applicable when confidence that the information and mechanisms referred to in the target requirements are of good quality is desired. In addition to Accessibility metrics, **Informativeness** metrics should be applied as well, as they test the excellence of the information (or mechanisms' output) provided, and how adequate they are when delivered to the end user;

TEAL3 is applicable when confidence that the information and mechanisms referred to in the target requirements are comprehensible is desired. In addition to Accessibility, and Informativeness metrics, **Understandability** metrics should be applied as well, as they test syntactic and semantic aspects of the knowledge the information (or mechanisms' output) provided intends to pass;

TEAL4 is applicable when confidence that the information and mechanisms referred to in the target requirements are precise and correct is desired. In addition to Accessibility, Informativeness, and Understandability metrics, **Validity**

metrics should be applied as well, as they test how appropriate the information (or mechanisms' output) provided is with regard to its goal.

A TEAL can only be fulfilled when all metrics associated with that quality factor are applied for each requirement in the target, and the previous TEAL levels have already been reached. In addition, if a threshold is defined for each metric, a given level can also represent the quality of the implementation, rather than only the rigour in which the requirements were tested. The minimum acceptable grade for each metric cannot be generally defined, but it will depend on the context of the system under evaluation. We do not attempt to define target grades for our metrics, as this task is outside of the scope of our work, and is the target of future research directions.

Regardless of the context in which transparency is desired, the interpretation of these results should provide an insight on the factors and requirements that have room for improvement, and guide the way to a better transparency.

4.5 Use case

To test the applicability of our metrics we conducted a complete evaluation of transparency in Microsoft HealthVault (please refer to section 1.1 to recall more details). Out of the 36 transparency requirements, 15 were identified as implemented by Microsoft HealthVault, either fully or partially. Even though our evaluation was conducted methodically and carefully, we do not claim to have exhaustively searched for evidences of an implementation of transparency in Microsoft's system. Some requirements may have passed unnoticed in this process. We consider this tolerable as our goal is solely to test the applicability of our metrics.

Here we discuss the evaluation highlights of two transparency requirements: *111.17 – S must make available a document explaining the procedures for leaving the service and taking the data out from the service*; and *222.1 – S must provide P with audit mechanisms*. The first is an information-based requirement, and the second is mechanism-based. We also summarise the evaluation results by presenting the average of grades achieved per metric. The full report of the results may be found in Appendix B.

4.5.1 Information-based requirement

To implement the first functionality (111.17), HealthVault provides information about closing accounts in "Help", under the section "Your HealthVault Account" – "How do I close my HealthVault account?". Additionally, further information can be found in "How do I export and save health information from HealthVault?".

To measure *reachability*, we first need to define the maximum number of acceptable interactions k. For this example, we chose $k = 3$ based on usability best practices. In particular, the "three-click rule" is an unofficial rule in web design that defends the users should be able to find any information within three clicks. Even though there is evidence suggesting that the number of clicks is not the most impacting factor in user experience, the three-click rule is still regarded as a good usability practice (see [174]). To reach these information, users simply need to access the "Help" section available through the main page of the system. Then go to "Your HealthVault Account" and finally reach the section about leaving the service ("How do I close my HealthVault account?"). Conversely, the information on how to take data out of the service is not immediately presented, as the users need to access the details on how to export and save their data. Since the information is spread throughout more than one document, we consider for this metric the total amount of interactions needed to reach all the desired content, in this case: $3 + 1 = 4$. The reachability metric result in $\mathcal{R}c \simeq 0.71$.

Regarding the *portability* of the account termination statements, Microsoft's systems reaches the value $\mathcal{P} = 0.8$. Applying Equation (4.2), we have the following: the information is provided in HTML, an open format; since it is presented as HTML, it is also structured, and available in a non-proprietary format; the information is available on the web and can be accessed through a Uniform Resource Locator (URL), which is a subset of a Uniform Resource Identifier (URI). Although the statements contain a few links to other information that provide a better understanding, these do not provide access to external data sources and cannot be considered linked data.

To test for *observability* we considered both pieces of information and chose the main statements for each of those topics:

1. "Once your account has been closed, any information that you had stored in your account will be permanently deleted, although data may remain on our servers for 90 days."

2. "To delete your account: Sign in to HealthVault. In the upper right, click your name and then click Account settings. At the bottom of the page, click Close account. Carefully review the information on the page, then click Close my account."

3. "The exception is if there are other custodians of records in your account. In that case, you'll be notified at the time you close the account, and those records will not be deleted."

4. "You can export and save your health information in two ways: as a spreadsheet;"

5. "or as a CCR or CCD or HTML file."

6. "To save health information as a spreadsheet: Sign in to HealthVault. On the left side of the page, click the name of the type of information you want to save as a spreadsheet. You'll see the list view for that type of data. Click Export. In the browser message that appears, click Save. Your information will be saved in a spreadsheet format (.csv) that can be opened in Excel or other spreadsheet software."

7. "You can create a CCR or CCD with information from your HealthVault record, but keep in mind that CCRs and CCDs don't support all types of health information, so they won't necessarily contain everything in your record."

8. "To save information in your HealthVault record as a CCR or CCD or HTML file: Sign in to HealthVault. On the Home page, click Current and then click Export. Select the file format that you want to use. Select the type or types of information that you want to export. If you want to, select the date range for the data. Click Export. In the browser message that appears, click Save. Your information will be saved as a file on your computer."

Statement 1 is the only one that cannot be observed in the system by a user. Hence, observability metric reaches $\mathcal{O}b = 0.88$.

To test for *accuracy* we considered statements 2 to 8 (only the observable ones). Statements 2, and 4 to 8 could be easily verified, as for each of those the system contains areas available to the users. Statement 3, on the other hand, cannot be considered accurate. The information provided leads the user to believe the data with more than one custodian cannot be deleted, but this is not true. At the moment of the account termination the user is notified about the existence of data with more custodians, and the system allows the user to chose whether to delete these data or not. One may argue the information provided is also not false. However, when a user chooses to delete all data, it stays unclear whether the data shared with other custodians was also deleted to them, or if they were simply deleted from the user's account and transferred to the other custodians. Because this misunderstanding is caused by the information provided to the users, we consider it not accurate. As a result we have $\mathcal{A}c = 0.86$.

Microsoft HealthVault provides no information on how long they take to update the help section once something has changed in the system. We do not have enough information to calculate *currentness*. Thus currentness is not measurable without access to the internal system.

In average, sentences in the account termination statements are 14.91 words long, considerably less than the mean considered in the metric. In other words, these statements are rather succinct. This value, applied to Equation (4.7), provides a *conciseness* value of $\mathcal{C}o \simeq 0.59$. The *readability* of the account termination statements is slightly better. When applied to these statements the *FRES* formula results in 63.95; applied to Equation (4.10), it provides a readability $\mathcal{R} \simeq 0.63$.

The *detailing* metric can be calculated considering the purpose for which the information has been made available. In this case, the user must have access to explanations about leaving the service and taking data out of it. So the account termination statements, ideally, should help the users understand what to do to leave the service, and how to proceed to take the data out of the service. For this requirement, the information is already separated into two categories, which we identify through a three-letter acronym to simplify the visualization of the results: "How do I close my HealthVault account?" (CMA) and "How do I export and save health information from HealthVault?" (ESI). The detailing metric reaches the maximum score $\mathcal{D} = 1$, as all the desired details are provided by the statements.

	Delivered Details	
Desired Details	CMA	ESI
How to proceed to leave the service?	✓	▨
How to proceed to take data out from the service?	▨	✓

TABLE 4.5: Detailing matrix 111.17: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

4.5.2 Mechanism-based requirement

The second requirement 222.1 – "S must provide P with audit mechanisms" is implemented by Microsoft HealthVault by providing a way for users to consult the history of accesses and changes made on their data. They can see the changes made by one specific person or application, or even see the history of access rights granted. These functions are centralised in a section called "Record history", under "All changes in the last 6 months" (which we abbreviate as CLM in the following), and also "Views of User's record in the last 30 days" (shortened in VUR). We consider the combination of these two tools as the *audit mechanism* provided by HealthVault.

The section "Record History" can be accessed with one click from the main page, provided the user is already logged in the system. Users then need another click to access one of the two previously-mentioned tools, summing up to 2 interactions needed to reach each tool. Similarly to the way we calculated reachability for the previous requirement, here we also consider that the user reaches the audit mechanism after having accessed both tools, with a total amount of $2 + 2 = 4$ interactions. Considering the same parameter $k = 3$, Microsoft HealthVault reaches again the score $\mathcal{R}c \simeq 0.71$ in the *reachability* metric with regard to this requirement.

The *portability* measurement is also similar to what we did for the previous requirement. However, the audit mechanism scores $\mathcal{P} = 0.6$, less than the account termination statements. This happens because, while the information provided by the CLM tool makes use of URIs, this is not true for the VUR tool. Since the mechanism is partitioned into the two parts, we cannot consider the overall mechanism's output portable if parts of it do not reach the same portability level.

In this work we interpret auditability and accountability as properties related to access control. Hence, to measure *currentness* we need to define the acceptable amount of time (t_{max}) in which the system has to provide information about a data access, after it has happened. Ideally, such information should be available shortly after the action took place. Thus, for the effect of the calculations we define it is acceptable to take up to 10 seconds for the system to display the information: $t_{max} = 10s$. According to our tests, Microsoft HealthVault displays information on accesses immediately after they happened. From the user's perspective, it is very difficult to precisely calculate the amount of time taken until this information is available, as it is necessary to isolate other external factors that may be interfering with the time perceived, e.g., network delays. However, even considering the time taken $t = 5s$ (more than the time perceived in every test we did), with regard to requirement 222.1 Microsoft HealthVault still reaches the maximum grade $\mathcal{C}u = 1$.

In our example, we claim that HealthVault provides audit mechanisms by making a "Record History" available to its users. As discussed in section 4.2.1, for a mechanism to be effective in helping a user to audit the actions executed in his or her record, it requires means to check details such as: what actions happened in the system with regard to the user's data; when the action happened; whether the action was successful; from where the action was executed; and which data suffered the action. As seen in Table 4.6, HealthVault reaches four out of the five desired goals in the CLM auditability tool, but only three out of five in the VUR tool. Thus, the *effectiveness* metric scores $\mathcal{E} = 0.7$.

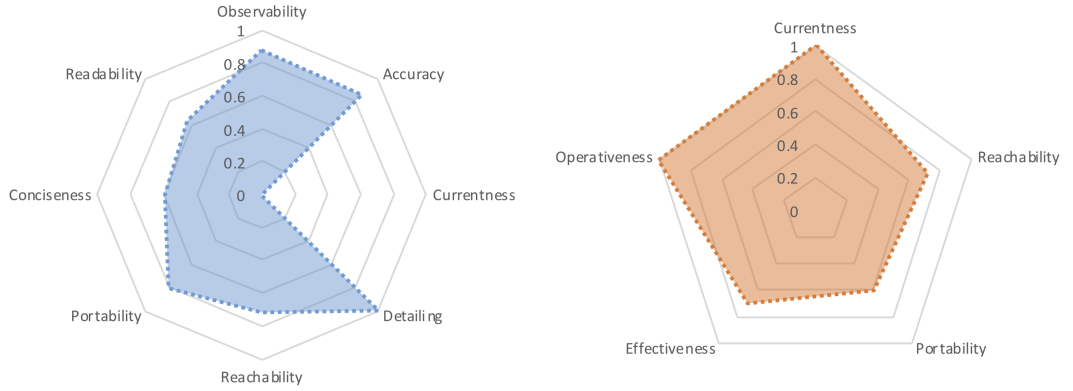
	Delivered Outputs	
Desired Goals	CLM	VUR
What is the action?	✓	✓
When did it happen?	✓	✓
What was the outcome?		
From what source/application?	✓	✓
Which data suffered the action?	✓	

TABLE 4.6: Effectiveness matrix 222.1: desirable goals compared with the real outputs. Greyed-out cells represent the non-pertinent goals.

Finally, to measure the *operativeness* of the HealthVault's audit mechanism, we first had to define the set $A = \{\text{createData, readData, updateData, deleteData}\}$ of actions to be tested in the system. For the effect of our study, we deemed it sufficient to test only one action per equivalence class. The test consisted in executing the actions in A, i.e., creating a personal record, reading a personal record, and so on; and checking if they were properly captured by the audit mechanism. As the test succeeded for every action executed, the audit mechanism reached $\mathcal{O} = 1$.

4.5.3 Summary

A summary of the results discussed previously is presented in Figure 4.5. The results for the first requirement (information-based) are shown in blue, and those for the second one (mechanism-based) are in orange.

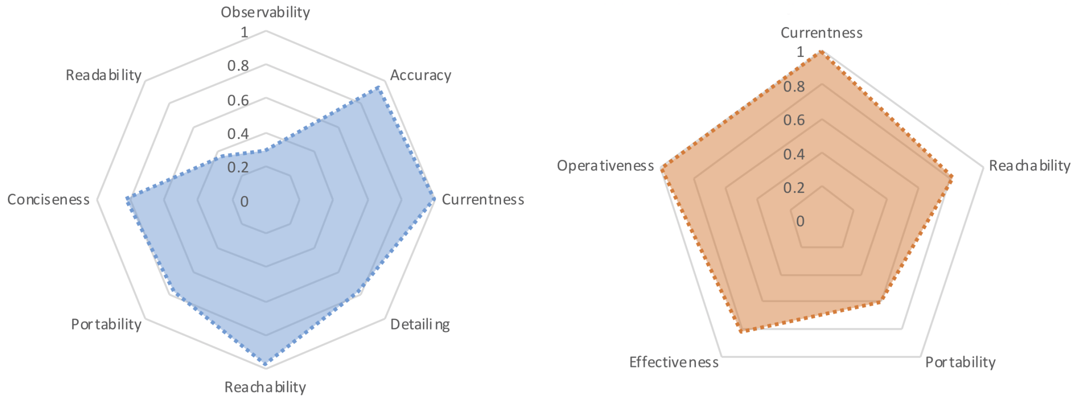


(A) Requirement 111.17.

(B) Requirement 222.1.

FIGURE 4.5: Examples of scores achieved by an Information-based and a Mechanism-based requirement.

The assessment of Microsoft HealthVault is presented in Figure 4.6. In here we consider the average of scores achieved by each requirement analysed. Non-applicable metrics are disregarded in the calculation of averages. Scores achieved by information-based requirements are shown in Figure 4.6a, whereas Figure 4.6b displays the scores for the mechanism-based ones.



(A) Information-based requirements.

(B) Mechanism-based requirements.

FIGURE 4.6: Synthesis of the transparency measurement in Microsoft HealthVault.

4.6 Discussion: on metrics' relevance and soundness

The GDPR discusses and presents transparency as a user-centric concept. This notion is supported in the guidelines by the WP29, which points out that "the *quality*, *accessibility* and *comprehensibility* of the information is as important as the actual content of the transparency information, which must be provided to data subjects." [10, paragraph 4]. Article 12 of the GDPR also sets the general rules regarding transparent information. It states that information must be *concise*, *transparent*, *intelligible*, *easily accessible*, and written in *clear and plain language*. All these concepts relate closely to the quality factors we explore in this work.

The same guidelines by WP29 offer interpretations to those concepts. According to the guidelines "concise and transparent" information should be understood as an information presented *efficiently* and *succinctly* in order to avoid information fatigue (paragraph 8). These concepts are captured by the conciseness, detailing and efficiency metrics. The concept "intelligible" means that information should be *understood* by an average member of the intended audience (paragraph 9). The guidelines suggest the level of intelligibility can be tested, among others, through *readability* tests. This concept clearly relates to our readability metric. The "easily accessible" concept means that the data subject *should not have to search for* the information, that how it can be accessed should be apparent (paragraph 11). For information provided in mobile applications, the guidelines suggest this requirement can be met by ensuring the information is never more than "two taps away". This concept closely relates to our reachability metric, which considers user interactions (including taps) in its formula.

Article 12 of the GDPR also states that information must be "in writing, or by other means, including, where appropriate, by electronic means". According to the transparency guidelines, written information should follow best practices for "clear and plain language". This includes having the information provided in a *simple* manner, *avoiding complex sentences and language structures*, and having *concrete* and *definitive* information (paragraph 12). These concepts are also captured by the conciseness and readability metrics. Regarding other electronic means, the WP29 recommends the use of *layered* privacy statements or notices whenever the data controller maintains a digital presence (paragraph 17), which is the scenario we consider in this work. The concept of layered information closely relates to the format in which information is presented, and our portability metric covers this aspect.

Articles 13 and 14 of the GDPR further add time constrains to the provision of information. Moreover, the guidelines suggest that providing information in a *timely* manner is a vital element of transparency and a fair processing of data (paragraph 27). These concepts are closely related to our currentness metric.

Another document is referred to by WP29 on best practices for clear writing [60]. This document suggests to follow the "7 questions approach" (What? Who? When? etc.) in order to determine if the relevant information is being covered in a text. This recommendation directly relates to detailing and effectiveness metrics. Also relevant to this work, it is suggested that a text should be short and simple, having 20 words per sentence on average. This is measured by the conciseness metric in our work, which also considers an average of 20 words per sentence on its formula.

The remaining metrics, e.g., observability, accuracy, and operativeness, do not have a direct correlation with transparency practices, as do the aforementioned ones. Yet they extrapolate the essence of the accountability principle, which requires the controller to *demonstrate* that processing happens in a lawful, transparent and fair manner (GDPR, Article 5.2). These three metrics assess how much of the information provided can be observed and tested for consistency with the real process of the system.

Our metrics have also proved to be sound when applied to a real use case. By conducting a complete assessment of transparency in Microsoft HealthVault, we demonstrate that our metrics are applicable to obtain a reasonable estimation of a system's transparency with respect to a specific set of desired requirements. Some of the results achieved in this assessment, however, may lead to a different conclusion. We comment on them next.

No requirement evaluated in HealthVault achieved the highest grade on *portability*. However, we do not believe this to be an indicator that our metric is unreasonable. To achieve the highest grade on portability, the information provided should be based on linked data, a principle not yet fully adopted by data controllers and providers (see [22]). However, linked data still represent the state of the art for portability of information. We expect to see some development in the area, especially in the light of the new right to data portability introduced by Article 20 of the GDPR, according to which data subjects shall have the right to receive data "in a structured, commonly used and machine-readable format".

Often, the *currentness* metric could not be applied to measure information-based requirements. This happens because of the lack of data regarding the time in which changes occurred in the system, preventing one to understand how timely the information is. However, this metric is justified by the timing requirements imposed by the GDPR. In the guidelines for transparency it is explained that providing timely information is crucial for transparency. Additionally, in light of the accountability principle, data controllers are required to "justify why the information was provided at the time it was" (paragraph 28). Even though this comment is made with regard to specific types of information, it demonstrates that our currentness metric is not measuring unrealistic aspects of transparency in a system.

Chapter 5

Private verification of access logs

Verification is, by the pure meaning of the word, “the process of establishing the truth, accuracy, or validity of something"[1]. Verifiability is regarded in literature as a property desired in many information systems (e.g., [52, 53, 128]). It is also presented as one of the properties composing the principle of transparency, which is said to promote accountability and to realize people’s right to privacy (see section 2.3).

In the medical systems domain, verifiability (also called auditability) has been explored with regard to access control (e.g., [71, 125]). Even though there are solutions proposed for verifying access of personal data in medical systems (e.g., [87, 89, 192, 206]), to the best of our knowledge, none do that while ensuring the details about patient’s information are kept confidential [87, 245]. In fact, according to Butin and Le Métayer [30], this is the most commonly used argument against verifiability in the context of personal data protection.

This chapter is dedicated to study the effects of privacy in aspects of transparency. In particular, we demonstrate how independent verifiability can be realized in a private fashion. We model an initial theoretical solution for detective compliance through verifiability in a patient-centred medical system. We use searchable encryption techniques for that. This solution allows for the access logs from medical system to be independently checked by a third party tool without leaking private information. It also protects the verification conditions by encrypting the queries executed by this third-party. Moreover, empowering users with the ability of privately checking compliance with access policies, helps supporting the confidence these users have in the system.

5.1 Aspects of Transparency and Privacy

The relationship between transparency and privacy is clearly troubled: transparency is a property related to disclosure of information, while privacy is often associated with confidentiality of information. If transparency is seen as the opposite of secrecy [173], transparency and privacy become contradicting requirements [208], and there should be a balance between transparent data access and the preservation of privacy [127].

However, transparency is still considered necessary to assert data ownership and privacy of users [205]. Transparency has been studied as a privacy goal, in the sense of increasing privacy awareness [150], and as a way of addressing users’ privacy concerns [100]. In fact transparency and privacy can still be conceptually realised if the information transparency intends to reveal is not the same that privacy intends to protect [19]. In particular, with regard to the interpretation we adopt in this work,

[1] Definition taken from the Online Oxford Dictionaries

helping patients understanding about their choices, the system's processes, the existence of entities which have access to personal data, and so on, can be done without leaking any sensitive data. That is the view point of the majority of our requirements (see chapter 3), they refer to transparency's sub-property of availability.

Instead, here we focus on requirements about the sub-property of verifiability, which pose more challenge to privacy. As verifiability is regarded as a property related to access control in the medical systems domain, realising it requires demonstrating that personal and private data has only been used in compliance with a given policy. This process may end up exposing the patients, as log on data access and usage itself reveals potentially sensitive information [100]. Allowing patients to manually verify compliance with policies is possible, and could potentially solve the friction between transparency and privacy, but is not ideal. It would overwhelm them with the technical charge.

A good verifiability solution in the medical domain should be *automatically executed*. To demonstrate good faith and commitment towards the fair use of personal data, it is also desired that medical systems allow the verification process to be executed *independently*. In a way that the patient can choose to trust the system with the verification task, or to execute it with an external auditing tool (e.g., a TET). However, those requirements are not easily achieved together with privacy. The independent verification requirement, while fostering the trust on the system may also become a privacy vulnerability to the the subjects involved if proper measures are not in place. *No personal and private information should be leaked* during the verification process, even if unintentionally.

5.2 Related works

A survey from Reuben et al. [188] classifies the existing automated audits for privacy compliance verification. They study several solutions and separate them according to their auditing goals. The authors highlight three main goals:

1. *Audit for ex post obligations* – which regards compliance with after-the-fact obligations that cannot be verified beforehand, e.g., mandatory deletion of data after a fixed amount of time;

2. *Audit for permitted exceptions* – which includes exceptional actions that happen in case of emergency (break-the-glass policies); and

3. *Audit for access legitimacy* – which intends to demonstrate compliance with the data owner's preferences.

Audits for ex post obligations do not necessarily imply on disclosure of personal data. In fact Butin and Le Métayer [30] propose a formal framework for verifying compliance in a privacy friendly way. They check compliance with data protection policies based on logs free of any personal data. However, they are not able to demonstrate compliance with access policies. They only verify properties such as “delete requests are fulfilled before expiration of request fulfilment delay", and “no personal data should appear in an abstract state after its global deletion delay has expired."

Audits for permitted exceptions and for access legitimacy pose more challenge for the privacy of personal and sensitive data. In most of the cases they mandate the analysis of audit logs, which contain information on *who* accessed *what kind* of information from *whom* [87, 245]. In here we intend to demonstrate how one could conduct these kind of audits in a private manner. For this purpose we show a model to automatically verify the latter (access legitimacy). Our scheme is capable of identifying accesses that do not match the user's preferences. Which can be later manually investigated for permitted exceptions (break-the-glass policies, for example). Automatic verification of permitted exceptions in a private manner would require a more in-depth study that is outside of the scope of this work.

In [87] authors point out security and privacy issues involved in making access policies and audit logs available in medical domain. They advocate that policies and logs, even though not containing personal and sensitive information (only references to it), may be enough for revealing details that should be kept private. Someone in possession of such policies and logs can gain knowledge of what kind of treatment a patient has received in the past, or what types of medical data are available. Authors advocate that by properly controlling the access to policies and logs it is possible to solve this privacy issue. They propose an adapted Information Accountability Framework [76] in which only the patient (data owners), medical professionals and medical authorities (e.g., government agency conducting audits) can access the policies and logs with restrictions according to their roles.

However, this work is not suitable to be applied to our context. In [87] independent auditing processes, one of our goals, are not considered. Even if this work was adapted to allow independent verification, the principle of privacy would still not be realised. External entities would still have access to more information than necessary to the purpose of verification. Restricted access control when applied in an uncontrolled environment (possibly insecure) does not suffice to prevent leakage of personal information.

While in [87] the confidentiality of sensitive information is realized only by controlling access to policies and logs, Walters *et al.* [245] propose a different solution for the problem: to operate on encrypted audit logs.

In [245], authors assume a scenario in which a system is being audited but the controllers of the system do not wish to share information from the audit logs with other entities. Similarly, the authors also believe it is possible to learn sensitive details about the system and the users by analysing the logs. For example, one can instantly learn what actions were conducted by a given user. The authors build an scheme for conducting searches in encrypted audit logs. For each log registered, the system should define a few keywords with which this log can be found. It then distributes searching capabilities for those keywords only to specific authorized persons. Each log is encrypted with a key that can only be retrieved by a person that possess searching capabilities for, at least, one of its keywords. Consequently, this scheme only allows authorized persons to decrypt the audit logs.

The audit process presented in [245] cannot be fully independent though. It relies on the system providing searching capabilities to the auditor for the given set of actions he or she can audit. Despite that, this scheme is also not in accordance with the privacy principle. In our scenario, in order to verify compliance with the patient's preferences the auditor would search for log entries matching the set of allowed actions and be able to decrypt them, in detriment of the patient's privacy. Ideally the external entity should not be able to decrypt, only learning whether or not a given log entry matches a search (and consequently is an allowed action) would suffice.

Two other works by Peeters, Pulls *et al.* propose a scheme for privacy-preserving transparency logging [172, 177]. The authors present a TET in the form of a cryptographic scheme that enables users to access logs of events that happened to their personal data. In [177], four main requirements shape the resulting scheme: 1. integrity of logs; 2. confidentiality of logs; 3. undistinguishable logs; and 4. unlinkable user identifiers. Their scheme allows for the storage of encrypted logs in a distributed fashion. Logs can only be accessed by the concerned users, and modifications to logged data cannot go undetected. In [172], the authors propose improvements to the original scheme to allow for publicly verifiable proofs of logs' author, time, recipient and message. The improved scheme combines concepts from authenticated data structures, forward key generation and secure messaging protocols to resist against stronger adversaries. While both works are comprehensive in addressing problems of confidentiality and integrity of logs, their goal is not to simplify the verification for compliance with policies. Their scheme allows only for manual verification of logs.

There are several other works that, similarly to the ones mentioned above, suggest schemes for privately processing personal data. The majority of those use searchable encryption techniques for that. In what follows we present the most relevant of those works while reviewing basic concepts of the technique.

5.2.1 Searchable encryption

Searchable Encryption (SE) techniques were initially introduced in the context of outsourced databases. With the growth of the amount of data generated, came an increasing need for outsourced options to store it. However, one cannot fully trust outsourced databases and may want to keep its data confidential. One possible solution to guarantee confidentiality involves encrypting the data before the storage on the database. Only the ones in possession of the key can decrypt it and learn its contents. However, denying the database access to the information increases the difficulty of performing queries and selectively retrieving data. Searchable encryption techniques try to approach this problem by allowing the database to execute queries on encrypted data.

Search on encrypted data was initially introduced by Goldreich and Ostrovsky [81], and Song *et al.* [216]. It is, to this day, an active research area with three main research directions [27]: to improve efficiency; to improve security; and to enhance the expressiveness of the search. Usually we see a trade-off between them. For example, guaranteeing a stronger *security* usually compromises the *efficiency*.

An important scheme based on searchable encrypted index was first presented by Goh [80] and later considered in other works (i.e. [32, 152, 170] and many others). For each encrypted data, keywords are extracted and those are used to generate an encrypted index. In the outsourced database scenario, the indexes are generated by the client and sent with the respective encrypted data to the database. Later, the client can send an encrypted query and the indexes will help the database/server to search over the encrypted data without the need of decryption. Indexes and queries should not leak information about the encrypted data, while guaranteeing that clients obtain what they are searching for.

There are specific techniques for searching on public key [24, 26, 78] and symmetric key [46, 80, 216] encrypted data. The last one is known as Symmetric Searchable Encryption (SSE). Several works presented solutions for searching single keywords [35, 46, 245]. Other schemes propose a search using more expressive keyword searches, such as conjunctions [25, 28, 82, 209], ranges [25, 209], or even dealing with keyword occurrence frequency [28]. This improves the expressiveness and security of searches, as opposed to perform several single-keyword searches and combining the results [152]. A few even more expressive schemes support general Boolean searches with conjunction, disjunction and negation of keywords in Disjunctive Normal Form (DNF) and/or Conjunctive Normal Form (CNF) [32, 66, 116, 129, 152, 170].

We demonstrate later that these works are of a special interest since it is possible to model our problem into queries in a Disjunctive Normal Form (DNF).

Symmetric searchable encryption are usually applied to scenarios where data owners want to query their own encrypted data stored in some third party server. In our work we propose the use of SSE techniques in a slightly different scenario, where data owners (patients) share their data with medical services and use SSE to independently verify accesses, while guaranteeing the confidentiality of their personal data.

It is necessary to note though, that we have a few different (and more relaxed) requirements in comparison to the conventional application of SSE in outsourced data storage. The first is related to the amount of data stored, searched and returned: while outsourced data applications may have to deal with large amounts of data, our application deals only with the event registers (logs) related to one specific patient (details in section 5.3). We assume these logs to be in a smaller scale. This implies that the use of SSE algorithms with non-optimal search time is not prohibitive in our application. Second, the patient already has access to all encrypted data and uses the verifier only for auditing. Therefore, if the search returns all the data, which is an expected result for the cases where no violation of the policy was made, we can save on communication and avoid returning everything again to the client, i.e., we can return just a positive message instead.

5.3 Technical aspects of Medical Systems

As discussed previously the term “medical systems" is broad and encompasses several types of systems with different goals: clinical data management systems, telemedicine systems, hospital information systems, pharmaceutical, etc. In this chapter we only distinguish those which are patient-centred. The goal of these systems is to allow the patient to be in control of the personal data being processed. Examples of patient-centred medical systems are Microsoft HealthVault[2], and the national Dossier de Soins Partagé[3] (Shared Care Dossier in English) from Luxembourg. The reader my refer to section 1.1 to review concepts related to these systems. From this point on we may refer to patient-centred systems simply as *medical systems*.

Generally speaking we can assume patient-centred medical systems to adopt a Discretionary Access Control (DAC) system [104]. In DAC systems the owner of a resource, in our case the patient, may grant or revoke access to other entities (users) based on their identities. We do not affirm that every patient-centred medical system implements DAC exactly as described in [104]. We just claim their access control method resembles DAC and could be modelled using it. For the sake of simplicity we assume discretionary access control policies as a set of fixed size clauses as shown in Equation (5.1), where id_i is the identity of the person authorized to realize an action $action_j$ on the patient's data.

$$\pi = \{(id_i, action_j)\} \tag{5.1}$$

It is, however, unrealistic to assume one access control system to be the perfect fit for every variation of medical systems. We do not attempt doing that. We instead chose to model our solution based on DAC systems to demonstrate that private verification can be accomplished even in systems implementing highly malleable and

[2] https://www.healthvault.com/

[3] https://www.esante.lu/portal/fr/espace-patient/le-dsp-au-quotidien,199.html?

granular access control mechanisms. We present arguments to endorse this claim in section 5.5. And later, in **??**, we discuss how our solution can also handle other types of policies richer in attributes.

Our simplified policy is only suitable to represent patient-centred medical systems though. In general these systems do not handle the definition of pre-conditions, post-conditions, obligations and other more complex policies that may be found in other types of medical system. To add more representativeness to the verification one could also explore revocation of access rights, which would mandate clauses to be time anchored. However, this is out of our scope. We restrict ourselves to the study of static policies and verification without temporal aspects.

Every action a person realizes on the patient's data, whether authorized or not, should be registered as an event in the audit logs. Similarly to how we defined the policies, we do for the register of events. We do not go into details on how they are in fact implemented because that may vary in different implementations. But according to a recent work [249] which surveys log files in the medical domain, it is reasonable to assume at least the following attributes would have to be registered in order to provide verifiability: 1. event identification (*action*) – the action performed; 2. date and time (t); 3. actor identification (*id*) – who performed the action; 4. object identification (*ob*) – the data that suffered the actions. Some standards are more complete and consider more attributes (i.e., RFC 3881 [147]), but in general these four attributes are commonly observed in medical systems [249]. We assume the register of events simply as the set of logs as displayed in Equation (5.2).

$$L = \{(action, t, id, ob)\} \tag{5.2}$$

5.4 Model description

As described in section 5.3, our scenario assumes a patient-centred medical system. Users of such a system should be able to verify whether their data has been accessed in compliance to the access policy. We assume three different players:

- **Medical System:** Stores patient's data, which can be accessed by its owner (the patient), and few predetermined professionals. This decision is agreed with the patient through an access policy.
- **Patient:** May want to verify if specific statements of the policy are being enforced, or search for possible violations.
- **Verifier:** Third party tool or mechanism responsible for verifying compliance of the medical system with regard to specific statements of the agreed policy.

Additionally, we also assume the ideal solution would take into consideration the following requirements:

- **Automated verification:** The medical system should provide means for the patients to avoid the overburden of manually verifying logs;
- **Independent audit:** Allowing a third party to verify compliance with privacy policies demonstrates good faith and commitment towards the fair use of personal data;

- **Privacy:** During the auditing, patients' privacy should be ensured – only the strictly necessary information to determine compliance should be disclosed. From this information one should not be able to infer any personal details about the patients.

Patients should access and be able to export logs of actions performed on their data. However, data and the logs are private and should only be accessed by its owner (the patient) and a few designated medical staff. Therefore, both patient and the medical system are interested on keeping communications confidential. We chose to encrypt data with a symmetric key that is only known by the medical system and the patient. Keys differ for each patient of the system.

Patients may require the logs related to their data to check if the agreed policy is being followed. They can decrypt all logs received and verify by themselves, or they have the option to execute this task with an independent verifier. For that, the patient simply redirects the encrypted logs to the verifier. Since the verifier does not have access to the key used for encryption, a (good) traditional symmetric encryption is enough to guarantee that this verifier will not learn any information about the events these logs represent. Finally, in order to allow the verifier to operate over the encrypted logs while protecting the patient's privacy, we propose the use of SSE.

5.4.1 Trust model

The medical system we model is assumed to be honest, but not trustworthy. In systems that implement break-the-glass, for example, the policy may be relaxed and this can cause abuses. It may also be the case that the access control mechanism implemented does not flawlessly represent the policy agreed prior the disclosure of data. In both cases the medical system does not act ill-intentioned, but the patients' data can still be misused, and this may cause mistrust. Hence, the medical system's goal is to regain the trust of its users. This is realized by allowing them to independently verify whether the system has acted in compliance with the agreed policy. By doing that, we also avoid requiring the patient to place major trust in one single entity.

Our attacker model also assumes an honest-but-curious verifier, which will not actively behave dishonestly, but my retain any information disclosed to it. We also assume an external attacker, who will try to extract or infer information on the patients. The attacker is assumed to have access to the verifier, and any information exchanged between the other players. Because our goal is to demonstrate how independent verifiability can be achieved in a private manner (without leaking any sensitive information), we are only interested in what an attacker can learn through the use of the verifier. The capabilities of the attacker towards the medical system are not explored in this work.

In order to avoid a possible collusion between medical system and verifier, we suggest the implementation of several verifiers by different entities. In this way, the patients can double-check with different verifiers in case of suspicion. Verifiers would avoid collusion with medical systems in order to maintain reputation, and medical systems would avoid collusion with verifiers as that can be identified by other verifiers. Verifiers can also be tested by the users with a set of logs and policies for which the expected results are known. Even though these approaches do not demonstrate the verifier correctness, they provide stronger evidences that can be used as criteria to support the choice of verifier.

It is important to note that we do not investigate into the matter of how to ensure the logs' accuracy and integrity. This topic is out of the scope of our work. We assume the medical system is honest and has its own reliable and trustworthy logging mechanism, and that it securely stores and handles data and logs. For insights on how logging mechanisms can be achieved accounting for logs' accuracy and integrity, we remand the reader to [172, 177]. The following section presents in details our proposal for verification using searchable encryption.

5.5 Solving verification with Searchable Encryption

Symmetric Searchable Encryption (SSE) schemes are popular in cloud settings. Data owners store encrypted data in an outsourced database, perform encrypted queries, and receive the encrypted data they searched for. We propose the use of SSE in a different setting: to verify whether the medical system is compliant to the access policy agreed with the patient. This verification is done through an external and independent audit. In our scenario, the verifier plays the role of the outsourced cloud service (even though it is not necessarily remote) and the patient is the data owner. We have added a third role played by the medical system, that is responsible for encrypting the data and generating the search indexes.

Next we present our scheme dividing it into the encryption of logs and index generation, the query generation and policy verification.

5.5.1 Encryption and index generation

For each patient that requires his or her logs, the medical system performs a *key agreement* process, where system and patient agree on a symmetric key k to be used for encryption and decryption. After that, the medical system encrypts each log individually and generates an index for each one of them, summarizing its content. The index includes all the *keywords* that can be searched in the encrypted data. Specifically for our scenario, the index of a log should contain the keywords related to the policy, such as the *action* registered by that log and the identity *id* of the user who performed the action (see Equation (5.2)). The index generation depends on the SSE method used, but a common requirement is that no *keyword* in the index should be exposed. This is usually achieved by encrypting or through the use of scrambling-related techniques [28, 66, 80, 152]. We abstract the process of encryption and index generation in Algorithm 1.

Algorithm 1 EncryptLogs($logs[n]$)

```
Input: array of $logs$ with $n$ entries
for each $i \in \{1, \dots, n\}$ do
    c[$i$] = Enc($k, logs[i]$)
    keywords = extractKeywords($logs[i]$)
    index[$i$] = generateIndex($k$, keywords)
end for
Output: c, index
```

5.5.2 Query generation

The medical system sends indexes and encrypted logs to the patient, who can redirect this information to the verifier for auditing purposes. On the patient's side, the main computation is related to the query generation. The query indicates which clauses the patient wants to verify. By generating one query containing each clause in the policy π (see Equation (5.1)), it is possible to determine compliance. We present here Algorithm 2 as a generic algorithm for query generation.

One may question the simplicity of our policy model; we only consider the identity of the actor and the action executed. We chose to do so in the interest of simplifying its description; our model supports other types of access control policies. It also supports any number of attributes by computing additional keywords in the indexes and conjunctions of the query. The model we propose can handle the verification of actors' roles, attributes, sections of personal data, for example. Given the medical system supports such attributes in its policy and register them in the audit logs.

In a traditional SSE approach, the data owner would generate an encrypted query and the database should simply execute this query over the indexes and return the respective encrypted data that matches the search. We adopt a similar approach. Here we assume that the patient has access to the policy agreed with the medical system. The patient then generates an encrypted query that contain the clauses from the policy, in order to check if the actions registered in the logs comply with the policy agreed. If the policy and the key used to encrypt the logs and indexes do not change, this query could also be further reused by the same patient.

We represent our query as a Boolean expression in a Disjunctive Normal Form (DNF). We assume a simple policy containing only a set of s *identities* and t *actions* as *keywords*, and relations in the format $(id_i, action_j)$ representing a clause of the policy allowing a person identified by id_i to execute $action_j$. To search for all logs that match the policy, the patient can generate a query in the DNF form as follows: $(id_{i_1} \wedge action_{j_1}) \vee \ldots \vee (id_{i_s} \wedge action_{j_t})$, where $(id_i \wedge action_j)$ is an allowed relation of the policy.

We abstract the query generation with a call to *"generate query"*. The details of this generation depend on the SSE method, but it basically identifies the clauses from the DNF expression and perform specific computations depending on the method used. Since we don't want the verifier to obtain information about the encrypted logs, some computation must be performed on the query as well to guarantee its confidentiality. This is a reasonable assumption considering that several SSE algorithms already guarantee that by using encryption or scrambling-based techniques [32, 116, 152]. As an example, the query generation by Moataz and Shikfa [152] consists on converting keywords to vectors, and applying consecutive multiplications, sums and divisions to them. The confidentiality in this case is guaranteed by incorporating random integers in the query computation (see [152, Section 4.2] for more details).

Note that the query generation is quite flexible, since it allows the patient to search for a range of different options. For example, he or she can search for all logs that match the policy, for some combination of specific clauses from the policy, or even for logs that do not match the policy by simply negating the search expression. It is important to note that most SSE schemes (specially the most traditional ones) search for single keywords on encrypted data. Here we require the use of a more expressive SSE that supports Boolean queries, such as the solutions proposed in [32, 116, 152]. Algorithm 2 summarizes the process of query generation.

Recall that we created indexes for the encrypted logs with the keywords (id_i, $action_j$) contained in each log. The verifier can then search through the logs indexes and identify the ones that match at least one of the conjunctions $(id_i \wedge action_j)$ from the query. Here we considered small policy clauses, but if necessary, we can easily

Algorithm 2 GenerateQuery(π)

```
Input: Policy $\pi = \{(id_i, action_i)\}$ with $m$ clauses
DNF = empty string
for each $i \in \{1, \dots, m\}$ do
    DNF = DNF $\|(id_i \wedge action_i)$
    if $i \neq m$ then
        DNF = DNF $\| \vee$
    end if
end for
$\mathcal{Q}$ = generateQuery(DNF)
Output: $\mathcal{Q}$
```

adapt the query to be more expressive. For example, by considering extra information such as identification of the objects that suffered the actions. In order to incorporate extra keywords in the search, these keywords also need to be incorporated in the policy and during the generation of the logs' indexes.

5.5.3 Policy verification

After the verifier receives the encrypted logs, respective indexes, and the query $\mathcal{Q}$, it has enough information to perform the verification for policy compliance. The search process consists on going through the encrypted logs to find the ones that match the query. For each log, the verifier obtains the corresponding index and use it to check if it matches the query. Here we call this comparison "test" and the logs that "pass" the test are added to the vector of results. If a log pass a test, it means that this log contains at least all the keywords from one of the conjunctions of the query, which represents compliance with one of the clauses of the policy.

Note that the search depends on the SSE method as well. Some constructions propose visiting each encrypted data and its indexes [152], while others present some more efficient search methods [66, 116, 170]. After the search, the verifier sends to the patient a list of encrypted logs that match the query. As logs, indexes, and queries are encrypted, the verifier is not able to learn anything about the confidential information. As an example, the verification by Moataz and Shikfa [152] consists on visiting every index and comparing it to the query. Generally speaking, every index is multiplied by the query and the ones that output a result equals to "1" correspond to logs that satisfy at least one clause from the policy. Algorithm 3 summarizes the our verification process.

Algorithm 3 Search($\mathcal{Q}, c[n], index[n]$)

```
Input: Encrypted query $\mathcal{Q}$, vector $c$ with $n$ encrypted logs, and their indexes
for each $i \in \{1, \dots, n\}$ do
    $r$ = test($\mathcal{Q}, index[i]$)
    if $r$ = true then
        $result$.add($c[i]$)
    end if
end for
Output: $result$
```

The results can be simplified by returning the number of logs that match the query, or a custom message for the special cases, such as "All logs match your query", or “No logs match your query". If further investigation is desired, Algorithm 3 can easily be adapted to return the logs that caused a mismatch. If the patient is interested in learning the cause for the mismatch he or she can decrypt those logs (using the key k) and understand what event is not compliant to the policy. Alternatively, these logs could be redirected to the medical system in order to inquire for a justification. How to better display and interpret the results, or how to request for justification are definitely relevant issues, but we understand they would require a research on their own. We refrain from delving into those matter in this work.

5.6 Complexity and security analysis

Several searchable encryption schemes are designed for the settings of big data applications, where there is a large amount of encrypted data and it is, for example, infeasible to search through every single record. Our scenario is slightly different and some of the assumptions in those settings are not applicable here. In what follows we discuss how technical aspects of SSE methods impact our solution. We first examine aspects of computational complexity of those methods (subsection 5.6.1) and later we discuss about their security (subsection 5.6.2).

5.6.1 Complexity

The efficiency of our scheme is directly related to the efficiency of the SSE method used. However, the use of non-optimal SSE methods, such as [32, 152], while prohibitive for big data applications, is acceptable in our scenario. In fact, SSE techniques are very well suited for our application. Our verifier processes only the audit logs related to one specific patient. These logs are assumed to be small pieces of data and in a much smaller scale than in cloud settings. Consequently, the efficiency problems presented in outsourced databases are not applicable here. Moreover, the generation of keywords in our application does not require complex calculations. The keywords are defined by the policy and logs, and can be automatically extracted from those.

Other more efficient SSE methods, such as the ones with sub-linear search time [116, 170], could also be considered here. In this case, the efficiency would depend on the query we are searching for. When searching for all logs that match the policy, it is expected the result to be close to the total amount of logs n. Hence, our search complexity will end up being close to $O(n)$ as well. However, when searching for the logs that *do not* match the policy, or that match some specific patters, we should expect a small number of results. In this case, methods that have search time close to the number of results may be the right choice. We assume the complexity of our worst-case scenario to be $O(n)$.

Intuitively one would tend to believe that the most efficient SSE methods on the literature are the best fit. However, there are trade-offs on these methods that need to be consider. Some of these methods use complicated structures and increase the spacial complexity, and others end up revealing parts of sensitive information. For a more extensive discussion on the trade-offs related to expressiveness of the query, efficiency, and security, the reader may want to refer to [27]. The choice of the method is not straightforward, it needs to be carefully studied. However, we suggest that in cases where the number of logs (n) is reasonable, it is a good practice to prioritize secure over efficient methods, even if they offer search complexity of $O(n)$.

5.6.2 Security

The confidentiality of personal information in our scheme is provided by the chosen symmetric key encryption algorithm. To avoid brute force and the most common attacks it is recommended to use encryption algorithms that have at least 112 bits of security (i.e. AES) [12]. Moreover, the use of deterministic encryption algorithms commonly implies in the leakage of patterns [27]. Therefore, the most secure SSE schemes are usually non-deterministic.

The security of the scheme is not only given by the encryption algorithm though, it also depends on the security of the SSE method itself. The SSE methods in the literature present a concern on the amount of information that can be inferred by the results of the search. Although they do not reveal directly the content of the encrypted data, the majority of these schemes will not prevent probabilistic analysis if the same data is repeatedly searched. This is a problem common to any application of this nature.

In our application the verifier returns all the results that match an specific query. This means that the verifier knows which encrypted logs are being returned, but not their plain content. The same applies to the attacker we consider in our model, since we assume it has access to the verifier and any exchanged message. There are SSE methods that aim to hide all information. In this way, the verifier is not even able to detect which logs are being returned to the data owner. However, these SSE methods are usually based on oblivious RAMs (ORAMs), and are not efficient in practice (for more details, see survey [27]).

We understand that the searches will usually be related to the logs that match or do not match the policy. By analysing the number of results from an specific query one could guess which search was performed. The search with several results is likely to be a search for all logs that match the policy, and the search with a few results is probably for the logs that do not match the policy. In this sense the verifier (or attacker) would be able to identify which logs match/do not match the policy, but would not be able to learn their content. We do not consider this as a threat to our scheme. A well chosen encryption algorithm would make sure that encrypted logs and queries are not available in plain text (they are encrypted or scrambled depending on the SSE scheme). Nonetheless, it is important to consider this case when applying our solution to other scenarios.

It is also important to note that any technical limitation of the underlying schemes (symmetric encryption or SSE) also reflects on a limitation of our proposed solution. We can cite, for example, the case of compromised or revoked private keys. In this case every data encrypted with that key is assumed to be compromised as well. A known solution to neutralize the potential damage is to reduce the lifetime of the key, and for example, use session keys instead of a single private key. In our scenario this solution would come at the cost of recalculating the queries, which could no longer be reused. This is the classical trade-off between efficiency and security.

Furthermore, a slight modification of our scheme is also needed to cope with the problem of compromised keys. Compromising one session key is enough for breaking privacy, even if forward and backwards secrecy are maintained, and no other message is obtained. The damage cause by compromising one session key is proportional to the amount of logs encrypted with that key. Therefore, to minimize this problem, only a small subset of logs should be verified at a time, i.e. the logs of the day or past week. Note that the maximum number of logs that are encrypted by the same session key is determined by the security guarantees required for specific applications of our scheme.

Chapter 6

Accomplishing Transparency in Medical Systems

The new European General Data Protection Regulation (GDPR) is now entirely in force, and electronic systems handling personal and identifiable data need to ensure that processing is *lawful*, *fair* and *transparent*. While the principles of lawfulness and of fairness express legalistic concepts, transparency can be interpreted as a socio-technical concept. It is a social concept because it is intended to aid individuals in understanding how their data is processed, and whether it is processed lawfully and fairly. It is technical because it should be realised as a technical feature whenever appropriate [10, see paragraphs: 4, 7].

The interest in transparency grew in the past few years after the European Union first proposed the principle in the early drafts of the GDPR. The interest has been mainly from a technical point of view. Transparency has been discussed as a principle of accountability in the cloud computing domain [19], it has been presented as a privacy goal and precondition for intervenability [149], and it has also been studied for its meaning in the area of electronic medical systems [218, 223]. Similarly, in the same period we have seen the emerging of several Transparency Enhancing Tools (TETs), which are typically system-independent tools intended to help individuals to gain more knowledge about their data (see [63, 256] for literature reviews on TETs).

Despite the rising number of works on transparency, defining compliance with the GDPR principles remains an open problem. Generally speaking, determining compliance with regulations is not an easy task. Regulations express legal requirements and define concepts in a generic language, which admits several interpretations. While this is done on purpose, so regulations reach a broad audience, it also hinders the task of defining compliance. However, from a purely technical perspective, one could attempt determining the degree of presumption of compliance concerning the principle of transparency by leveraging on the existing literature. How far are we from realising transparency in real systems? Can TETs help systems in the task of providing transparency to their users? In this chapter, we explore these questions, specifically in the domain of electronic medical systems.

The domain of medical systems is particularly interesting for a use case as it deals with highly sensitive and private personal data; thus reviewing the technical requirements proposed to implement transparency in the domain (see chapter 3), and comparing them to Articles extracted from the GDPR and a few selected TETs recently discussed in the literature may reveal interesting correlations.

6.1 Related works

To the best of our knowledge, only a few works discuss matters of compliance with the GDPR principles (i.e., [21, 149, 185]). In [149], the authors systematically assess the privacy goal of intervenability and explore the relationship between intervenability requirements with transparency ones. To this aim, the authors first derive and structure technical requirements by analysing the international standard ISO/IEC 291000 and the European GDPR for descriptions of the privacy principle and the formulations of the regulation. The requirements were then extracted with formulations close to the found in the original documents. Even though in this work technical (international standard) and legal (GDPR) documents are used, they are not compared. The requirements studied in this work are instead extracted from these documents.

In [21] the authors propose a Transparency Enhancing Tool (TET) in the form of a privacy dashboard. To define the relevant features to be implemented, they derived technical requirements from the *right of access* presented by the GDPR, the previous European Data Protection Directive, and the Federal Data Protection Act from Germany. The authors present eight requirements extracted from the data protection laws but do not compare them with any other source. Similarly, Raschke *et al.* propose a GDPR-compliant dashboard in [185], which is shaped by requirements extracted from the GDPR. In this work, however, only four high-level features are presented: the right to access data, obtaining information about involved processors, rectification and erasure of data, and consent review and withdraw.

Four works review TETs [63, 159, 167, 256]. The work by Murmann and Fischer-Hübner [159] surveys the literature searching for tools achieving *ex post* transparency. The authors explore aspects of usable transparency— derived from legals provisions in the GDPR, and well accepted usability principles. The authors identify meaningful categories of tools based on functionalities and implementation, for instance, and propose a classification using those categories. Although this work is comprehensive in exploring the characteristics of usable TETs, it does not explicitly map technical aspects of the tools with the GDPR provisions they help accomplishing. Compliance with the GDPR, hence, is not in the scope of this study.

There are works, however, which compare and map legal requirements and technical requirements, principles and designs. In particular, [67] reviews usability principles of Human-Computer Interaction (HCI) in a few selected TETs. To this aim, the authors first gather requirements from workshops and by reviewing the proposal of the GDPR (document available at the time), the previous European Data Protection Directives, and a few other related documents, such as the opinions from the Article 29 Data Protection Working Party. Legal provisions for transparency and accountability that have implications about HCI are considered in this work. These requirements are then mapped to three HCI concepts, which in turn are discussed in the context of the TETs. Even though the mappings and correlations presented in this work are thoroughly discussed, the authors do not present a structured procedure followed when defining them. It is our interpretation that those correlations were identified manually.

The German Standard Data Protection Model (SDM)[1] also classifies GDPR's provision in terms of *data protection goals* (e.g., availability, transparency, intervenability), and comments on *technical measures* that help to guarantee transparency, such as, documentation of procedures, logging of access and modifications. These measures

[1] https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf

relate to our requirements, but are more high-level. We believe our requirements could be classified according to them, allowing us to select TETs that can accomplish transparency as described by the SDM. We leave this task to future works. We will discuss here the similarities between our work and the SDM, and clarify where they differ.

6.2 Transparency in the GDPR

Transparency is a property championed by the GDPR as one of the main principles in personal data processing (see chapter 4). But how transparency is characterised by the Regulation? The GDPR gives no clear characterisation of it. For that, one must review the Articles of the Regulation that refer to the principle, even if indirectly. We selected those Articles by following a systematic peer review approach in four rounds: 1. Selection; 2. Filtering; 3. Revision; and 4. Validation of Articles. These rounds were conducted with the help of two other researchers, and are depicted in Figure 6.1.

The first round, *Selection*, was executed independently by two researchers, each researcher selected a preliminary list of Articles relating to transparency according to their understanding. Both researchers had previous experience with transparency and TETs, so the expectation was that the combined knowledge covers the general perception of transparency in different technical domains. The selection was conducted separately so the understanding of one researcher would not bias the other, and the selections would be as comprehensive as possible.

Following that, the second round, *Filtering*, consisted in combining the two preliminary lists and revisiting every Article selected by, at least, one researcher. The two researchers defended their interpretation of transparency, agreed on a common understanding, and extracted categories of Articles that cover that understanding. These categories comprise not only Articles about transparency but also other properties and artefacts that support the implementation of transparency. The categories are the following:

1. *Concerning data subjects (SUB)* – Articles describing the knowledge that should be made available to the data subjects concerning their data;

2. *Concerning authorities (AUT)* – Articles describing the knowledge that should be made available to authorities (e.g., Data Protection Officers, or auditors) concerning the processing of personal data;

3. *Empowerment (EMP)*[2] – Articles mandating the provision of means for the data subjects to react (e.g., rectification, and erasure);

4. *Quality of transparency (QUA)* – Articles which qualify transparency and describe how information should be presented to data subjects (e.g., concise, easy to understand);

5. *Certification (CER)* – Articles which foresee certification as a means to demonstrate that personal data is being processed according to the regulations;

6. *Consent (CON)* – Articles commenting on the need for the data subjects to consent with usage and processing of data.

[2] Also know as intervenability [149].

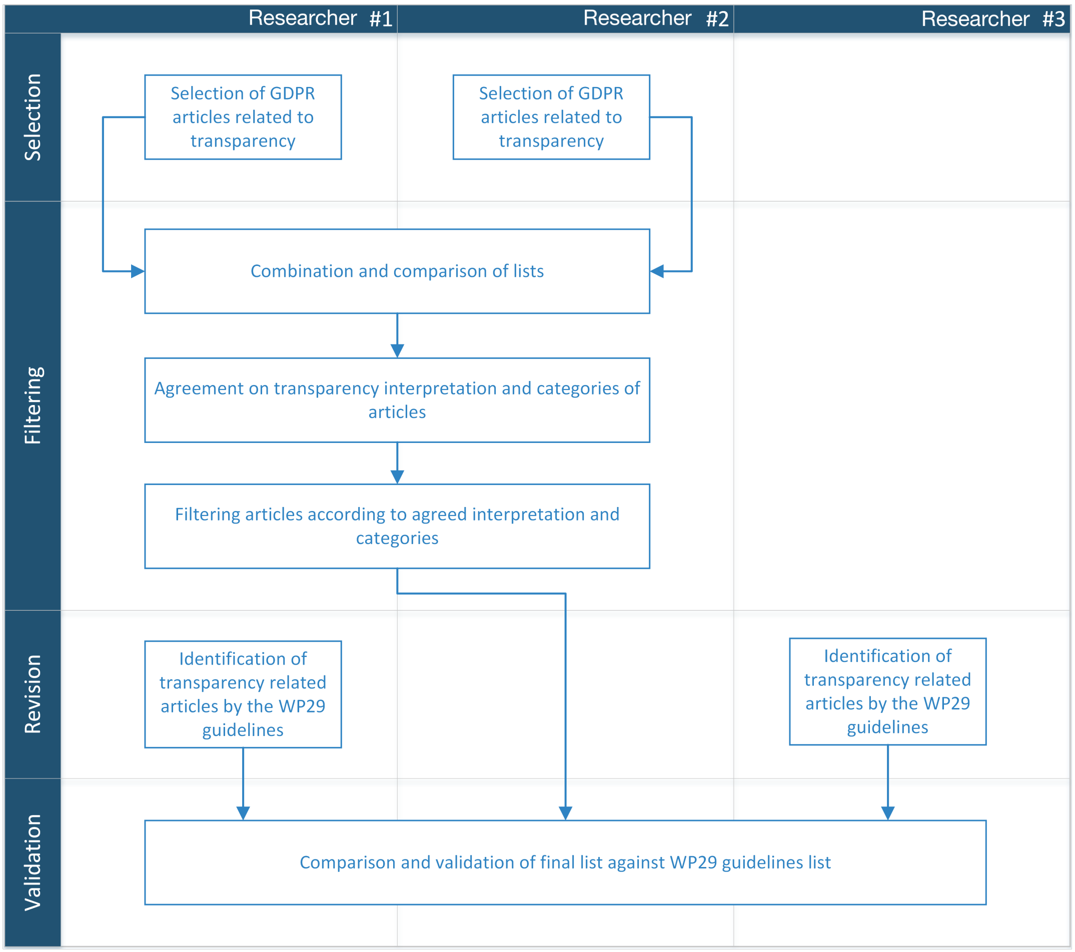

Researcher #1
Researcher #2
Researcher #3
Selection
Filtering
Revision
Validation
Selection of GDPR articles related to transparency
Selection of GDPR articles related to transparency
Combination and comparison of lists
Agreement on transparency interpretation and categories of articles
Filtering articles according to agreed interpretation and categories
Identification of transparency related articles by the WP29 guidelines
Identification of transparency related articles by the WP29 guidelines
Comparison and validation of final list against WP29 guidelines list

FIGURE 6.1: Methodology for selecting transparency related Articles from the GDPR.

We then filtered the Articles according to the categories. The resulting list consists mostly of the intersection of the two preliminary lists, but it is complemented by a few other Articles agreed among the researchers.

Third round, *Revision*, was also executed by two researchers, one of which was not involved in the previous steps of the analysis to reduce selection bias. The researchers independently reviewed the guidelines by the Working Party. Both researchers selected the Articles that, according to their interpretation, are mentioned in the guidelines as related to transparency. The resulting lists were then compared and combined. In this round, the lists were very similar. We believe this happened because the guidelines are more explicit about their interpretation of transparency.

Finally, the fourth round, *Validation*, was conducted as a sanity check for our selection of Articles. We compared our list with the list resulting from the tasks in the third round. The comparison intended to understand the relevancy of our selection of Articles by calculating how many Articles mentioned in the guidelines were covered by us (in first and second rounds). Our selection covers approximately 93% of the Articles in the guidelines. We consider our list sufficiently relevant.

We comment here only on the Articles mentioned in the guidelines that we opted not to include in our study. Article 12.5 describes when the charge of a fee may (or may not) be applied when information is provided to data subjects regarding personal data. Even though this Article is related to transparency, it does not describe a technical feature of a TET or system. Article 20 describes the *right to portability*. Articles 25.1 and 25.2 are both regarding the implementation of *data protection by design and by default*. This concept is instead related to the security property of privacy. Hence those Articles were not selected in our list. However, we include Article 25.3, which foresees the use of certification mechanisms to demonstrate compliance with Article 25.1 and 25.2. We understand this Article defends the right of data subjects to be aware of how their data is processed (in line with data protection principles), and as such, is in line with our interpretation of transparency.

In addition, we also compare our list with the presented by the SDM regarding the protection goals of transparency and intervenability (the ones we consider in our work as well).

Our selection does not contradict the list presented by the SDM, it is simply more detailed. The majority of Articles listed by the SDM are also considered in our selection. With the exception of Articles 5.1.(d), 5.1.(f), and 20 — regarding accuracy of data, security of personal data, and portability of data— which contain provisions on the quality of the data provided by transparency, and should be verified for compliance in every tool. Article 40, referring to the design of codes of conduct for controllers and processors, and could hardly be accomplished through the use of TETs. And Article 42, on certification, which are considered in section 6.4.

Our final list of selected transparency-related GDPR Articles (paragraphs and sub-paragraphs) comprises 79 items. The list can be found in Table 6.1.

Art.	Par.	Sub-par.	SUB	AUT	EMP	QUA	CER	CON
5	1	a				✓		
	2		✓					
6	1	a						✓
7	1							✓
	2							✓
	3				✓			✓
9	2	a						✓
11	2		✓					

12	1					✓		
	3				✓			
	4				✓			
	7					✓		
13	1	a	✓					
		b	✓					
		c	✓					
		d	✓					
		e	✓					
		f	✓					
	2	a	✓					
		b	✓					
		c	✓					
		d	✓					
		e	✓					
		f	✓					
	3		✓					
14	1	a	✓					
		b	✓					
		c	✓					
		d	✓					
		e	✓					
		f	✓					
	2	a	✓					
		b	✓					
		c	✓					
		d	✓					
		e	✓					
		f	✓					
		g	✓					
	3	a				✓		
		b				✓		
		c				✓		
	4		✓					
15	1	a	✓					
		b	✓					
		c	✓					
		d	✓					
		e	✓					
		f	✓					
		g	✓					
		h	✓					
	2		✓					
	3		✓					
16					✓			
17					✓			
18					✓			
19					✓			
21	1				✓			
	2				✓			

	3				✓			
	4				✓			
	5				✓			
22	1				✓			
	2	c			✓			✓
25	3						✓	
26	1		✓					
	2		✓					
	3				✓			
30	1			✓				
	2			✓				
	3			✓				
	4			✓				
32	3						✓	
33	1			✓		✓		
	2			✓		✓		
	3			✓				
	4			✓		✓		
	5			✓				
34	1		✓					
	2		✓			✓		

TABLE 6.1: Transparency-related GDPR Articles, paragraphs and sub-paragraphs, categorised according to the 6 categories identified in the second round of our methodology.

6.3 Correlating GDPR Articles and technical requirements

To correlate the Articles from the GDPR and the technical requirements for transparency in medical systems, we developed a simplified parser based on natural language processing techniques. Our process consists in the analysis of the *text corpora* (6.3.1), extraction of *corpus*-based glossaries and parsing of the *corpora* (6.3.2), and final adjustments (6.3.3). We did not conduct any statistical analysis, nor part-of-speech tagging (techniques applied in more sophisticated natural language processing algorithms). Instead, we iterated a few times realising small adjustments in our glossaries, re-evaluating the results of the parsing and, whenever needed, manually adding or removing a correlation.

Our approach is indeed only possible as our glossaries are context-based, limited to the terminology found in the GDPR and our requirements. We are aware of existing efforts in interpreting and translating laws, regulations, and other legal documents (e.g., [13, 162, 250]). We do mean to compete with them, but rather state that our parser, in the specific problem herein addressed, has given sufficiently good results.

6.3.1 Text corpora analysis

The first step was carried out manually. We first analysed the two text *corpora*: the Articles and provisions in the GDPR, and a set of technical requirements for transparency in the medical domain (see chapter 3). A text *corpus* is described as a “large body of linguistic evidence typically composed of attested language use", but has

GDPR terms	Technical terms
[action (not)] taken on a request	N/A
[identity] of the controller	responsible for handling owned data
[identity] data protection officer	who has the authority to investigate
purpose of processing	terms [of use]
legal basis for processing	policy; regulation
[conditions for] provision of data	regulation; terms [of use]

TABLE 6.2: Glossary of equivalent terms regarding the information to be provided to data subjects. Information between brackets are contextual and do not constitute the key-term.

GDPR terms	Technical terms
rectification	N/A
erasure [of personal data]	revoked consent
restriction [of processing]	N/A
copy of the personal data	mechanisms for accessing [personal data]
object [process of data]	N/A
not to be subject [to a decision]	N/A
exercise his or her rights	N/A
withdraw his or her consent	revoked consent

TABLE 6.3: Glossary of equivalent terms regarding the rights of data subjects. Information between brackets are contextual and do not constitute the key-term.

been used nowadays for a wide variety of text collections [151]. Our set of requirements is not a text *corpus* in its typical meaning, as they are not composed by standardised terms. In this sense, our requirements constitute a text *corpus* in its modern interpretation: a text collection tailored to one specific domain. The GDPR, on the other hand, represents better a classic text *corpus*, as it is stable, well-established and composed by standard legal terminology.

We analysed the text *corpora* and familiarised with the differences between the terminologies, as one *corpus* comprises technical terms and the other legalistic jargon. The terms found in one *corpus* were interpreted and linked to terms in the other *corpus*. As a result of this task, we highlighted potential connections between requirements and GDPR Articles and established a preliminary list of correlations.

6.3.2 Extraction of corpus-based glossaries and Parsing

To ensure the consistency of our correlation procedure, we automated the comparisons by extracting possibly-equivalent terms and structuring them in glossaries. Terms found in the GDPR were mapped to their equivalent technical terms, found in the list of requirements. The knowledge base needed for realising this step came from revisiting the preliminary list of correlations, from where we extracted the key-terms that seem to have triggered each correlation. We identify correlations according to a few textual elements present in the GDPR Articles: the *information* to be provided to the data subject; the *rights* the data subject must have; the *techniques* described in the Article; and few selected *keywords*. We organised each of these in hash tables that represent, in way, simplified *corpus*-based glossaries (see Table 6.2, 6.3, 6.4, and 6.5).

GDPR terms	Technical terms
[do not] permit identification	data privacy; to protect [data]; [data] protection; [data is] protected; separation [of data]
appropriate security	to protect
withdraw	revoke
not in a position to identify	N/A
automated decision-making	N/A
obtaining [personal data]	gather; infer; aggregate
copy of personal data	mechanism for accessing [personal data]
automated means	N/A
only personal data which are necessary	data minimisation
record of [processing of data]	accountability; audit
unauthorised	without authorisation
unlawful	vulnerability; breach
accidental loss	data loss; breach
accidental destruction	N/A
accidental damage	N/A
profiling	N/A
data minimisation	N/A
existence of the right	ownership
shall not apply	N/A

TABLE 6.4: Glossary of equivalent terms regarding the techniques described in the GDPR. Information between brackets are contextual and do not constitute the key-term.

GDPR terms	**Technical terms**
security	security
consent	consent
request for consent	N/A
written declaration	terms [of use]
purposes of the processing	terms [of use]
concise [information]	N/A
intelligible [information]	N/A
[information] easily accessible	N/A
[information] using clear [language]	N/A
[information using] plain language	N/A
icons	N/A
third party	third party; third parties; sub-providers; whom it purchases services
recipients	who has access; sub-providers; third party; whom it purchases services
international	other countries; extraterritorial; country
adequacy decision by the commission	comply with legal requirements; issues with respect to laws and regulations; legislative regimes
period	N/A
categories of personal data	detailed information [on the data collected]
source [from where of personal data originate]	[information on] data collected about [the data subject]
not collected from the data subject	[information on] data collected about [the data subject]
joint controllers	different parties
arrangement	agreement
responsibilities	responsibilities
respective roles	responsibilities
breach	breach
without undue further delay	timely
document comprising facts [that enables to verify compliance]	evidence
able to demonstrate	evidence
shall not apply	N/A

TABLE 6.5: Glossary of equivalent terms regarding the keywords found in the GDPR. Information between brackets are contextual and do not constitute the key-term.

Some key-terms were intentionally marked as *not applicable* as they brought almost no contribution to the final correlation list. For example, the term "transparency" found in Article 5.1(a) "Personal data shall be processed lawfully, fairly and in a transparent manner in relation to the data subject ('lawfulness, fairness and transparency')". This Article is comprehensive and should relate to every single requirement from our list, as it mandates data to be processed transparently. To ensure our list had only the most meaningful correlations, we decided to explicitly mark this term as not applicable (N/A). The same applies to the term "shall not apply", which is present in Articles (or paragraphs and sub-paragraphs) describing an exception to another Article. In other words, it presents the circumstances in which our requirements do not need to be implemented. Hence, any correlation found with an Article of this sort is likely to be a false-positive. To avoid this, we marked the term as not applicable. It is important to note that terms marked like this are not the same as terms absent from our glossaries. While the first will force a mismatch between a GDPR Article with that term and any possible requirement in our list, the second will just be disregarded when computing the correlations.

The computation of the correlations is based on an automatic parser. Initially, it parses each GDPR Article to identify the all the key-terms they contain. Then the requirements are parsed, searching for the ones which present at least one equivalent term for each key-term found. Our criteria for a match between an Article and a requirement is that all key-terms from the first are represented in the second. The correlation procedure is abstracted in Algorithm 4.

The correlation computation is realised in steps (as shown in Algorithm 5): we run the same parsing algorithm for each glossary, and later we merge the results of each comparison in one final list. By doing so, we maintained the correlating criterion decoupled, which simplified the process of re-evaluation of the terms and their possibly-equivalents. It also helped in balancing the asymmetry between GDPR Articles and our technical requirements, as the Articles are generally more verbose and encompass too many key-terms. Separating the terms into four glossaries ensured our criterion is not too restrictive, and that Articles can be correlated by one or several categories of textual elements.

6.3.3 Final adjustments

After computing the correlations based on the glossaries of terms, we reviewed the resulting list and compared with our preliminary list of correlations. Each correlation was analysed, but we focused on the discrepancies between the lists. For those, we semantically interpreted the Article and requirement marked as correlating to understand the context in which the key-terms appeared, and whether or not they had the similar meaning. We realised this procedure in a peer review manner. The correlations were then adjusted accordingly. We highlight here a few of the manually adjusted correlations.

According to our initial list, requirement 111.2 on information about how data are stored and who has access to them, should correlate with Article 15.1(c), which describes the rights of the data subject in obtaining from the controller the recipients of personal data. The requirement and the Article have a clear correlation. However, it was being disregarded by our parser as the Article contains the key-term "third countries" which does not appear in the requirement. As this key-term is responsible for several other well-fitted correlations, we opted for adjusting this exception manually. Similarly, the correlations with requirement 111.18, on describing the ownership of the data, had to be adjusted. We understand that *describing the*

Algorithm 4 Correlate($articlesGDPR[n], requirements[m], glossary\{\}[]$)

```
Input: array $articlesGDPR$ with $n$ entries, array of $requirements$ with $m$ entries, hash table of lists representing the $glossary$ of equivalent terms

$keys$ = $glossary$.getKeys()
for each $i \in \{1, \ldots, n\}$ do                                        ▷ For each GDPR Article
    for each $key$ in $keys$ do
        if $articlesGDPR[i]$.containsString($key$) then
            $keyTerms[i]$.add($key$)
        end if
    end for
    for each $j \in \{1, \ldots, m\}$ do                                    ▷ For each requirement
        $matchFound$ = FALSE
        for each $term$ in $keyTerms[i]$ do
            $equivalentTerms[]$ = $glossary\{term\}$
            for each $value$ in $equivalentTerms$ do
                if $requirements[j]$.containsString($value$) then
                    $matchFound$ = TRUE
                    break
                end if
                $matchFound$ = FALSE
            end for
            if !$matchFound$ then
                break
            end if
        end for
        if $matchFound$ then
            $correlatedArticles[i]$.add($requirements[j]$)
        end if
    end for
end for
Output: $correlatedArticles$
```

Algorithm 5 Init()

```
Let: $articlesGDPR[n]$ be the list of $n$ selected GDPR Articles, $requirements[m]$ be the list of $m$ technical requirements, $information\{\}[]$ be a glossary of information that should be provided to the data subject, $rights\{\}[]$ be a glossary of the rights the data subject has, $technique\{\}[]$ be a glossary of techniques mentioned in an Article, $keywords\{\}[]$ be a glossary of keywords found in the Articles;

$resultI[]$ = Correlate($articlesGDPR[], requirements[], information\{\}[]$)
$resultR[]$ = Correlate($articlesGDPR[], requirements[], rights\{\}[]$)
$resultT[]$ = Correlate($articlesGDPR[], requirements[], technique\{\}[]$)
$resultK[]$ = Correlate($articlesGDPR[], requirements[], keywords\{\}[]$)

for each $i \in \{1, \ldots, n\}$ do
    $finalCorrelation[i] = resultI[i] \cup resultR[i] \cup resultT[i] \cup resultK[i]$
end for
Output: $finalCorrelation$
```

ownership means to clarify what means to be the owner of a piece of data. In other words, to inform and describe the rights the data subjects have regarding the control of their data. In this sense, requirement 111.18 also relates to Articles 13.2.(c), 14.2.(c) and 21.4. Our parser captured a few relevant correlations for this requirement, but not all of them. We manually added those remaining correlations.

We also adjusted Articles and requirements that were marked as correlating by key-terms but were semantically different. For example, requirement 111.3, which requires the system to inform the users about the purchase of services, and Article 19, which requires the controller to communicate the erasure or rectification of personal data to its recipients. The same goes for requirement 111.19, regarding the disclosure of policies, regulations and terms, and Article 16, regarding the right to rectification of data. In both cases, the requirements and Articles were erroneously correlated and manually removed from the final list. Finally, we did the same for requirement 221.7, which mandates the provision of evidence that revoked consent has been executed. It had been erroneously correlated with Articles 7.1, 13.2.(c) and 14.2.(d) caused by the key-terms “consent" and “withdraw", present in those Articles.

Some other correlations were also considered for adjustments, as they were not present in our preliminary list, but were left untouched after a closer semantic analysis. For example, requirement 111.7, about describing procedures and mechanisms planned in cases of security breaches, correlating to Articles 33.3 and 33.5, and requirement 111.15 about informing on who has the authority to investigate any policy compliance, which is also correlated with 33.3. These Articles describe the information to be provided to data subjects in case of a data breach. Initially, the correlation was not considered as the requirements are ex ante (information to help the users understand what will happen to their data), and the Articles are, in a sense, ex post, as the data breach already happened. However, if the information described in the requirement is made available beforehand, in the event of a data breach, it will facilitate compliance with Article 33 from the GDPR. For this reason, we keep these correlations.

Similarly, requirements 221.2,5,8 are correlated with Article 5.2 of the GDPR (controller shall be accountable and responsible for demonstrating compliance with the lawfulness, fairness and transparency principles). The requirements, at first glance, seem unrelated to the Article, and to each other. However, the three requirements demand the users be presented with evidence of security breaches, of recovery from them, and of permission history. As evidence, by definition, is a piece of information or data that is used to prove or disprove something, we understand they contribute to *demonstrate compliance*. Even though these correlations were not identified in our initial list, we decided to keep them.

GDPR	Requirements	GDPR	Requirements
5.1.(a)		14.3.(c)	
5.2	111.16, 111.20, 221.1, 221.2, 221.3, 221.4, 221.5, 221.7, 221.8	14.4	
6.1.(a)	221.7	15.1.(a)	111.19
7.1		15.1.(b)	221.6
7.2		15.1.(c)	111.2, 111.4
7.3	221.7	15.1.(d)	
9.2.(a)		15.1.(e)	111.18
11.2		15.1.(f)	
12.1		15.1.(g)	221.6

12.3		15.1.(h)	
12.4		15.2	111.4, 111.11, 221.3
12.7		15.3	112.1
13.1.(a)	111.1	16	
13.1.(b)	111.15	17	221.7
13.1.(c)	111.19	18	
13.1.(d)	111.3, 111.4, 111.14	19	111.2, 111.4,
13.1.(e)	111.2, 111.3, 111.4	21.1	
13.1.(f)	111.4, 111.11, 221.3	21.2	
13.2.(a)		21.3	
13.2.(b)	111.18	21.4	111.18
13.2.(c)	111.18	21.5	
13.2.(d)		22.1	
13.2.(e)		22.2.(c)	
13.2.(f)		25.3	
13.3		26.1	111.14
14.1.(a)	111.1	26.2	111.14
14.1.(b)	111.15	26.3	111.14
14.1.(c)	111.19	30.1	221.5, 222.1, 232.1
14.1.(d)	221.6	30.2	221.5, 222.1, 232.1
14.1.(e)	111.2, 111.3, 111.4	30.3	
14.1.(f)	111.4, 11.11, 221.3	30.4	
14.2.(a)		32.3	
14.2.(b)	111.3, 111.4, 111.14	33.1	111.7, 211.1, 211.4, 221.8
14.2.(c)	111.18	33.2	111.7, 211.1, 211.4, 221.8
14.2.(d)	111.18	33.3	111.7, 111.15, 211.1, 211.4, 221.8
14.2.(e)		33.4	211.4
14.2.(f)	221.6	33.5	111.7, 211.1, 211.4, 221.8
14.2.(g)		34.1	111.7, 211.1, 211.4, 221.8
14.3.(a)	211.5	34.2	
14.3.(b)			

TABLE 6.6: Final list of correlated GDPR Articles and technical requirements. 72% of the requirements are correlated (26 out of 36).

6.4 Transparency Enhancing Tools

We conducted a review of the literature looking for any recent scientific work or project indexed by the keywords “transparency enhancing tools". We restricted our search to works published from 2014 onward, the year the GDPR started to be strongly supported by the European Parliament[3]. By adding this time restriction, we include in our study only tools potentially designed in line with the GDPR principles. We then broaden our study with the works related to our initial pool of selected works. A few works surveying TETs helped us defining a list of tools for our study (i.e., [21, 63, 159, 167, 210, 256]). To help selecting the relevant tools we classified them according to the following categories proposed in [256]:

[3] http://europa.eu/rapid/press-release_MEMO-14-186_de.htm

- **Application time –** describes the point of time at which the tool provides transparency to the data subjects;
- **Execution environment –** where the tool is operated;
- **Data type –** the types of data the tool provides insights about;
  - *Volunteered* – data a user actively and knowingly discloses;
  - *Observed* – data a user passively discloses (results from interactions with the system);
  - *Incidental* – data about a user that is disclosed by others;
  - *Derived* – data inferred about the user;
  - *Policy* – insights on the service's privacy policy;
- **Target –** the audience the tool is targeted for;
- **Delivery mode –** how the tool notifies the data subjects about relevant information on their data;
- **Authentication level –** the level of authentication of users the tool requires;
- **Interactivity level –** the level of control the data subjects can exercise over their data (from a technology perspective);
  - *Read-only* – tool only provides insights on the users data;
  - *Interactive* – allows for restriction/modification of *Collection* and *Usage* practices, or *Modification* and *Deletion* of data;
- **Scope –** the range of services/organizations the tool considers when providing transparency;
- **Assurance level –** the extent to which data subjects can determine the correctness and completeness of the information provided by the tool;
  - *Not trusted* – cannot be verified;
  - *Semi trusted* – cannot be guaranteed by technical means, but can be manually verified;
  - *Trusted* – guaranteed by technical means;
- **Transparency dimension –** information extent with regard to different stages of data utilisation cycle;
  - *Collection* – by whom data is collected;
  - *Analysis* – information on inference antecedents;
  - *Usage* – purposes for usage of data;
  - *Second usage* – how third-parties use personal data, and conditions for data transfer;
- **Attacker –** the source of possible threats;
- **Information source –** the source of the information provided by the tool.

As a result of this exercise, we found 27 tools that are potentially linked to the transparency principle. In what follows, we present them classified by their TETs category, proposed in [256]. This categorisation, TETCat, takes into account the *Assurance level*, *Application time* and *Interactivity level* of the tools. The full categorisation is shown in Table 6.7.

6.4.1 Assertion tools

Tools are classified as the assertion type whenever the correctness and completeness of the information they provide cannot be verified (either technically or manually). These tools can only provide users with information on the data controller's alleged processing practices. The TETCat does not further distinguish between assertion tools as their trustworthiness remains unaffected even under different manifestation of other parameters. As a consequence, this category covers tools with diverse goals.

Examples of assertion tools are third-party tracking blockers. These tools are commonly implemented as web-browser plug-ins which help the users becoming aware of trackers gathering information about them while browsing the web, for the purpose of, e.g., advertising or analytic. These tools also allow the users to interact and block such trackers. Mozilla Lightbeam[4] (ML), Disconnect me[5] (DM), and Privacy Badger[6] (PB) are examples of tracking blocker tools.

Those tools offer very similar features to the users, with the exception of Privacy Badger (PB). When this tool detects a new third-party script is tracking the user in three different websites, it automatically blocks them, without the need for the users to configure their preferences.

Tools that educate users on matters related to privacy protection are also considered assertion tools. One example of such a tool is the Privacy Risk Analysis (PRA) [48], which allows users to express their preferences, and visualise the impact on privacy risks through a user-friendly interface. Another example is Me and My Shadow[7] (MMS) which informs users about what happens to their data, how traceable they are on the internet and gives tips about existing privacy tools and digital shadow.

Privacy Score[8] (PS) can also be classified as an assertion tool. It tests websites and ranks them according to their security and privacy features (tracking, encryption of traffic and messages, protection against attacks). For each feature tested it also presents brief explanations which serve as material to educate users on privacy protection subjects.

Finally, Access My Info[9] (AMI) also falls under the assertion category. AMI is a web application that helps users to create legal requests for copies of their data from service providers based on the Canadian privacy legislation (PIPEDA). This tool differs from the previous ones as it does not *per se* provide information on the service's practices, nor educates the users on privacy matters. However, we consider it under the same category as it cannot ensure the service providers will properly process the requests. The tool provides a wizard which guides users in requesting data from dating, fitness, and telecommunications services. Despite being a web application, the wizard is implemented as a script running on the user's browser. AMI collects no information about the users unless explicitly authorised by them.

6.4.2 Awareness tools

These are the first type of tools providing information verifiable for completeness and correctness. The TETCat suggests different terminology for tools which provide technical means to verify its information (i.e., *Trusted*), and tools which information

[4] https://www.mozilla.org/lightbeam

[5] https://disconnect.me/

[6] https://www.eff.org/privacybadger

[7] https://myshadow.org/

[8] https://privacyscore.org/

[9] https://openeffect.ca/access-my-info/

can be verified manually by a user or an auditor (i.e., *Semi Trusted*). However, for the TETCat, they do not distinguish between the two assurance levels. Similarly, we refrain from evaluating this aspect of the tools. We only distinguish them between *Not trusted* and *(Semi) Trusted*, being the last the assurance level given to tools that provide somewhat trustworthy information.

Awareness tools provide *Ex ante* transparency, and interactivity level of *Read only*. Tools in this category help the user becoming aware of the privacy policy of the service provider but do not provide the users with controls over the processing of data. Examples of such tools are machine readable or interpreted policy languages and certification seals and marks.

Platform for Privacy Preferences Project[10] (P3P) is an example of machine-readable language tool. It proposes a language for describing a website's privacy policy in a standard format which can be retrieved and interpreted automatically by web-browsers. It enables the users to be informed of the website intentions towards the use and collection of their data in a consistent way, without requiring them to read the entire privacy policy of each website they visit. Even though works on P3P are currently suspended, we include it in our study as it has strong support from the academic community.

On a different approach, the Usable Privacy Project[11] [199] proposes a tool that automatically annotates privacy policies. The tool eases the reading of policies by interpreting it and highlighting parts of the text according to a fine-grained annotation scheme.

Other examples of awareness tools are the certification seals. European Privacy Seal (EuroPriSe), for example, provides a transparent privacy compliance certification of IT products and IT-based services with European data protection regulations [61]. Another example is the TrustArc (TArc), a tool which provides a trust mark on privacy practices and data governance. It follows certification standards based upon recognised laws and regulatory standards, such as OECD Privacy Guidelines, and GDPR [236].

6.4.3 Declaration tools

These tools are very similar to awareness tools, but they offer some level of interactivity. In our pool only one tool falls under this category: PrimeLife Policy Language (PPL) [68]. With this tool, users can interact and negotiate policies.

PPL is comparable to the awareness tool P3P as it proposes a machine-readable language for privacy policies. However, PPL further supports the description of privacy preferences from the users. So the service provider's declared intentions can be matched and checked for compliance with the user's preferences. PPL expresses policy in terms of authorisations, e.g., for what purposes the service provider will use the data, and obligations it is willing to fulfil for collected data items (e.g., to delete the data after a certain period, or to log all accesses to the data).

6.4.4 Audit tools

Audit TETs present users with *Ex post* or *Real time* transparency. Tools in this category include those that allow for access and verifiability of data, but do not provide means for the users to interact and intervene with the data processing (i.e., *Read only* tools).

[10] https://www.w3.org/P3P/

[11] https://explore.usableprivacy.org/

Examples of tools easing access to personal data are: A4Cloud Data Track[12] (DT) [69], Personal Data Table (PDT) [210], Digi.me[13], and the Blue Button[14].

Data Track is a user side ex post transparency tool that displays what personal data the service provider has stored, which was received from the user explicitly, implicitly, or derived. The tool is a proof-of-concept that parses location history from Google take-out. Personal Data Table is a similar tool, however in an earlier stage of maturity. PDT is a transparency implementation pattern. It describes a standardised table which contains information on personal data the service provider handles, such as, the data itself, the reasons for collection, who has access to it, and so on.

Digi.me is an application that helps to retrieve a copy of personal data from several different services (e.g., social media, finance, and health). The application does not store any personal data, it copies the data into the storage of the user's preference. By using this tool the user can visualise, search, and choose to share these data with other apps. Even though Digi.me allows the users to share, and consequently to control the collection and usage of personal data, it is not considered interactive. That is because it does not provide means for the users to control processing from the source where the data were retrieved.

Finally, the Blue Button is an initiative to standardise the right to access personal medical data in the USA. Blue Button-enabled portals display a logo, which symbolises that users are allowed to visualise and download their data.

On the verifiability side, there are discussions regarding transparency, but tools of this type are still in the idealisation phase. Privacy Evidence (PEv) [194], for example, proposes the generation of pieces of evidence based on structured policies (P3P and NAPS), secure logs (with hash chain scheme to guarantee confidentiality and integrity, for instance), and logs view that allow to scan through the logs and match with the policy. Transparent Accountable Data Mining (TAMI) [247] similarly proposes *a posteriori* privacy compliance checks on data mining. It is intended to check for data usage that is logically allowed to happen, but that legally should not be used in support to a given conclusion (inference). The proposed architecture is composed of a policy-aware logs module, a policy language framework, and a policy reasoning tool. Both tools are thoroughly discussed, but we found no implementation of them.

Finally, Private Verification of Access (PVA) (see chapter 5) also proposes a scheme for *a posteriori* access control compliance checks, but that operates under a data minimisation principle. The scheme suggests the use of a third-party tool which can operate on encrypted data access logs to check for matches (or mismatches) with a given access policy. The tool allows for a private independent audit of a system.

6.4.5 Intervention tools

Tools in this category allow users to verify properties about the processing of their data. They differ from audit tools as they also provide means for them to interact and control the terms of data collection and usage.

Privacy Through Transparency (PTT) [206], for example, proposes the use of a Provenance Tracker Network (PTN) which stores the logs for any transaction realised in a personal data flagged as *sensitive*, and allows for *a posteriori* audits. The logs are distributed in a network of trusted peers, preventing a single point of failure. Every sensitive data has a usage restriction associated with it, and every use of

[12] https://github.com/pylls/datatrack

[13] https://digi.me/

[14] https://www.healthit.gov/topic/health-it-initiatives/blue-button

data needs to be justified by a *usage intention*. This tool allows data owners to analyse logs and search for mismatches between the usage restrictions and intentions. They are allowed to request for explanations in case mismatches are found. The model assumes a non-prohibitive access control mechanism and supports Break-the-Glass (BTG) policies.

Privacy eSuite[15] (PeS) is a web-service consent engine that centralises consent and access rules with support to purpose of use. This tool also supports the integration with other services, such as the myConsentMinder, a web application that allows patients to manage their privacy preferences, and the Universal Audit Repository, that logs all accesses and attempts, notifies when a BTG happens, and simplifies audits through searches and report capabilities.

6.4.6 Remediation tools

These are the most comprehensive tools according to the TETCat. They comprise functionality to exercise control over data collection and usage, and also to modify and delete personal data stored by a data controller. Tools in this category are usually found in the format of privacy dashboards or data vault/marketplace applications.

PrivacyInsight (PI) [21] and GDPR Privacy Dashboard[16] (GPD) [185] are both examples of privacy dashboards within this category of TETs. PrivacyInsight is a dashboard whose main feature is to visualise (as a provenance graph) the flow of personal data into, through and out of an organisation. PrivacyInsight also provides full access to all personal data and allows users to exercise their rights over that data (e.g., erasure, and rectification). The GDPR Privacy Dashboard is intended to help users visualising, and requesting rectification or erasure of the data stored by a service provider. Both tools are designed to be easily adopted by any organisation.

Google Dashboard[17] (GD), and Microsoft Dashboard[18] (MD) are also examples of such tools, however they serve only their own organisation. Both tools allow the users to manage privacy settings, and to see, download, and manage personal data stored in their account.

Finally, the openPDS (oPDS) [156], and Meeco[19] (Mee) are examples of data vault/marketplace applications. The openPDS tool is a meta-data storage. Combined with SafeAnswers it allows for the privacy of the users by computing answers on the client side, and only sending third-party applications anonymous results. The results can also be aggregated with the ones from other users. Meeco, on the other hand, is a personal data marketplace which allows users to add, organise, edit, and progressively share their information. The Meeco client stores the terms the user agreed to, and records events of interaction with personal data in an event chain.

[15] http://hipaat.com/privacy-esuite/

[16] http://philip-raschke.github.io/GDPR-privacy-dashboard

[17] https://myaccount.google.com/dashboard

[18] https://account.microsoft.com/account/privacy

[19] https://www.meeco.me/

TET	Applic. time	Exec. envir.	Data type	Target	Deliv. mode	Auth. level	Interac. level	Scope	Assur. level	Transp. dim.	Attack.	Info. source	TETCat
Mozilla Lightbeam (ML)	Real time, Ex post	Client-side	Obs.	Data Subject	Pull	Anonym.	Read-only	Multi-org.	Not trusted	C	TP	(T)TP	Assertion
P3P	Ex ante	Server-side	Policy	Data Subject	Push	Anonym.	Read-only	Multi-org.	(Semi) Trusted	C/U/2ndU	Serv. Prov.	Data Contr.	Awareness
PrimeLife Policy Language (PPL)	Ex ante	Hybrid	Policy	Data Subject	Push	Anonym.	Interac. (C/U)	Multi-org.	(Semi) Trusted	C/U/2ndU	Serv. Prov.	Data Contr.	Declaration
Data Track (DT)	Ex post	Hybrid	Volunt., Obs., Incid., Deriv.	Data Subject	Pull	Full Id.	Read-only	Multi-org.	(Semi) Trusted	C/A	Serv. Prov.	Data Contr.	Audit
Privacy-Insight (PI)	Ex post	Hybrid	Volunt., Incid., Obs., Deriv.	Data Subject	Pull	Full Id.	Interac. (C/U/M/D)	Multi-org.	(Semi) Trusted	C/A/U/2ndU	Serv. Prov., TP, Users	Data Contr.	Remediation
Privacy Risk Analysis (PRA)	Ex ante	(T)TP-based	Policy	Data Subject	Pull	Anonym.	Read-only	Multi-org.	Not trusted	C/A/U/2ndU	Serv. Prov., Users, TP	(T)TP	Assertion
GDPR Privacy Dashboard (GPD)	Ex post	Server-side	Volunt., Incid., Obs., Deriv.	Data Subject	Pull	Full Id.	Interac. (C/U/M/D)	Multi-org.	(Semi) Trusted	C/A/U/2ndU	Serv. Prov., TP, Users	Data Contr.	Remediation
Personal Data Table (PDT)	Ex post	Server-side	Volunt., Incid., Obs., Deriv.	Data Subject	Pull	Full Id.	Read-only	Service	(Semi) Trusted	C/A/U/2ndU	Serv. Prov.	Data Contr.	Audit
Disconnect me (DM)	Real time, Ex post	Client-side	Obs.	Data Subject	Push	Anonym.	Interac. (C/U)	Multi-org.	Not trusted	C/2ndU	TP	(T)TP	Assertion

Me and My Shadow (MMS)	Ex ante	(T)TP-based	Policy	Data Subject	Pull	Anonym.	Read-only	Multi-org.	Not trusted	C/A/U/2^{nd}U	Serv. Prov., Users, TP	(T)TP	Assertion
EuroPriSe	Ex ante	(T)TP-based	Policy	Data Subject, Auditor	Push	Anonym.	Read-only	Multi-org.	(Semi) Trusted	C/A/U/2^{nd}U	Serv. Prov., TP	(T)TP	Awareness
Privacy Score (PS)	Ex ante	(T)TP-based	Policy	Data Subject, Auditor	Pull	Anonym.	Read-only	Multi-org.	Not trusted	2^{nd}U	Serv. Prov., TP	(T)TP	Assertion
Google Dashboard (GD)	Ex post	Server-side	Volunt., Incid., Obs., Deriv.	Data Subject	Pull	Full Id.	Interac. (C/U/M/D)	Org.	(Semi) Trusted	C/A/U/2^{nd}U	Serv. Prov.	Data Contr.	Remediation
Privacy Evidence (PEv)	Ex post	Hybrid	Policy	Auditor, Data Subject	Pull	Full Id.	Read-only	Multi-org.	(Semi) Trusted	C/U	Serv. Prov.	Data Contr.	Audit
TAMI Project	Ex post	Hybrid	Volunt., Incid., Obs., Deriv.	Auditor, Data Subject	Pull	Full Id.	Read-only	Multi-org.	(Semi) Trusted	U	Users	Data Contr.	Audit
Privacy Through Transp. (PTT)	Ex post	Server-Side	Volunt.	Data Subject, Auditor	Pull	Full Id.	Interac. (C/U)	Multi-org.	(Semi) Trusted	C/U	Users	(T)TP	Intervention
Private Verif. of Access (PVA)	Ex post	Hybrid	Volunt., Obs., Incid., Deriv.	Data Subject	Pull	Anonym.	Read-only	Multi-org.	(Semi) Trusted	C/U	Users, Serv. Prov.	(T)TP	Audit
Privacy Badger (PB)	Real time, Ex post	Client-side	Obs.	Data Subject	Push	Anonym.	Interac. (C/U)	Multi-org.	Not trusted	C	TP	(T)TP	Assertion
Access My Info (AMI)	Ex post	Client-side	Volunt., Incid., Obs., Deriv.	Data Subject	Pull	Full Id.	Read-only	Multi-org.	Not trusted	C/A	Serv. Prov.	Data Contr.	Assertion

TrustArc	Ex ante	(T)TP-based	Policy	Data Subject, Auditor	Push	Anonym.	Read-only	Multi-org.	(Semi) Trusted	C/A/U/2^{nd}U	Serv. Prov., TP	(T)TP	Awareness
openPDS	Real time, Ex post	Client-side	Volunt., Incid., Obs., Deriv.	Data Subject	Pull	Full Id.	Interac. (C/U/M/D)	Multi-org.	(Semi) Trusted	C/A/U	Serv. Prov.	(T)TP	Remediation
Digi.me	Real time, Ex post	Hybrid	Volunt., Incid., Obs.	Data Subject	Pull	Full Id.	Read-only	Multi-org.	(Semi) Trusted	C	Serv. Prov.	Data Contr.	Audit
Microsoft Dashboard (MD)	Ex post	Server-side	Volunt., Incid., Obs., Deriv.	Data Subject	Pull	Full Id.	Interac. (C/U/M/D)	Org.	(Semi) Trusted	C/A/U/2^{nd}U	Serv. Prov.	Data Contr.	Remediation
Privacy eSuite (PeS)	Real time, Ex post	Hybrid	Volunt., Incid.	Data Subject, Auditor	Pull, Push	Full Id.	Interac. (C/U)	Multi-org.	(Semi) Trusted	C/U	Serv. Prov.	Data Contr.	Intervention
Meeco (Mee)	Real time, Ex post	Hybrid	Policy, Volunt.	Data Subject	Pull	Full Id.	Interac. (C/U/M/D)	Multi-org.	(Semi) Trusted	U	Serv. Prov.	(T)TP	Remediation
Blue Button (BB)	Ex post	Server-side	Volunt., Obs., Incid., Deriv.	Data Subject	Pull	Full Id.	Read-only	Multi-org.	(Semi) Trusted	C	Serv. Prov.	Data Contr.	Audit
Usable Privacy (UP)	Ex ante	(T)TP-based	Policy	Data Subject	Pull	Anonym.	Read-only	Multi-org.	(Semi) Trusted	C/A U/2^{nd}U	Serv. Prov.	Data Contr.	Awareness

TABLE 6.7: Transparency Enhancing Tools (TETs) classified according to their characteristics. (T)TP = (Trusted) Third Party; C = Collection; U = Usage; M = Modification; D = Deletion; A = Analysis; 2^{nd}U = Second Usage.

6.5 General picture

To have a general picture of transparency's development, we compared the list of selected TETs with our technical requirements. Doing so enabled us to understand the extent in which TETs can realise transparency in medical systems, and also to have, by transitivity, a list of TETs which can help achieve compliance with the provisions of the GDPR.

The TETs categorisation facilitated the comparison between the tools and the list of requirements. Mainly, we pre-selected the tools and requirements by their application time (i.e., *ex ante*, *ex post*/*real time*) and matched them manually according to the other categories, and descriptions whenever needed. The result of this effort is shown in Table 6.8. Exceptions were made only in two specific cases: regarding requirement 112.1, and when comparing certification seals tools.

The first is concerning requirement 112.1 on the provision of mechanisms for accessing personal data. In the context of medical systems, this requirement is considered *ex ante* as the data about the patients are typically generated by other users in the system, rather than being provided by the patients themselves. As a consequence, allowing these patients to access their data can be interpreted as a mandatory pre-condition for them to anticipate what will happen to their data. However, in the context of TETs, tools which allow for the access of personal data are considered *ex post*. In this specific case, we understand there is a close correlation between the requirement 112.1 and those tools, even if their application times do not match.

The second exception is regarding certification seals. We consider them *ex ante*, but admit a correlation between them and *ex post* requirements. Certification seals are tools which can serve as convincing evidence that a system complies with a given criterion. If the criteria regard the processing of data, these seals can help a data subject anticipating what will happen to their data, and whether it is going to be processed in a secure manner. However, from the perspective of the system, when it is evaluated for the certification, the processing of data is already happening. For this reason, we accept the correlation between ex ante certification tools and a few relevant ex post requirements.

After matching the TETs with our technical requirements, we managed to determine the tools which can help achieve compliance with the GDPR provisions. We did so by transitivity, for each tool matched to a given requirement, we set that this tool is also closely linked to the GDPR Articles that given requirement matches (see Table 6.6). This exercise highlighted, for example, the transparency aspects which are not yet covered by TETs. In Table 6.8 we summarised the results of this comparison, a full report of them may be found in Appendix C, where we expand the GDPR Articles into the paragraphs and sub-paragraphs relevant to this work. In what follows, we comment on our findings concerning the technical and legal aspects of transparency.

6.5.1 Technical aspects

Three requirements regarding terms and conditions seem not to be addressed by any TET: 111.1 on information regarding the physical location where data is stored; 111.4 on the existence of third-party services and sub-providers; and 111.14 on clarifications of responsibility in case of the existence of third-party services. We believe this information could be provided together with the terms and conditions of service. Even though the tool provided by the Usable Privacy Project (UP) aims at facilitating the reading of information provided in the terms and conditions, we did not

TET	Requirements	GDPR Articles
Mozilla Lightbeam	211.5, 221.6	14, 15
P3P	111.2, 111.3, 111.16, 111.18, 111.19	5, 13, 14, 15, 19, 21
PrimeLife Policy Language	111.2, 111.3, 111.16, 111.18, 111.19	5, 13, 14, 15, 19, 21
Data Track	112.1, 221.5, 221.6, 221.7	5, 6, 7, 14, 15, 17, 30
Privacy Insight	112.1, 221.4, 221.5, 221.6, 221.7	5, 6, 7, 14, 15, 17, 30
Privacy Risk Analysis	111.9, 111.13	
GDPR Privacy Dashboard	112.1, 211.5, 221.4, 221.6, 221.7	5, 6, 7, 14, 15, 17
Personal Data Table	112.1, 211.2, 211.3, 211.5, 221.4, 221.6, 221.7	5, 6, 7, 14, 15, 17
Disconnect me	211.5, 221.6	14, 15
Me and My Shadow	111.8, 111.13, 111.16, 111.19	5, 13, 14, 15
EuroPriSe	111.16, 221.1, 221.3, 221.4	5, 13, 14, 15
Privacy Score	111.6, 111.12, 111.13	
Google Dashboard	112.1, 211.5, 221.6, 221.7	5, 6, 7, 14, 15, 17
Privacy Evidence	221.1, 221.4, 221.5, 222.1, 232.1	5, 30
TAMI Project	211.2, 211.3, 211.5, 221.1, 221.4, 222.1, 232.1	5, 14, 30
Privacy Through Transparency	211.2, 211.3, 221.1, 221.4, 221.5, 222.1, 232.1	5, 30
Private Verif. of Access	211.2, 211.3, 221.1, 221.4, 222.1, 232.1	5, 30
Privacy Badger	211.5, 221.6	14, 15
Access My Info	112.1, 221.6	14, 15
TrustArc	111.16, 221.1, 221.3, 221.4	5, 13, 14, 15
openPDS	211.5, 221.6, 221.7	5, 6, 7, 14, 15, 17
Digi.me	221.6, 221.7	5, 6, 7, 14, 15, 17
Microsoft Dashboard	112.1, 211.5, 221.6, 221.7	5, 6, 7, 14, 15, 17
Privacy eSuite	221.1, 221.5, 221.7, 222.1, 232.1	5, 6, 7, 9*, 17, 30
Meeco	221.6, 221.7	5, 6, 7, 14, 15, 17
Blue Button	112.1, 221.6	14, 15
Usable Privacy	111.5, 111.10, 111.11, 111.15, 111.17, 111.19	13, 14, 15, 33

TABLE 6.8: Transparency Enhancing Tools (TETs), the technical requirements and GDPR Articles they help realising (* added manually). Articles not addressed by TETs: 11, 12, 16, 18, 22, 25, 26, 32, 34.

identify tags for the requirements above. For this reason, we do not consider these requirements as addressed.

There are other relevant developments on the reading of terms and conditions, and policies, such as the CLAUDETTE project[20], which makes use of artificial intelligence to automatically evaluate the clauses of policy for their clarity and completeness in the light of the GDPR provisions. Another relevant functionality in this regard is the Lost in Small Print[21] from Me and My Shadow (MMS), which reveals and highlights the most relevant information in the policy of a few selected popular services. We decided not to include those tools in our study as the first only evaluates the quality of the policy, without helping data subjects in the understanding of its contents, and the second for only providing a few selected examples of policies. Nevertheless, it is possible to see the matter is already subject of attention. We expect to see a different scenario concerning tools for terms and conditions in the future.

We also observed a lack of tools covering technical aspects of data processing. For example, requirements 111.5 about informing how the system ensures data is not accessed without authorisation, and requirement 111.20 on evidence of separating personal data from metadata, are not addressed by any of the tools we studied. The reason for this is not clear, as other requirements about the use of specific security mechanisms (111.12), and how to protect data (111.13) also cover technical aspects and seem to be subject of attention of TETs. We speculate this lack of attention may be due to the target audience, which in general has no technical education and would not value the provision of such information. Another possible explanation is that this sort of information is provided together with others, and we missed to identify them in our selected tools.

Finally, another set of requirements which seem to have less attention is regarding security breaches and attacks. They constitute the majority of requirements not addressed by any TET: 111.7, 211.1, 211.4, 221.2, and 221.8. As security breaches are unforeseen events, it does not come as a surprise that there are no tools for aiding the understanding of issues related to them. Nonetheless, it is important to notice that the GDPR reserves two Articles to provisions on personal data breaches (Art. 33 and 34), one of which is dedicated to describing how to communicate such matters to the affected data subjects. Being the health-care industry among the ones with most reported breaches, and being medical data in the top three most compromised variety of data (for more details, see results of the data breach investigation [239]), we consider this to be an area in need of further development.

6.5.2 Legal aspects

Only a few Articles from the GDPR do not seem to be covered by any of our selected transparency tools. We consider an Article as not covered when none of its paragraphs or sub-paragraphs is correlated to at least one TET. Examples of this are the Articles related to certification (articles marked as *CER* in Table 6.1). While Article 25 regards data protection by design and by default, Article 32 has provisions on security of processing, but both mention that compliance with such Articles may be demonstrated through the use of approved certification mechanisms referred to in Article 42.

Despite having included two certification seals in the list of TETs we studied (i.e., EuroPriSe, and TrustArc), we cannot confirm they are approved certification mechanisms. According to EuroPriSe, their criteria catalogue has not been approved

[20] https://claudette.eui.eu/

[21] https://myshadow.org/lost-in-small-print

pursuant to Article 42(5) GDPR, and they have not been accredited as a certification body pursuant to Article 43 GDPR yet[22]. Regarding TrustArc, we did not find enough information about this matter.

A few transparency quality and empowerment related Articles (*QUA* and *EMP* in Table 6.1) are also not addressed by our selected tools. Article 12, for example, qualifies the communications with the data subject and states that it should be concise, easily accessible, using clear and plain language, and by electronic means whenever appropriate. In our understanding, this Article does not correlate to any specific tool because it is transverse to all of them. This Article has provisions regarding the quality of communications; hence, all tools communicating information to data subjects should be affected by it. In chapter 4 we discuss metrics for transparency which, in line with this reasoning, consider the information provided to final users “being concise", or “being easily accessible" as indicators that transparency is properly implemented.

Article 12 also has provisions regarding the data subject's rights, as do Articles 16, 17, 18, 19, 21, 22, and 26. While Articles 17, 19 and 21 do relate to some tools as transparency and empowerment are closely linked, empowerment related Articles are either partially addressed by transparency tools, or not addressed at all. Meis and Heisel [149] present relevant developments in this topic. The authors discuss the privacy goal of empowerment (referred to by the authors as intervenability) and its relationship to transparency. For instance, Article 12 relates to their requirement T4 and T5, and Article 17 relates to requirement I10. The analysis of the requirements proposed in [149] and their relationship with TETs falls out of this work's scope. Despite that, at least concerning Articles describing the rights the data subject towards the processing of personal data (e.g., Art. 22, and 26), we believe policy, terms and conditions tools could also address them, but we found no tool addressing those subjects.

It is important to notice that a few Articles which appear not to be covered by any TET, are not considered in this analysis because they do not match by key-terms with any of our requirements. We investigate two of them manually: Articles 11, and 9. Article 11 has provisions on processing which does not require identification. We consider this Article in our study as its paragraph 2 states that the controller shall inform the data subjects when it is not in a position to identify them (category *SUB* in Table 6.1). It also further states that in such a case, Articles 15 to 20 (on the exercise of data subject's rights) shall not apply. In this sense, Article 11 describes a case when empowerment tools (related to Articles 15 to 20) are not required. It does not make sense to discuss the relationship of this Article and TETs in our list.

Article 9, on the other hand, has provisions on data subject's consent for data processing of special categories of personal data, including data concerning health. Privacy eSuite tool (PeS) is a web-service consent engine specifically tailored to collect and centralise consent for the processing of health data. This tool is connected with Article 9, and in the interest of completeness, we manually added this correlation in Table 6.8. However, PeS is a proprietary tool designed in line with the Canadian regulations. We found no means to determine to which extent this tool can help achieving the provisions in the GDPR.

Being consent one of the basis for lawful processing of personal data described in the GDPR, the number of tools addressing this subject seems suspiciously low. This fact does not imply that medical systems and other services are currently operating

[22] See `https://www.european-privacy-seal.eu/EPS-en/Criteria`.

illegally. We are aware that collecting consent for processing data is a practice. However, we are interested in tools designed that facilitate the task of collecting consent and help users to be truly informed and aware of the consequences of consent they are giving.

We investigated this more closely and searched for tools aiming at informed consent. Among our findings there are mostly tools and frameworks aiding the collection of informed consent for digital advertising[23]. We also found mentions to the EnCoRe (Ensuring Consent and Revocation) project, which presents insights on the role of informed consent in online interactions [248]. The project appears to have finalised, and we found no tool proposed to address the collection of informed consent.

One could claim that informed consent can be collected when the user agrees with the terms and conditions, or privacy policies, for which there are tools proposed (e.g., P3P, PPL, and UP). While that may be one possible solution, special attention is required that the request for consent is distinguishable from other matters (as per GDPR Article 7). It is also important to note that consent to the processing of personal data shall be freely given, specific, informed, and unambiguous[24]. In such case, implicitly collecting consent for processing data is arguably against the provisions in the GDPR, a viewpoint also defended in [248]. In that work, the authors discuss the extent to which terms and policies are even read and understood, and that, in this sense, consent is unlikely to be truly informed and freely given.

[23] See Conversant, IAB Europe, and ShareThis.

[24] GDPR Article 4 (11).

Chapter 7

Concluding remarks

Transparency is a new property that is becoming crucial as a promoter of the quality of service and as a guarantee of respect for users' rights. This interpretation is the essence of the principle proposed in the General Data Protection Regulation (GDPR), which upholds that people must have the right to know whether devices and online services entrusted with their personal data manage it securely and privately. Providing such information to end users is of paramount importance: what a device, an application, a service do, what they access, and for what purpose. Transparency comes into play by enabling users to endow devices and services (and their manufacturers and providers) with a motivated trust. Used to express commitment to users and clarify accountability, transparency may also become a significant competition factor.

Designing for transparency, however, is not a simple task. The problem is complex: as much relevant information as possible should be provided to the users; however, since users might lack the technical skills to understand the content of the information or to isolate meaningful material in an information flood, the information should be carefully selected and presented in a concise and intelligible form. Moreover, transparent solutions should be designed with the best interest of users in mind. Transparency should not put personal and private information at risk. Understanding how to realise this in the context of medical systems is the purpose of this research project. We recall here our goal:

Research goal. *To provide a formal operational definition for transparency and to design solutions to achieve it in medical data systems.*

This research project contributes to the understanding of transparency. It sheds light on how to decide if a solution complies with the data protection regulation and the dramatic changes it brought when it became applicable, on 25 May 2018[1]. The result of this research represents a first step into the definition of a framework to guide the implementation of *transparency-by-design*. It does so by: 1. clarifying the understanding of transparency in the medical data systems context; 2. defining a set of metrics that can be used to measure transparency, and how one should conduct such measurement; 3. modelling a private Transparency Enhancing Tool (TET) for the transparency sub-property of verifiability; 4. and finally by discussing how current TETs can help a medical system in the task of accomplishing transparency. In what follows we review our research questions, and discuss how our work has answered them.

[1] Regulation (EU) 679/2016, Article 99.2.

How can transparency be defined in medical data systems and how does it relate to other security properties?

Transparency is not a monolithic concept. It is instead a complex quality partitioned into several properties and concepts. In the first part of this work, we have studied various interpretations for transparency, and its relationship with other well-known properties (see chapter 2). We cannot claim to have included all possible concepts that one may find be linked to transparency. However, at least in the domain of medical data systems availability, verifiability/auditability, and accountability are the properties that we have found to contribute the most to a precise understanding of transparency.

We also studied transparency in respect to other properties, namely empowerment, usability and privacy. Empowerment, which is about giving patients control on their data, emerged to be a complementary property to transparency. Together, transparency and empowerment help realise openness, a concept that we argue includes transparency. Usability and privacy do not contribute directly to the notion of transparency, but support it and help enhance its quality.

In order to provide an operational definition of transparency, we have selected the most suitable interpretation we found and proposed a definition for it in the medical systems domain. Based on this definition, we then elicit 36 technical requirements that suggest how to realise transparency (see chapter 3). These requirements are diverse, but there are a few factors they have in common: they all demand for the provision of information (e.g., about policies, processes), or mechanisms to get that information. These factors offer different perspectives under which transparency can be viewed.

How can transparency be assessed in a system?

To answer this question, we have proposed a Model-Driven Engineering (MDE) approach to the transparency of a system. We introduce a UML model that unfolds transparency into basic and concrete elements, much easier to measure than the high-level property of transparency itself. By regarding accountability as one of the building blocks for transparency, we demonstrate the original meta-model (tailored to model accountability) applies to the domain of transparency in general.

The MDE approach presented in this work clarifies that the implementation of transparency is not so much relevant as the output they deliver to the users. Under this new perspective, it is possible to gather how well implemented the transparency of a system is by looking at the information provided to the users, and the output of a mechanism available to them.

In this work, we prove that the *transparency* of a system is not just a high-level concept, but a quality that can be measured. We do so by defining a set of metrics that can be used to evaluate some of the most significant factors of transparency, and also by proposing a methodology that helps perform a thorough assessment of the implementation of transparency in a system (see chapter 4). Our metrics and our measurement methodology provide a meaningful way of benchmarking transparency and comparing systems. We do not claim, however, to have a complete set of metrics, nor that our metrics are as accurate as possible. However, we have demonstrated our metrics are relevant both a) in the context of the new data protection regulation, and b) technically, when applied to real systems.

How can transparency be realised in a privacy-friendly manner?

To answer this question, we investigated the transparency sub-property of *verifiability*, which we believe to pose more challenges to the privacy of patients. To be able to verify whether a system acted in compliance with a given policy the verifier needs access to audit logs. These logs may reveal private information about the patients. Revealing them is not in the best interest of the patients. But not revealing them would mean the patient needs to trust the medical system with the verification; obliging the patient to place significant trust in one single entity. In this work, we demonstrate that Symmetric Searchable Encryption (SSE) can be adapted to provide the right balance between transparency and privacy.

In chapter 5 we propose the introduction of an entity for auditing the medical system on behalf of the patient. We name this entity *verifier*. We propose the implementation of the verifier as a Transparency Enhancing Tool (TET) controlled by the patient or by a third party would suffice to accomplish: 1. *automated verification* – patients should not be required to manually verify audit logs; 2. *independent audit* – demonstrates the honest intentions of the medical system and helps building reputation; and 3. *privacy* – protects the right for privacy of the patients.

By using SSE methods, we allow the verifier to operate on encrypted logs. In this way, protecting the interests of the patient. Our scheme defines that compliance is achieved whenever a log entry matches, at least, one clause in the policy. This scheme is possible since the policy describes every allowed action in the system. The SSE method allows then the verifier to search for those matches over encrypted audit logs and the obfuscated policy clauses. Thus ensuring no third-party will learn any sensitive information. With this scheme, one can only learn the number of logs that match (or not) a given search. Something we consider acceptable in our scheme since the logs are encrypted and indistinguishable from each other, and the policy is obfuscated. We understand that this is a necessary trade-off between privacy and verifiability in medical systems.

Can transparency be achieved with the existing tools?

The implementation of transparency as defined in this work will make medical systems fully patient-centred. This change may come with some resistance, as it will require significant architectural modifications in the current Health Information Technology (Health IT). However, several tools have been proposed to enhance transparency and can be leveraged by the most diverse systems.

We finalise our research project by systematically reviewing the literature of Transparency Enhancing Tools (TETs) in search of what exists to implement the principle of transparency as described by the GDPR. We guided our selection by the technical requirements for medical systems that we have found be semantically correlated with the Articles of the GDPR that define, directly or indirectly, transparency.

Our contribution, however, goes beyond a comparative review of the literature. We systematically analyse transparency in support to identify the GDPR concepts still in need of more development. We also discuss the tools which can help accomplish transparency, or give suggestions on how to implement it in medical systems. Out of the 21 GDPR Articles we study here, 12 seem to be, at least partially, addressed by our selected TETs.

This selection mediated by technical requirements may look like a limitation of our approach, but by doing so, we managed to have insights on issues that have less attention in works tailored to discuss compliance with the provisions of the GDPR. For instance, we noticed that matters related to Break-the-Glass (BTG) (i.e., requirements 211.2 and 211.3) are not correlated with any provisions from the GDPR. This topic may be of specific interest in the medical systems domain. Although we did not find a clear correlation between these requirements and any GDPR Article, we also have no reasons to believe BTG is out of the scope when discussing data protection principles. A clear indication of that is the number of TETs addressing the subject (e.g., PDT, TAMI, PTT and PVA): although in their early stage of development, some still in the idealisation phase which suggests the subject is new, but of interest for the TETs community. Works defending that exercising access control of data in one single point ignores the genuine possibility that data is available or can be inferred from somewhere else [247], suggests that adopting BTG is a suitable alternative that will help emphasise the importance of individual accountability towards the usage of data.

Similarly, we also found TETs which only correlate to our requirements (e.g., PRA, and PS). We believe they may serve as an inspiration to fill the gap we identified regarding tools for consent and security breaches. Privacy Score (PS), which tests web pages for known security vulnerabilities and provide a short explanation of them, could serve as inspiration for the development of tools explaining security breaches to a broad public. While Privacy Risk Analysis (PRA), which explains the risks and consequences of having a piece of personal data disclosed, could be adapted to help users in giving *de facto* informed consent.

7.1 Future works and Open problems

Throughout the development of this project, we identified some future works and open problems that remain to be explored. We classified them in four main categories. In what follows we explore them.

Transparency assessment. In this work, we assess transparency in a medical system. However, assessing it in different domains could bring interesting results. Based on that, one could analyse the differences in the results in order to classify the various sub-factors of transparency according to their importance in specific domains. We study transparency from the end-users' perspective, but alternatively one could evaluate the transparency implementation in a new use case, but having access to the internal documentation and Systems Development Life Cycle (SDLC) (i.e., with the assistance of the service provider). Such an analysis could unveil details (which could be assessed on their own) about the asymmetry of information between the provider and the user. The information asymmetry problem is well-known but, to the best of our knowledge, has never been explored from an analytic perspective.

The metrics proposed to assess transparency in this work have a clear limitation, they only account for textual information. Several Transparency Enhancing Tools (TETs) represent information with aid of graphical and visual elements (e.g., PS, PI, UP). A possible future direction for this work is to understand how visual elements can be included in the measurement of transparency. One starting point is to study the TETs categories presented by Murmann and Fischer-Hübner [159], which consider aspects of information representation, visual guidance, and visualisation perspective. However, to the best of our knowledge there are no standardised icons or graphic guidelines to help informing on data protection subjects. Thus making the task of objectively assessing such graphical elements far from trivial.

Verifier. The verifier we propose in this work is limited to the identification of log entries that match and the ones that do not match a given policy. The latter can then be manually investigated for permitted exceptions (Break-the-Glass (BTG) policies), or other events also relevant in medical systems, such as delegation. Including these events in our verifier is a natural evolution of our proposal.

The formalisation of our scheme is another possible future work. A first actionable task towards this goal would be to extend that model to account for access legitimacy. To do so, we will have to take a more careful look into the representation of events (logs) and authorised actions (policy) and to define protocols for obtaining and transferring these data between the players. A good starting point is to study and adapt the work from Butin and Le Métayer [30]. We will also need to investigate deeper on the SSE schemes in order to select the most suitable ones. The extension of searching capabilities is directly dependant on the evolution of these schemes.

Transparency Enhancing Tools. In this study, we reason about the tools on which a system can leverage to accomplish transparency as a technical principle: we do not discuss how to ensure legal compliance with the GDPR. However, we identified a few future developments which we believe will contribute to better coverage of transparency. We present in this work several tools tailored to one single use case (a few even designed for one specific organisation). Although they are comprehensive in addressing transparency, other systems could not immediately apply them. Examples are the Google and Microsoft Dashboards (GD and MD). Those tools should serve as a role model for a possible generic Transparency Enhancing Tool. Other tools are already prepared for general use but are designed with a focus on other regulations in mind. One example of such a tool is the Privacy eSuite (PeS), which is tailored to Canadian regulations. Similarly, Usable Privacy (UP) intends to highlight the most relevant parts of a privacy policy for the American public. Adapting those tools to the provisions in the GDPR seems to be an interesting future development for the state-of-the-art in transparency.

Trustworthiness. A future research direction that stretches along the line of this work is to define a methodology to assess how transparency affects the trustworthiness of a system. Trustworthiness has several interpretations, but one that seems to be well accepted is that it is related to the assurance the system will perform as expected (e.g., [8, 154, 171]). Transparency can foster trust if interpreted as a means to provide evidence of the well-functioning of a system concerning data usage and protection. However, recent works demonstrate that, in certain circumstances, providing too much transparency could erode the user's trust in the system [126]. This work explores the effects of transparency in the context of algorithmic interfaces, such as search results personalisations, and creation of custom radio stations. To the best of our knowledge, no similar study has been conducted in the medical data systems domain. How much can transparency affect patient's perceptions of awareness and trust? This question remains unanswered.

One other possible direction is to investigate the approach proposed by Stark and Wagner [225] in the context of electronic voting. The authors propose an approach to collect substantial evidence that the reported outcome of an election is correct. Three main components compose this approach: strongly software-independent voting systems; compliance audits; and risk-limiting audits.

We believe it is possible to apply this approach in medical systems through the use of transparency mechanisms (e.g., verifier, but not limited to it). Suggesting that the three components described by Stark and Wagner can be achieved, at least to some extent, through a combination of our transparency requirements. In order to verify this hypothesis, it would be necessary to determine which components map to our transparency requirements and whether or not our requirements suffice to cover the three components.

It remains an open problem how to demonstrate that this framework can be adapted to provide convincing evidence that medical systems are functioning as intended. Nevertheless, if such a task can be realised, the resulting framework could provide grounds to reinforce the trust framework of the system.

Appendix A

Transparency measurement procedure

In this document we present metrics descriptors in a format adapted from ISO/IEC 27004 standard. The categories *Suitability*, *Computation* and *Considerations* were added to ease the understanding, and the categories *Frequency* and *Responsible parts* are not filled, as they highly depend on the system being measured. Additionally, the category *Information need*, also suggested in the standard, was omitted. This category was intended to clarify the contribution of each metric. We judged it unnecessary in our context, as the *Measure ID*, in combination with the requirement being measured already clarify that.

A.1 Measure descriptors

Measure ID	**Reachability**
Suitability	Applies to information and mechanisms;
Measure	Linear and inverse exponential
Computation	1. Determine a number k maximum number of interactions that is considered acceptable to perform in order to find the information/mechanism's output; 2. Whenever the system allows login, start analysing from the screen after the successful login; Otherwise start from the main screen; 3. Extensively search for information/mechanism that implement the requirement; 4. Stop when reaching the information or the expected output of the mechanism (even if incomplete); 5. Count the amount of interaction N_{int} needed to reach it from the initial screen; An interaction is a click, typing, or anything that requires the user to actively do something to change the current state of the system; 6. Measure $\mathcal{R}c$.

Formula/scoring	$\mathcal{R}c = \begin{cases} 1, & \text{if } 0 \leq N_{\text{int}} \leq k \\ e^{(1-\frac{N_{\text{int}}}{k})}, & \text{if } N_{\text{int}} > k \end{cases}$
Target	1
Implementation evidence	Any kind of information or mechanism's output; Number of acceptable interactions; Grade reached by that number of interactions;
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to users; Mechanism's output;
Reporting format	Grade; k; N_{int}
Considerations	In case the evidence is spread across multiple parts of the system, calculate the amount of interaction N_{int} needed to reach every single data source, and measure $\mathcal{R}c$ considering their sum.

TABLE A.1: Reachability metric

Measure ID	**Portability**
Suitability	Applies to information and mechanisms;
Measure	Scale
Computation	1. Measure $\mathcal{P}$.
Formula/scoring	$\mathcal{P} = \begin{cases} 0, & \text{if no information available} \\ 0.2, & \text{if available in any open format} \\ 0.4, & \text{if available as a structured data} \\ 0.6, & \text{if available in a non-proprietary format} \\ 0.8, & \text{if uses URI} \\ 1, & \text{if based on linked data} \end{cases}$
Target	1
Implementation evidence	Any kind of information or mechanism's output;
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to users; Mechanism's output;
Reporting format	Grade
Considerations	In case the evidence is spread across multiple parts of the system, calculate portability for every single data source, and consider the lowest grade.

TABLE A.2: Portability metric

Measure ID	**Observability**
Suitability	Only suitable for information;

Measure	Proportion
Computation	1. Determine whether the information contains statements with claims or affirmations about the system's behaviour; only applicable if it does; 2. Select a total of $LS + NLS$ of statements, at least one per section/subject of the information; 3. Determine the number LS of statements which can be observed or linked to the system's process; 4. Determine the number NLS of statements which cannot be linked, either because not present, or dubious; 5. Measure $\mathcal{O}b$.
Formula/scoring	$\mathcal{O}b = \frac{LS}{LS+NLS}$
Target	1
Implementation evidence	Descriptive documents; List of entities;
Frequency	
Responsible parties	
Data source	Policies; Terms of use; Any document that describes the practice of the system;
Reporting format	Grade, statements
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

TABLE A.3: Observability metric

Measure ID	**Accuracy**
Suitability	Only suitable for information;
Measure	Proportion
Computation	1. Determine the number LS of statements which can be observed or linked to the system's process; only applicable for those; 2. Determine the number ALS of statements that accurately (correctly and consistently with the user's experience) describe some part of the system's process; 3. Measure $\mathcal{A}c$.
Formula/scoring	$\mathcal{A}c = \frac{ALS}{LS}$
Target	1
Implementation evidence	Descriptive documents; List of entities;
Frequency	

Responsible parties	
Data source	Policies; Terms of use; Any document that describes the practice of the system;
Reporting format	Grade, statements
Considerations	Builds on top of Observability metric (see item A.3); In case the evidence is spread across multiple parts of the system consider everything as one single data source.

TABLE A.4: Accuracy metric

Measure ID	**Currentness**
Suitability	Applies to information and mechanisms;
Measure	Inverse exponential
Computation	1. Determine the maximum acceptable delay t_{max} in which the information or mechanism output should be made available; 2. Collect the time t taken for the system to provide the information or mechanism output in the same unit as the ideal time frame; 3. Measure $\mathcal{C}u$.
Formula/scoring	$\mathcal{C}u = \begin{cases} 1, & \text{if } t \leq t_{max} \\ 2^{-\left\lceil \frac{t-t_{max}}{t_{max}} \right\rceil}, & \text{if } t > t_{max} \end{cases}$
Target	1
Implementation evidence	Any kind of information or mechanism's output; The time in which the information was made available; The tolerable amount of time for the information to be made available;
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to users; Mechanism's output;
Reporting format	Grade, t_{max}
Considerations	In case the evidence is spread across multiple parts of the system, calculate currentness for every single data source, and consider the lowest grade.

TABLE A.5: Currentness metric

Measure ID	**Conciseness**
Suitability	Only suitable for information;
Measure	Average words per sentence

Computation	1. Determine the nature of the information, only applicable if it is a text (with at least one sentence); 2. Select a tool to aid calculating the average sentence length ASL; 3. Measure $\mathcal{C}o$.
Formula/scoring	$\mathcal{C}o = e^{-\frac{1}{50}(ASL-20)^2}$
Target	1
Implementation evidence	Any kind of information provided in text format
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to the user;
Reporting format	Grade
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

TABLE A.6: Conciseness metric

Measure ID	**Detailing**
Suitability	Only suitable for information;
Measure	Proportion
Computation	1. Separate the data source into n_I pieces of information (e.g., sections of a document, elements in a list, . . .); 2. Determine a list of questions related to the requirement; [One question per subject in the requirement statement] OR [Apply the 5W (Who, What, Where, When and Why)]; 3. For each piece of information $i = 1 \dots n_I$ select a number P_i^D of pertinent questions for which details should be provided; non-pertinent questions should not be considered; 4. For each piece of information $i = 1 \dots n_I$ identify the number d_i of questions for which the details are provided, and number u_i of questions for which details are not provided, such that $d_i + u_i = P_i^D$ (do not consider how well explained the details are); 5. Measure $\mathcal{D}$.
Formula/scoring	$\mathcal{D} = \frac{\sum_{i=1}^{n_I} d_i}{\sum_{i=1}^{n_I} P_i^D}$
Target	1

Implementation evidence	Any kind of information or mechanism's output; The details it is supposed to provide to the user;
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to users; Mechanism's output;
Reporting format	Grade, matrix representing the pieces of information *i* and the questions;
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

Table A.7: Detailing metric

Measure ID	**Readability**
Suitability	Only suitable for information;
Measure	Flesch reading ease
Computation	1. Determine the nature of the information; Only applicable if it is a text (with at least one sentence); 2. Select a tool to aid calculating the average sentence length *ASL* and average number of syllables per word *ASW*; 3. Calculate *FRES*; 4. Measure $\mathcal{R}$.
Formula/scoring	$FRES = 206.835 - (1.015 \times ASL) - (84.6 \times ASW)$ $\mathcal{R} = \begin{cases} 0, & \text{if } FRES < 0 \\ \frac{FRES}{100}, & \text{if } 0 \leq FRES \leq 100 \\ 1, & \text{if } FRES > 100 \end{cases}$
Target	1
Implementation evidence	Any kind of information provided in text format
Frequency	
Responsible parties	
Data source	Documents; Notifications; Communications to the user;
Reporting format	Grade
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

Table A.8: Readability metric

Measure ID	**Effectiveness**
Suitability	Only suitable for mechanism;
Measure	Proportion

Computation	1. Separate the mechanism's output into n_I pieces of information (e.g., tool's output, if more than one tool is provided for the same requirement, elements in a list, ...); 2. Determine a list of questions a user intends to have answered when using the mechanism (i.e., the goals of the mechanism); [One question per subject in the requirement statement] OR [Apply the 5W (Who, What, Where, When and Why)]; 3. For each piece of information $i = 1 \ldots n_I$ select a number P_i^E of pertinent questions which should be answered by it; non-pertinent questions should not be considered; 4. For each piece of information $i = 1 \ldots n_I$ identify the number e_i of questions which are answered by the mechanism (goals reached), and number v_i of questions which are not answered (goals not reached), such that $e_i + v_i = P_i^E$; 5. Measure $\mathcal{E}$.
Formula/scoring	$\mathcal{E} = \frac{\sum_{i=1}^{n_I} e_i}{\sum_{i=1}^{n_I} P_i^E}$
Target	1
Implementation evidence	Mechanism's output;
Frequency	
Responsible parties	
Data source	Mechanism's output; The goals the mechanism is supposed to reach;
Reporting format	Grade, matrix representing the delivered outputs and the desired goals (questions);
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

TABLE A.9: Effectiveness metric

Measure ID	**Operativeness**
Suitability	Only suitable for mechanism;
Measure	Proportion

Computation	1. Define the set of equivalence classes $E = C \cup R \cup U \cup D$, the union of all possible actions relevant to the system (e.g., create document, edit personal information, ...); where C contains create actions, R contains read actions, U contains update actions, D contains delete actions; 2. Select a sub-set of actions $A = \{a_0, a_1, \dots, a_{k-1}\} : (A \subseteq E)$, that contains at least one action of each class (i.e., $(A \cap C \neq \emptyset) \wedge (A \cap R \neq \emptyset) \wedge (A \cap U \neq \emptyset) \wedge (A \cap D \neq \emptyset)$) 3. Measure $\mathcal{O}_A$.
Formula/scoring	$\mathcal{O}_A = \lfloor n/k \rfloor$
Target	1
Implementation evidence	Mechanism's output
Frequency	
Responsible parties	
Data source	Mechanism's output, Actions to be tested;
Reporting format	Grade; set of actions A tested
Considerations	In case the evidence is spread across multiple parts of the system consider everything as one single data source.

TABLE A.10: Operativeness metric

Appendix B

Evaluation of Microsoft HealthVault

B.1 Information-based requirements

B.1.1 111.1 – S must provide P with real time information on physical data storage and data storage location of different types of data

The information used to measure this requirement can be found in the “Microsoft Privacy Statement", under “Other Important Privacy Information" – “Where We Store and Process Personal Data" (WPD).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8
Observability	Statements: 1. “Typically, the primary storage location is in the customer’s region or in the United States, often with a backup to a data centre in another region." 2. “The storage location(s) are chosen in order to operate efficiently, to improve performance and to create redundancies in order to protect the data in the event of an outage or other problem." 3. “When we engage in such transfers, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data." 4. “Microsoft Corporation complies with the EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information transferred from the European Union and Switzerland to the United States." 5. “If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern."	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.9626282259
Detailing	See Table B.2	0.25

Readability		0.227023

TABLE B.1: Attributes and grades per metric referring to requirement 111.1.

	Delivered Details
Desired Details	WPD
Is the information provided in real time?	
Is there information on physical storage?	
Where is the data stored?	✓
Which type of data is stored?	

TABLE B.2: Detailing matrix 111.1: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

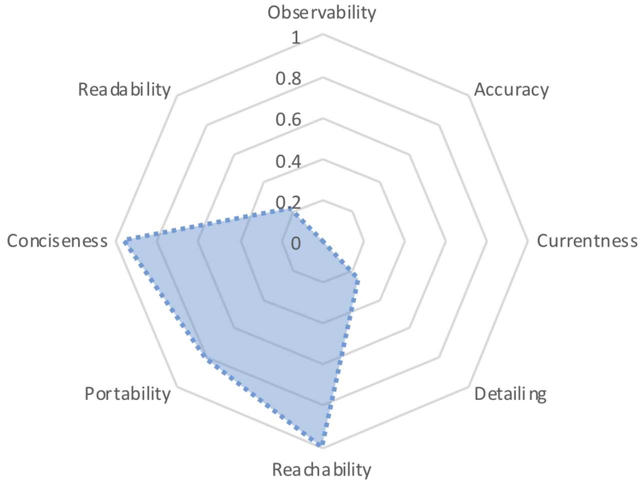


FIGURE B.1: Transparency measurement of requirement 111.1.

B.1.2 111.2 – S must inform P on how data are stored and who has access to them.

The information used to measure this requirement can be found in the “Microsoft Privacy Statement", under “Other Important Privacy Information" – “Security of Personal Data" (SPD).

Metric	**Attributes**	**Grade**
Reachability	$k = 3; N_{\text{int}} = 3$	1
Portability		0.8

Observability	Statements: 1. “We store the personal data you provide on computer systems that have limited access and are in controlled facilities." 2. “When we transmit highly confidential data (such as a credit card number or password) over the Internet, we protect it through the use of encryption." 3. “Microsoft complies with applicable data protection laws, including applicable security breach notification laws."	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.9372548956
Detailing	See Table B.4	0.5
Readability		0.2593

TABLE B.3: Attributes and grades per metric referring to requirement 111.2.

	Delivered Details
Desired Details	SPD
How is data stored?	✓
Who has access to data?	

TABLE B.4: Detailing matrix 111.2: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

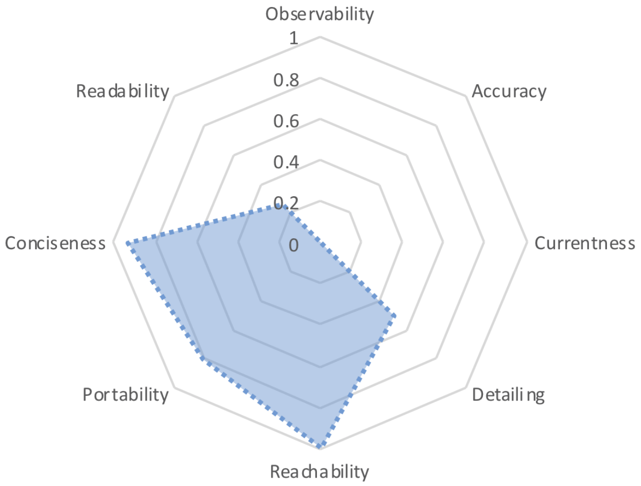


FIGURE B.2: Transparency measurement of requirement 111.2.

B.1.3 111.5 – S must inform P how it is assured that data are not accessed without authorisation.

The information used to measure this requirement can be found in the “Microsoft Privacy Statement", under “Other Important Privacy Information" – “Security of Personal Data." (SPD).

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8
Observability	Statements: 1. “We store the personal data you provide on computer systems that have limited access and are in controlled facilities." 2. “When we transmit highly confidential data (such as a credit card number or password) over the Internet, we protect it through the use of encryption." 3. “Microsoft complies with applicable data protection laws, including applicable security breach notification laws."	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.9372548956
Detailing	See Table B.6	1
Readability		0.2593

TABLE B.5: Attributes and grades per metric referring to requirement 111.5.

	Delivered Details
Desired Details	SPD
How is it assured that data are not accessed without authorisation?	✓

TABLE B.6: Detailing matrix 111.5: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

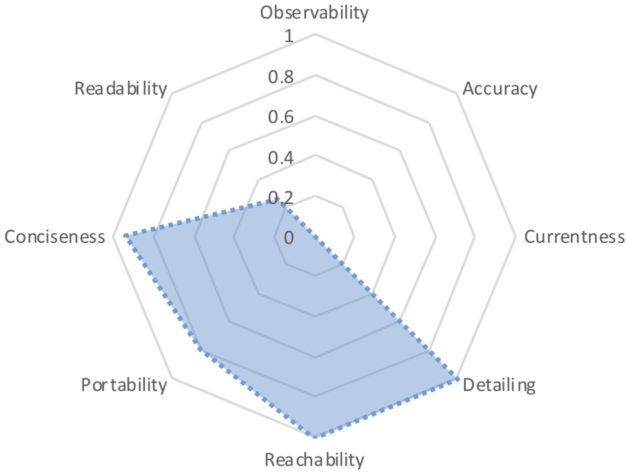


FIGURE B.3: Transparency measurement of requirement 111.5.

B.1.4 111.6 – *S* should make available a document that describes the adopted mechanisms for securing data against data loss as well as data privacy vulnerabilities.

The information used to measure this requirement can be found in the “Help", under “Privacy and Security" – “How does HealthVault help keep my information private?" (KIP).

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8
Observability	Statements: 1. “We apply security and privacy standards throughout the HealthVault development process." 2. “Microsoft won’t use your information in HealthVault to personalise ads or services without explicit permission." 3. “Microsoft HealthVault allows you to manage access not just by other people, but by apps you use as well. " 4. “HealthVault servers are located in controlled facilities." 5. “All health information transmitted between HealthVault servers and program providers’ systems is encrypted." 6. “When we back up data, the media are encrypted."	0.17
Accuracy	Statement 3.	1
Currentness		N/A
Conciseness		0.5388748092
Detailing	See Table B.8	0.5
Readability		0.356684

TABLE B.7: Attributes and grades per metric referring to requirement 111.6.

	Delivered Details
Desired Details	KIP
Which are the mechanisms adopted for securing data against data loss?	
Which are the mechanisms adopted for securing data against privacy vulnerability?	✓

TABLE B.8: Detailing matrix 111.6: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

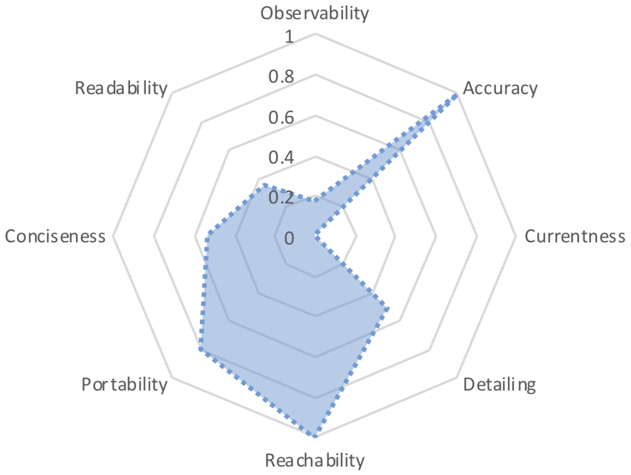


FIGURE B.4: Transparency measurement of requirement 111.6.

B.1.5 111.7 – S should make available a document that describes the procedures and mechanisms planned in cases of security breaches on P's data.

The information used to measure this requirement can be found in the “Help", under “Privacy and Security" – “What happens if someone gains access to my HealthVault account?" (GAA)

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 3$	0.8
Portability		0.8

Observability	Statements: 1. “If we learn of any potential breach of a HealthVault account, we will investigate, and, where appropriate, take actions possibly including blocking or suspending access to your account." 2. “If we determine there might have been a breach of your account, we will notify you via the contact information you have provided in your account." 3. “To provide an alternative contact address: Sign in to HealthVault. In the upper right, click your name and then click Account settings. Under Security, click Change security info. Enter the alternative contact information and click Save."	0.33
Accuracy	Statement 3.	1
Currentness		N/A
Conciseness		0.8241176336
Detailing	See Table B.10	1
Readability		0.4248765

TABLE B.9: Attributes and grades per metric referring to requirement 111.7.

	Delivered Details
Desired Details	GAA
Which are the procedures planned in case of security breach?	✓
Which are the mechanisms planned in case of security breach?	✓

TABLE B.10: Detailing matrix 111.7: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

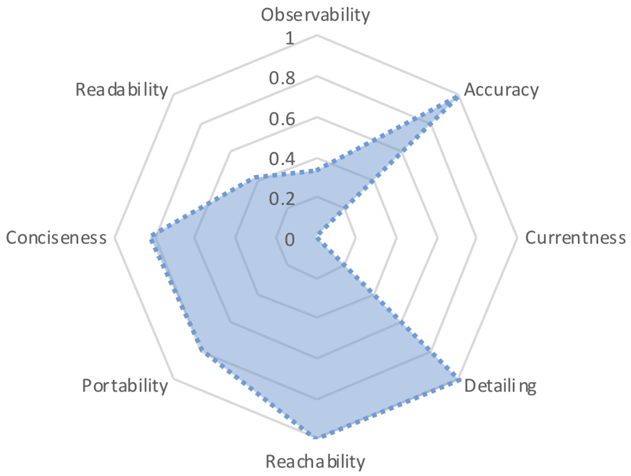


FIGURE B.5: Transparency measurement of requirement 111.7.

B.1.6 111.9 – P must be made aware of the consequences of their possible choices in an unbiased manner.

The information used to measure this requirement can be found in the “Sharing" section, as a warning before inviting someone to share the personal data. Additionally, further information can be found in the following page, under “What can a record custodian do?" (WCD).

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 2 + 1$	1
Portability		0.6
Observability	Statements: 1. “Sharing your record with a person you trust allows them to see, update, or delete information, depending on the level of access you give them." 2. “A custodian is someone who has full access to all the information in a HealthVault record, with the ability to see, change, add to, share and delete any of that information." 3. “Custodians can see information marked as confidential by other users, and they can see a history of all changes made to the record, including deleted items in the HealthVault trash." 4. “Custodians can permanently delete information from the record." 5. “In US accounts, custodians can manage Direct email addresses and send Direct messages on behalf of the record." 6. “All custodians have equal access to the record." 7. “Be very selective about who you give custodian access to, since they will have full control over the record, including the ability to remove your access to it."	0.86
Accuracy	Statements 1 to 7.	1

Currentness	$t_{max} = 5s$ (before the actual choice, but at most 5 seconds after the user enters the sharing section)	1
Conciseness		0.9866420204
Detailing	See Table B.12	1
Readability		0.401633

TABLE B.11: Attributes and grades per metric referring to requirement 111.9.

	Delivered Details	
Desired Details	Sharing	WCD
What are the consequences?	✓	✓
Is the information unbiased?	✓	✓

TABLE B.12: Detailing matrix 111.9: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

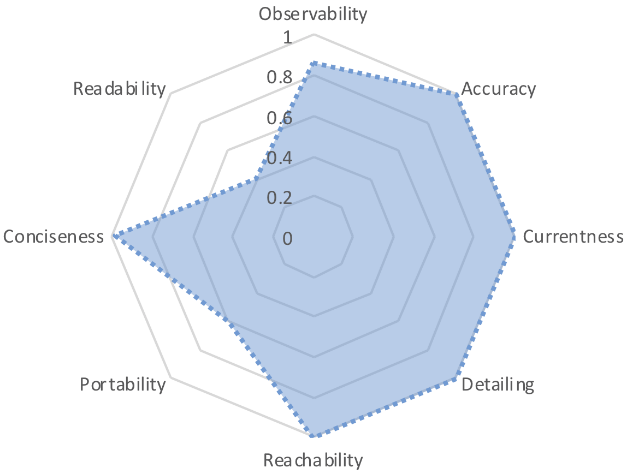


FIGURE B.6: Transparency measurement of requirement 111.9.

B.1.7 111.11 – *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.

The information used to measure this requirement can be found in the “Microsoft Privacy Statement", under “Other Important Privacy Information" – “Where We Store and Process Personal Data." (WPD)

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 3$	1
Portability		0.8

Observability	Statements: 1. “Typically, the primary storage location is in the customer’s region or in the United States, often with a backup to a data centre in another region." 2. “The storage location(s) are chosen in order to operate efficiently, to improve performance and to create redundancies in order to protect the data in the event of an outage or other problem." 3. “When we engage in such transfers, we use a variety of legal mechanisms, including contracts, to help ensure your rights and protections travel with your data." 4. “Microsoft Corporation complies with the EU-US Privacy Shield Framework and Swiss-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use and retention of personal information transferred from the European Union and Switzerland to the United States." 5. “If there is any conflict between the terms in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern."	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.9626282259
Detailing	See Table B.14	1
Readability		0.227023

TABLE B.13: Attributes and grades per metric referring to requirement 111.11.

	Delivered Details
Desired Details	WPD
Are data stored in other countries?	✓
Are there compliance issues related to that?	✓

TABLE B.14: Detailing matrix 111.11: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

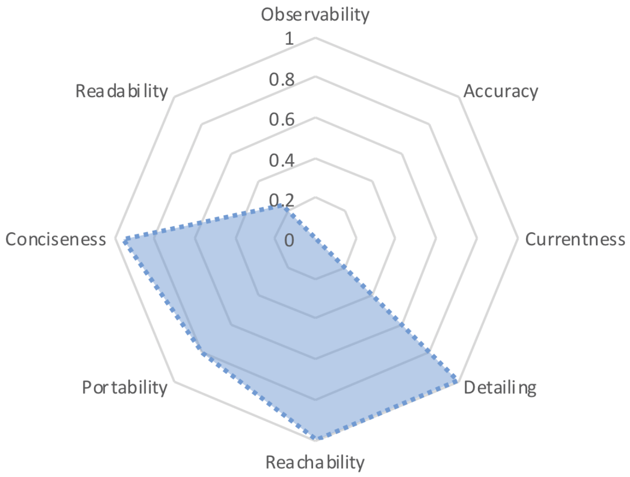


FIGURE B.7: Transparency measurement of requirement 111.11.

B.1.8 111.13 – S must inform P on how to protect data or how data are protected.

The information used to measure this requirement can be found in the "Help", under "Privacy and Security" – "How does HealthVault help keep my information private?" (KIP).

Metric	Attributes	Grade
Reachability	$k = 3; N_{\text{int}} = 3$	1
Portability		0.8
Observability	Statements: 1. "We apply security and privacy standards throughout the HealthVault development process." 2. "Microsoft won't use your information in HealthVault to personalise ads or services without explicit permission." 3. "Microsoft HealthVault allows you to manage access not just by other people, but by apps you use as well." 4. "HealthVault servers are located in controlled facilities." 5. "All health information transmitted between HealthVault servers and program providers' systems is encrypted." 6. "When we back up data, the media are encrypted."	0.2
Accuracy	Statement 3.	1
Currentness		N/A
Conciseness		0.53887480925
Detailing	See Table B.16	0.5
Readability		0.356684

TABLE B.15: Attributes and grades per metric referring to requirement 111.13.

	Delivered Details
Desired Details	KIP
How can someone protect data?	
How is data protected?	✓

TABLE B.16: Detailing matrix 111.13: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

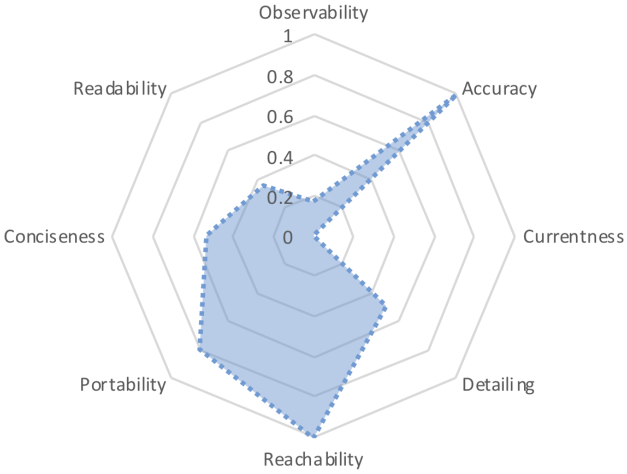


FIGURE B.8: Transparency measurement of requirement 111.13.

B.1.9 111.17 – S must make available a document explaining the procedures for leaving the service and taking the data out from the service.

The information used to measure this requirement can be found in the “Help", under “Your HealthVault Account" – “How do I close my HealthVault account?" (CMA). Additionally, further information can be found in “How do I export and save health information from HealthVault?" (ESI).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 3 + 1$	0.7165313106
Portability		0.8

Observability	Statements: 1. “Once your account has been closed, any information that you had stored in your account will be permanently deleted, although data may remain on our servers for 90 days.” 2. “To delete your account: Sign in to HealthVault. In the upper right, click your name and then click Account settings. At the bottom of the page, click Close account. Carefully review the information on the page, then click Close my account.” 3. “The exception is if there are other custodians of records in your account. In that case, you’ll be notified at the time you close the account, and those records will not be deleted.” 4. “You can export and save your health information in two ways: as a spreadsheet;” 5. “or as a CCR or CCD or HTML file.” 6. “To save health information as a spreadsheet: Sign in to HealthVault. On the left side of the page, click the name of the type of information you want to save as a spreadsheet. You’ll see the list view for that type of data. Click Export. In the browser message that appears, click Save. Your information will be saved in a spreadsheet format (.csv) that can be opened in Excel or other spreadsheet software.” 7. “You can create a CCR or CCD with information from your HealthVault record, but keep in mind that CCRs and CCDs don’t support all types of health information, so they won’t necessarily contain everything in your record.” 8. “To save information in your HealthVault record as a CCR or CCD or HTML file: Sign in to HealthVault. On the Home page, click Current and then click Export. Select the file format that you want to use. Select the type or types of information that you want to export. If you want to, select the date range for the data. Click Export. In the browser message that appears, click Save. Your information will be saved as a file on your computer.”	0.88
Accuracy	Statements: 2 to 8. Statement 3 is not considered accurate.	0.86
Currentness		N/A
Conciseness		0.5956142816
Detailing	See Table B.18	1
Readability		0.6395535

TABLE B.17: Attributes and grades per metric referring to requirement 111.17.

	Delivered Details	
Desired Details	CMA	ESI
How to proceed to leave the service?	✓	
How to proceed to take data out from the service?		✓

TABLE B.18: Detailing matrix 111.17: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

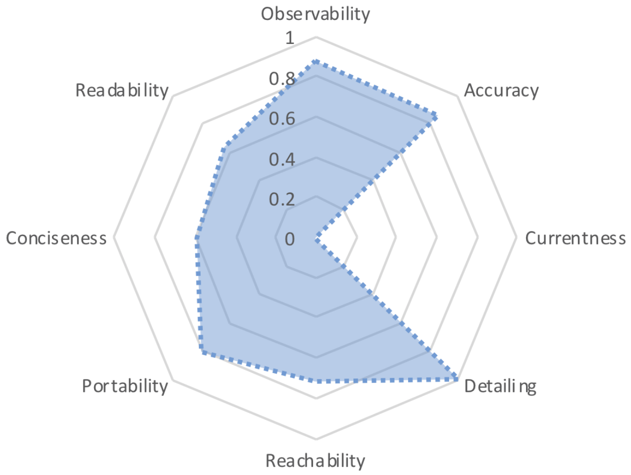


FIGURE B.9: Transparency measurement of requirement 111.17.

B.1.10 111.19 – S must provide P with disclosure of policies, regulations or terms regarding data sharing, processing and the use of data.

The information used to measure this requirement can be found in the “Microsoft Privacy Statement", and it is spread throughout several sections: “Personal Data That We Collect" (PDC), “How We Use Personal Data" (UPD), “Reasons We Share Personal Data" (SPD), “Cookies & Similar Technologies" (CST), “Other Important Privacy Information" (IPI), and “Microsoft Health Services" (MHS). To test for Observability and Accuracy we only consider statements exclusively related to HealthVault (MHS).

Metric	**Attributes**	**Grade**
Reachability	$k = 3; N_{\text{int}} = 1 + 1$	1
Portability		0.8

Observability	Statements: 1. “You can use more than one credential with HealthVault to help ensure continued access”; 2. “You can add or remove data to a health record you manage at any time”; 3. “As a custodian, you can share data in a health record with another person by sending an email invitation through HealthVault. You can specify what type of access they have (including custodian access), how long they have access, and whether they can modify the data in the record”; 4. “In the United States, we enable participating providers to obtain reports about whether the information they send to a record is used”; 5. “You can review, edit or delete your HealthVault account data, or close your HealthVault account at any time”; and 6. “You can unsubscribe from these emails [communications] at any time”.	0.83
Accuracy	Statements 1, 2, 3, 5 and 6. Statement 1 is not considered accurate.	0.8
Currentness		N/A
Conciseness		0.9620950775
Detailing	See Table B.20	1
Readability		0.3481985

TABLE B.19: Attributes and grades per metric referring to requirement 111.19.

	Delivered Details					
Desired Details	DWC	UPD	SPD	CST	IPI	MHS
How is data shared? With whom? For what purpose?			✓			
How is data processed? For what purpose?	✓	✓				
How is data used? For what purpose?				✓	✓	✓

TABLE B.20: Detailing matrix 111.19: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

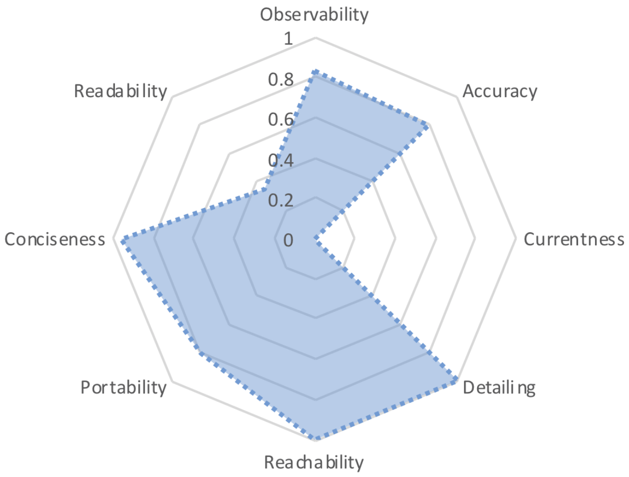


FIGURE B.10: Transparency measurement of requirement 111.19.

B.1.11 211.5 – S must inform P if and when data is gathered, inferred or aggregated.

The information used to measure this requirement can be found in the "Microsoft Privacy Statement" (MPS), and it is spread throughout the entire document. To test for Observability and Accuracy we only consider statements related to collection of personal data ("Personal Data That We Collect").

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 1$	1
Portability		0.8
Observability	Statements: 1. "The data we collect depends on the context of your interactions with Microsoft and the choices that you make, including your privacy settings and the products and features that you use. We also obtain data about you from third parties." 2. "Where providing the data is optional, and you choose not to share personal data, features like personalisation that use such data will not work for you."	0
Accuracy		N/A
Currentness		N/A
Conciseness		0.8671199163
Detailing	See Table B.22	0.5
Readability		0.4592695

TABLE B.21: Attributes and grades per metric referring to requirement 211.5.

	Delivered Details
Desired Details	MPS
Is information gathered?	✓
Is information inferred?	✓
Is information aggregated?	✓
When is information gathered?	
When is information inferred?	
When is information aggregated?	

TABLE B.22: Detailing matrix 211.5: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

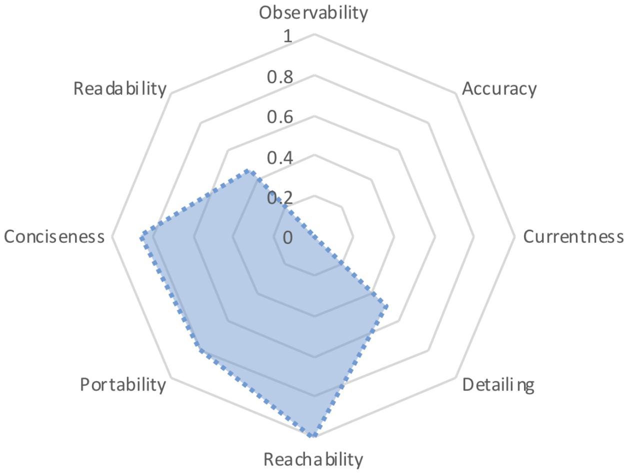


FIGURE B.11: Transparency measurement of requirement 211.5.

B.1.12 221.5 – S must provide P with evidence regarding permissions history for auditing purposes.

The information used to measure this requirement can be found in the "Record history" section, under "Miscellaneous and access-related changes to Username's record" (MAC).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 2$	1
Portability		0.6
Observability		N/A
Accuracy		N/A
Currentness	$t_{max} = 10s$	1
Conciseness		N/A
Detailing	See Table B.24	1
Readability		N/A

TABLE B.23: Attributes and grades per metric referring to requirement 221.5.

	Delivered Details
Desired Details	MAC
Is there information regarding permission history?	✓

TABLE B.24: Detailing matrix 221.5: desirable details compared with the delivered details. Greyed-out cells represent the non-pertinent questions.

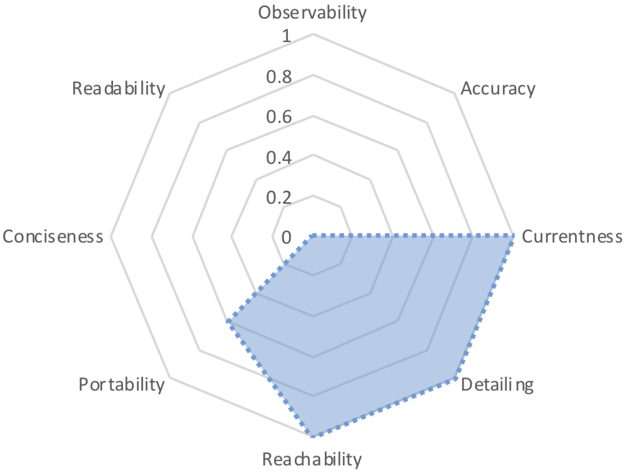


FIGURE B.12: Transparency measurement of requirement 221.5.

B.2 Mechanism-based requirements

B.2.1 112.1 – S must provide P with mechanisms for accessing personal data.

The evidence used to measure this requirement can be found in the “Home" page.

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 0$	1
Portability		0.6
Currentness	$t_{max} = 10s$	1
Effectiveness	See Table B.26	1
Operativeness	A = {createData, updateData, deleteData, createSharedData, updateSharedData, deleteSharedData}	1

TABLE B.25: Attributes and grades per metric referring to requirement 112.1.

	Delivered Outputs
Desired Goals	Home
Does the mechanism provide access to personal data?	✓

TABLE B.26: Effectiveness matrix 112.1: desirable goals compared with the real outputs. Greyed-out cells represent the non-pertinent goals.

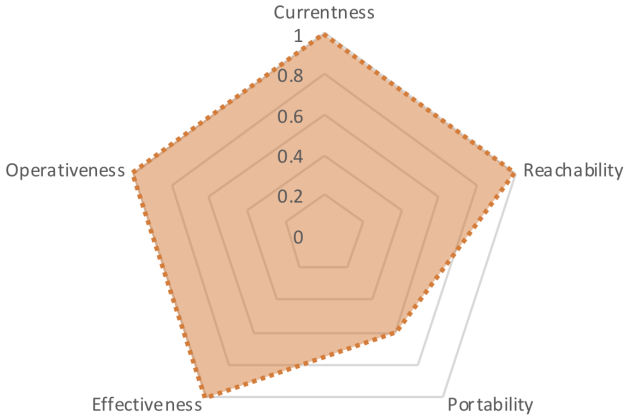


FIGURE B.13: Transparency measurement of requirement 112.1.

B.2.2 222.1 – S must provide P with audit mechanisms.

The evidence used to measure this requirement can be found in the “Record history" section, under “All changes in the last 6 months" (CLM), and also “Views of Username’s record in the last 30 days" (VUR).

Metric	**Attributes**	**Grade**
Reachability	$k = 3$; $N_{\text{int}} = 2 + 2$	0.7165313106
Portability		0.6
Currentness	$t_{max} = 10s$	1
Effectiveness	See Table B.28	0.7
Operativeness	A = {createData, readData, updateData, deleteData}	1

TABLE B.27: Attributes and grades per metric referring to requirement 222.1.

	Delivered Outputs	
Desired Goals	CLM	VUR
What is the action?	✓	✓
When did it happen?	✓	✓
What was the outcome?		
From what source/application?	✓	✓
Which data suffered the action?	✓	

TABLE B.28: Effectiveness matrix 222.1: desirable goals compared with the real outputs. Greyed-out cells represent the non-pertinent goals.

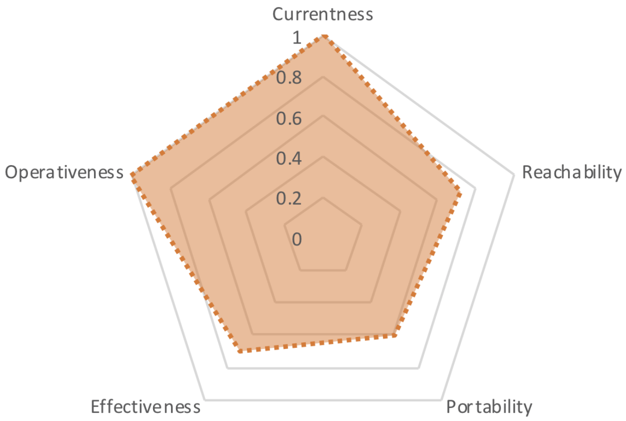


FIGURE B.14: Transparency measurement of requirement 222.1.

B.2.3 232.1 – S must provide P with accountability mechanisms.

The evidence used to measure this requirement can be found in the "Record history" section, under "All changes in the last 6 months" (CLM), and also "Views of Username's record in the last 30 days" (VUR).

Metric	Attributes	Grade
Reachability	$k = 3$; $N_{\text{int}} = 2 + 2$	0.7165313106
Portability		0.6
Currentness	$t_{max} = 10s$	1
Effectiveness	See Table B.30	0.75
Operativeness	$A = \{$createData, readData, updateData, deleteData$\}$	1

TABLE B.29: Attributes and grades per metric referring to requirement 232.1.

	Delivered Outputs	
Desired Goals	CLM	VUR
What is the action?	✓	✓
When did it happen?	✓	✓
What was the outcome?		
Who did the action?	✓	✓
From what source/application?	✓	✓
Which data suffered the action?	✓	

TABLE B.30: Effectiveness matrix 232.1: desirable goals compared with the real outputs. Greyed-out cells represent the non-pertinent goals.

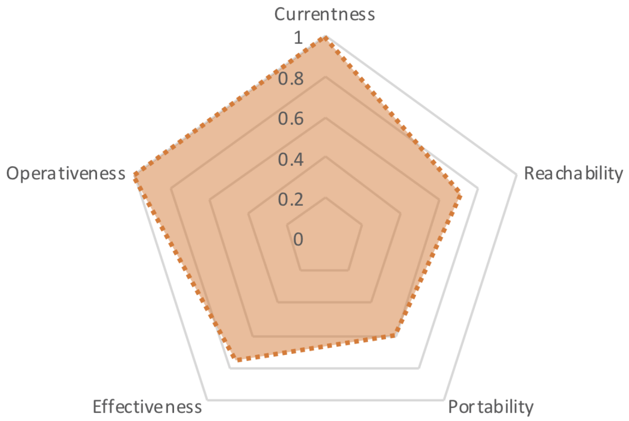


FIGURE B.15: Transparency measurement of requirement 232.1.

B.3 Summary

In what follows, two radar charts are presented to summarise the grades achieved by Microsoft HealthVault in the transparency measurement. The chart depicted in Figure B.16 represents the average grade achieved by the Information-based requirements analysed. While the one in Figure B.17 represents the average grade achieved by Mechanisms-based ones. Metrics not applied (grade shown as N/A) are not counted in the average.

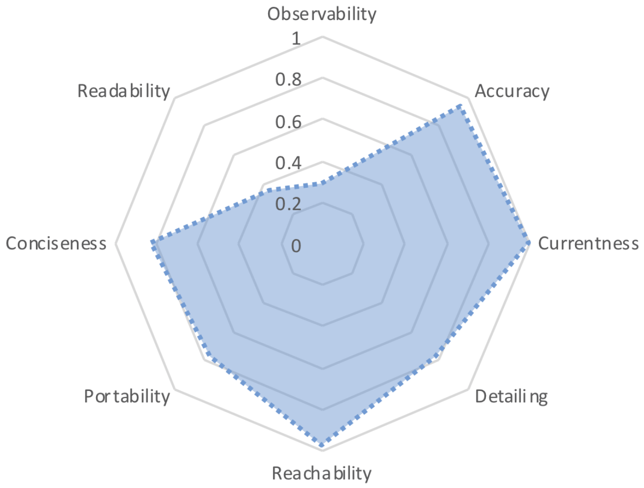


FIGURE B.16: Average of grades for Information-based requirements.

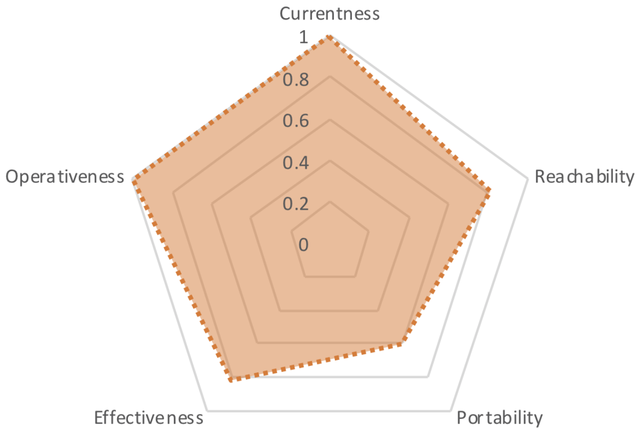


FIGURE B.17: Average of grades for Mechanism-based requirements.

Appendix C

Transparency Enhancing Tools in the context of the GDPR

TETs Art.	ML	P3P	PPL	DT	PI	PRA	GPD	PDT	DM	MMS	EuroPriSe	PS	GD	PEv	TAMI	PTT	PVA	PB	AMI	TArc	openPDS	Digi.me	MD	PeS	Mee	BB	UP	**Total**
5.1.(a)																												0
5.2		x	x	x	x		x	x		x	x		x	x	x	x	x			x	x	x	x	x	x			19
6.1.(a)				x	x		x	x					x								x	x	x	x	x			10
7.1																												0
7.2																												0
7.3				x	x		x	x					x								x	x	x	x	x			10
9.2.(a)																								x*				1
11.2																												0
12.1																												0
12.3																												0
12.4																												0
12.7																												0
13.1.(a)																											x	1
13.1.(b)																											x	1
13.1.(c)		x	x							x																	x	4
13.1.(d)		x	x																									2
13.1.(e)		x	x																									2
13.1.(f)											x									x							x	3
13.2.(a)																												0
13.2.(b)		x	x																									2
13.2.(c)		x	x																									2
13.2.(d)																												0
13.2.(e)																												0
13.2.(f)																												0
13.3																												0
14.1.(a)																											x	1
14.1.(b)																											x	1
14.1.(c)		x	x							x																	x	4
14.1.(d)	x			x	x		x	x	x				x					x	x		x	x	x		x	x		14

14.1.(e)		x	x																									2
14.1.(f)											x									x							x	3
14.2.(a)																												0
14.2.(b)		x	x																									2
14.2.(c)		x	x																									2
14.2.(d)		x	x																									2
14.2.(e)																												0
14.2.(f)	x			x	x		x	x	x				x					x	x		x	x	x		x	x		14
14.2.(g)																												0
14.3.(a)	x						x	x	x				x		x			x			x		x					9
14.3.(b)																												0
14.3.(c)																												0
14.4																												0
15.1.(a)		x	x							x																	x	4
15.1.(b)	x			x	x		x	x	x				x					x	x		x	x	x		x	x		14
15.1.(c)		x	x																									2
15.1.(d)																												0
15.1.(e)		x	x																									2
15.1.(f)																												0
15.1.(g)	x			x	x		x	x	x				x					x	x		x	x	x		x	x		14
15.1.(h)																												0
15.2											x									x							x	3
15.3				x	x		x	x					x						x				x			x		8
16																												0
17				x	x		x	x					x								x	x	x	x	x			10
18																												0
19		x	x																									2
21.1																												0
21.2																												0
21.3																												0
21.4		x	x																									2
21.5																												0
22.1																												0
22.2.(c)																												0

25.3																												0
26.1																												0
26.2																												0
26.3																												0
30.1				x	x									x	x	x	x							x				7
30.2				x	x									x	x	x	x							x				7
30.3																												0
30.4																												0
32.3																												0
33.1																												0
33.2																												0
33.3																											x	1
33.4																												0
33.5																												0
34.1																												0
34.2																												0

TABLE C.1: Transparency Enhancing Tools (TETs) and the GDPR Articles, paragraphs, and sub-paragraphs they help realising (* added manually).

Bibliography

[1] AM Adeshina and R Hashim. "Computational approach for securing radiology-diagnostic data in connected health network using high-performance gpu-accelerated aes". In: *Interdisciplinary Sciences: Computational Life Sciences* 9.1 (2017), pp. 140–152.

[2] Laksono Adhianto et al. "HPCToolkit: Tools for performance analysis of optimized parallel programs". In: *Concurrency and Computation: Practice and Experience* 22.6 (2010), pp. 685–701.

[3] Shaden Al-Aqeeli, Mznah Al-Rodhaan, and Yuan Tian. "Privacy preserving risk mitigation strategy for access control in e-healthcare systems". In: *Informatics, Health & Technology (ICIHT), International Conference on*. IEEE. 2017, pp. 1–6.

[4] A. AL Faresi, D. Wijesekera, and K. Moidu. "A Comprehensive Privacy-aware Authorization Framework Founded on HIPAA Privacy Rules". In: *In Proc. of the 1st ACM International Health Informatics Symposium*. Arlington, Virginia, USA: ACM, 2010, pp. 637–646.

[5] F. Al-Nayadi and J. H. Abawajy. "An Authentication Framework for e-Health Systems". In: *IEEE International Symposium on Signal Processing and Information Technology*. Dec. 2007, pp. 616–620.

[6] F. Al-Nayadi and J. H. Abawajy. "An Authorization Policy Management Framework for Dynamic Medical Data Sharing". In: *The International Conference on Intelligent Pervasive Computing*. Oct. 2007, pp. 313–318.

[7] Yousra Abdul Alsahib S Aldeen, Mazleena Salleh, and Yazan Aljeroudi. "An innovative privacy preserving technique for incremental datasets on cloud computing". In: *Journal of biomedical informatics* 62 (2016), pp. 107–116.

[8] Nagham Alhadad et al. "Trust Evaluation of a System for an Activity". In: *Int. Conf. on Trust, Privacy and Security in Digital Business*. Springer. 2013, pp. 24–36.

[9] A Antonidoss and D Manjula. "Intelligent Data Aggregation and Merging Algorithms for Secured Storage of Medical Information in Cloud". In: *International Journal of Scientific Research in Science, Engineering and Technology* 2.2 (2016).

[10] Article 29 Working Party. *Guidelines on Transparency under Regulation 2016/679*. WP260 rev.01. 2018. 40 pp. URL: http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=622227.

[11] Faezeh Sadat Babamir and Ali Norouzi. "Achieving key privacy and invisibility for unattended wireless sensor networks in healthcare". In: *The Computer Journal* (2013), bxt046.

[12] Elaine Barker. *NIST Special Publication 800-57 Part 1 Revision 4—Recommendation for Key Management (Part 1: General)*. 2016.

[13] Cesare Bartolini et al. "A Framework to Reason about the Legal Compliance of Security Standards". In: *Proceedings of the Tenth International Workshop on Juris-informatics (JURISIN)*. 2016.

[14] R. Basavegowda and S. Seenappa. "Electronic Medical Report Security Using Visual Secret Sharing Scheme". In: *15th International Conference on Computer Modelling and Simulation*. Apr. 2013, pp. 78–83.

[15] Benoit Baudry, Clémentine Nebut, and Yves Le Traon. "Model-driven Engineering for Requirements Analysis". In: *Proc. of the 11th IEEE Int. Enterprise Distributed Object Computing Conference*. IEEE, 2007, pp. 459–466. ISBN: 0-7695-2891-0. DOI: 10.1109/EDOC.2007.15.

[16] Boris Beizer. *Black-box testing: techniques for functional testing of software and systems*. New York, NY, USA: John Wiley and Sons, 1995. ISBN: 0-471-12094-4.

[17] J. Benaloh et al. "Patient Controlled Encryption: Ensuring Privacy of Electronic Medical Records". In: *In Proc. of the 2009 ACM Workshop on Cloud Computing Security*. CCSW '09. Chicago, Illinois, USA: ACM, 2009, pp. 103–114.

[18] Tim Berners-Lee. *Linked Data*. Last accessed in February 2018. 2009. URL: https://www.w3.org/DesignIssues/LinkedData.html.

[19] S. Berthold et al. "Crime and Punishment in the Cloud - Accountability, Transparency, and Privacy". In: *Pre-Proc. of Int. Workshop on Trustworthiness, Accountability and Forensics in the Cloud in conjunction with the 7th IFIP WG 11.11 Int. Conf. on Trust Management* (2013).

[20] Sreedevi N Bharti Ratan Madnani. *Attribute Based Encryption for Scalable and Secure Sharing of Medical Records in Cloud Computing Design and Implementation*. 2013.

[21] Christoph Bier, Kay Kühne, and Jürgen Beyerer. "PrivacyInsight: the next generation privacy dashboard". In: *Annual Privacy Forum*. Springer. 2016, pp. 135–152.

[22] Christian Bizer, Tom Heath, and Tim Berners-Lee. "Linked data-the story so far". In: *International journal on semantic web and information systems* 5.3 (2009), pp. 1–22.

[23] Emma Bondy-Chorney et al. "Staufen1 Regulates Multiple Alternative Splicing Events either Positively or Negatively in DM1 Indicating Its Role as a Disease Modifier." In: *PLoS Genetics* 12.1 (2016), pp. 1 –22. ISSN: 15537390.

[24] Dan Boneh, Ananth Raghunathan, and Gil Segev. "Function-private identity-based encryption: Hiding the function in functional encryption". In: *Advances in Cryptology–CRYPTO 2013*. Springer, 2013, pp. 461–478.

[25] Dan Boneh and Brent Waters. "Conjunctive, subset, and range queries on encrypted data". In: *Theory of Cryptography Conference*. Springer. 2007, pp. 535–554.

[26] Dan Boneh et al. "Public key encryption with keyword search". In: *International Conference on the Theory and Applications of Cryptographic Techniques*. Springer. 2004, pp. 506–522.

[27] Christoph Bösch et al. "A survey of provably secure searchable encryption". In: *ACM Computing Surveys (CSUR)* 47.2 (2015), p. 18.

[28] Christoph Bösch et al. "Selective document retrieval from encrypted database". In: *International Conference on Information Security*. Springer. 2012, pp. 224–241.

[29] Dalel Bouslimi and Gouenou Coatrieux. “A crypto-watermarking system for ensuring reliability control and traceability of medical images”. In: *Signal Processing: Image Communication* 47 (2016), pp. 160–169.

[30] Denis Butin and Daniel Le Métayer. “Log analysis for data protection accountability (Extended Version)”. In: *International Symposium on Formal Methods*. Springer. 2014, pp. 163–178.

[31] Claudia Cappelli. “Uma abordagem para transparência em processos organizacionais utilizando aspectos”. PhD thesis. PUC-Rio, 2009.

[32] David Cash et al. “Highly-scalable searchable symmetric encryption with support for boolean queries”. In: *Advances in Cryptology–CRYPTO 2013*. Springer, 2013, pp. 353–373.

[33] Christopher A. Cassa, Rachel A. Miller, and Kenneth D. Mandl. “A novel, privacy-preserving cryptographic approach for sharing sequencing data.” In: *JAMIA* 20.1 (2013), pp. 69–76.

[34] Don Chalmers. “Biobanking and Privacy Laws in Australia.” In: *Journal of Law, Medicine & Ethics* 43.4 (2015), pp. 703 –713. ISSN: 10731105. URL: http://search.ebscohost.com.proxy.bnl.lu/login.aspx?direct=true&db=aph&AN=111985083&site=ehost-live&scope=site.

[35] Yan-Cheng Chang and Michael Mitzenmacher. “Privacy preserving keyword searches on remote encrypted data”. In: *International Conference on Applied Cryptography and Network Security*. Springer. 2005, pp. 442–455.

[36] Chin-Ling Chen et al. “Design of a secure medical data sharing system via an authorized mechanism”. In: *Systems, Man, and Cybernetics (SMC), 2016 IEEE International Conference on*. IEEE. 2016, pp. 002478–002482.

[37] Min Chen et al. “Privacy protection and intrusion avoidance for cloudlet-based medical data sharing”. In: *IEEE Transactions on Cloud Computing* (2016).

[38] Koji Chida et al. “Implementation and evaluation of an efficient secure computation system using ‘R’ for healthcare statistics”. In: *Journal of the American Medical Informatics Association* 21 (2014), e326–e331.

[39] Kwok Tai Chui et al. “Disease Diagnosis in Smart Healthcare: Innovation, Technologies and Applications”. In: *Sustainability* 9.12 (2017), p. 2309.

[40] Lawrence Chung et al. *Non-Functional Requirements in Software Engineering*. Vol. 5. Int. Series in Software Engineering. Springer US, 2000. 440 pp. ISBN: 978-1-4613-7403-9. DOI: 10.1007/978-1-4615-5269-7.

[41] Gouenou Coatrieux et al. *Watermarking - a new way to bring evidence in case of telemedicine litigation*. 2011.

[42] Common Criteria Consortium and others. *Common Criteria for Information Technology Security Evaluation*. Tech. rep. 2012. URL: https://www.commoncriteriaportal.org/.

[43] R. Cruz-Correia et al. “Integration of Hospital Data Using Agent Technologies - A Case Study”. In: *AI Communications* 18.3 (Aug. 2005), pp. 191–200. ISSN: 0921-7126.

[44] D. Cruzes and M. Jaatun. *D:B-2.4 Requirements Report Deliverable*. 2014.

[45] Daniela S. Cruzes and Martin Gilje Jaatun. “Cloud Provider Transparency: A View from Cloud Customers”. In: *5th Int. Conf. on Cloud Computing and Services Science*. 2015, pp. 30–39. ISBN: 978-989-758-104-5. DOI: 10.5220/0005439000300039.

[46] Reza Curtmola et al. “Searchable symmetric encryption: improved definitions and efficient constructions”. In: *Journal of Computer Security* 19.5 (2011), pp. 895–934.

[47] M. Cutts. *Oxford Guide to Plain English*. Oxford University Press, 2007.

[48] Sourya Joyee De and Daniel Le Métayer. “Privacy risk analysis to enable informed privacy settings”. In: *2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*. IEEE. 2018.

[49] M. A. C. Dekker. “Flexible Access Control for Dynamic Collaborative Environments”. CTIT PhD.-thesis series ISSN 1381-3617, Number 09-159, IPA Dissertation series. PhD thesis. University of Twente, 2009.

[50] Yong-Yuan Deng et al. “Internet of Things (IoT) Based Design of a Secure and Lightweight Body Area Network (BAN) Healthcare System”. In: *Sensors* 17.12 (2017), p. 2919.

[51] Christian Denger, Daniel M. Berry, and Erik Kamsties. “Higher Quality Requirements Specifications through Natural Language Patterns”. In: *Proc. of the IEEE Int. Conf. on Software: Science, Technology and Engineering*. IEEE, 2003, pp. 80–90. ISBN: 0-7695-2047-2. DOI: 10.1109/SWSTE.2003.1245428.

[52] Jannik Dreier, Hugo Jonker, and Pascal Lafourcade. “Defining verifiability in e-auction protocols”. In: *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*. ACM. 2013, pp. 547–552.

[53] Jannik Dreier et al. “A framework for analyzing verifiability in traditional and electronic exams”. In: *Information Security Practice and Experience*. Springer, 2015, pp. 514–529.

[54] Alevtina Dubovitskaya et al. “A multiagent system for dynamic data aggregation in medical research”. In: *BioMed research international* 2016 (2016).

[55] Fatma E.-Z. A. Elgamal, Noha A. Hikal, and F E Z Abou-Chadi. “Secure Medical Images Sharing over Cloud Computing environment”. In: *International Journal of Advanced Computer Science and Applications(IJACSA)* 4.5 (2013).

[56] Organisation for Economic Co-operation and Development. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Organisation for Economic Co-operation and Development, 1980.

[57] Jean Anderson Eloy et al. “Readability assessment of patient education materials on major otolaryngology association websites”. In: *Otolaryngology–Head and Neck Surgery* 147.5 (2012), pp. 848–854.

[58] Jieun Eom, Dong Hoon Lee, and Kwangsu Lee. “Patient-controlled attribute-based encryption for secure electronic health records system”. In: *Journal of medical systems* 40.12 (2016), p. 253.

[59] T. Ermakova and B. Fabian. “Secret Sharing for Health Data in Multi-provider Clouds”. In: *IEEE 15th Conference on Business Informatics*. July 2013, pp. 93–100.

[60] European Commission. *How to write clearly*. Last accessed in May 2018. 2011. URL: https://publications.europa.eu/en/publication-detail/-/publication/c2dab20c-0414-408d-87b5-dd3c6e5dd9a5.

[61] European Privacy Seal. *EuroPriSe Certification Criteria (v201701)*. https://www.european-privacy-seal.eu/EPS-en/Criteria. Last accessed in October 2018. 2017.

[62] A. Ferreira et al. "Envisioning secure and usable access control for patients". In: *IEEE 3rd International Conference on Serious Games and Applications for Health (SeGAH 2014)*. Rio de Janeiro, Brazil, May 2014.

[63] Ana Ferreira and Gabriele Lenzini. "Can Transparency Enhancing Tools Support Patient's Accessing Electronic Health Records?" In: *New Contributions in Information Systems and Technologies*. Springer, 2015, pp. 1121–1132.

[64] Anna Ferreira et al. "How to break access control in a controlled manner". In: *Computer-Based Medical Systems, 2006. CBMS 2006. 19th IEEE International Symposium on*. IEEE. 2006, pp. 847–854.

[65] Eduardo Castelló Ferrer et al. "RoboChain: A Secure Data-Sharing Framework for Human-Robot Interaction". In: *CoRR* abs/1802.04480 (2018). arXiv: 1802.04480. URL: http://arxiv.org/abs/1802.04480.

[66] Ben A Fisch et al. "Malicious-client security in blind seer: A scalable private DBMS". In: *Security and Privacy (SP), 2015 IEEE Symposium on*. IEEE. 2015, pp. 395–410.

[67] S. Fischer-Hübner, J. Angulo, and T. Pulls. "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*. Vol. 421. IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg, 2014, pp. 77–92.

[68] Simone Fischer-Hübner and Leonardo A Martucci. "Privacy in social collective intelligence systems". In: *Social collective intelligence*. Springer, 2014, pp. 105–124.

[69] Simone Fischer-Hübner et al. "Transparency, Privacy and Trust–Technology for Tracking and Controlling My Data Disclosures: Does This Work?" In: *IFIP International Conference on Trust Management*. Springer. 2016, pp. 3–14.

[70] Rudolf Franz Flesch. *How to Write Plain English*. Barnes & Noble, 1981. ISBN: 978-0064635363.

[71] Alejandro Enrique Flores and Victor Medel Vergara. "Functionalities of open electronic health records system: A follow-up study". In: *6th Int. Conf. on Biomedical Engineering and Informatics*. IEEE. 2013, pp. 602–607.

[72] G. Frey and L. Litz. "A measure for transparency in net based control algorithms". In: *IEEE Int. Conf. on Systems, Man, and Cybernetics*. Vol. 3. 1999, 887–892 vol.3. DOI: 10.1109/ICSMC.1999.823345.

[73] Carmen Fernández Gago and David Nuñez. "Metrics for Accountability in the Cloud". In: *Accountability and Security in the Cloud*. Vol. 8937. Lecture Notes in Computer Science. Springer International Publishing, 2015, pp. 129–153. ISBN: 978-3-319-17198-2. DOI: 10.1007/978-3-319-17199-9_6.

[74] Alban Gaignard and Johan Montagnat. "A distributed security policy for neuroradiology data sharing". In: *Stud Health Technol Inform.* 147 (2009), pp. 257–262.

[75] R. Gajanayake, R. Iannella, and T. Sahama. "Sharing with Care: An Information Accountability Perspective". In: *IEEE Internet Computing* 4 (July 2011), pp. 31–38.

[76] Randike Gajanayake et al. "Designing an information accountability framework for eHealth". In: *IEEE Healthcom 2013 15th International Conference on E-Health Networking, Application & Services*. Instituto Superior de Ciências Sociais e Políticas – Technical University of Lisbon, Lisbon, Portugal, 2013. URL: https://eprints.qut.edu.au/60690/.

[77] Y. Gao et al. "Research on K anonymity algorithm based on association analysis of data utility". In: *2017 IEEE 2nd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*. Mar. 2017, pp. 426–432. DOI: 10.1109/IAEAC.2017.8054050.

[78] Craig Gentry. "A fully homomorphic encryption scheme". PhD thesis. Stanford University, 2009.

[79] Martin Glinz. "On Non-Functional Requirements". In: *Proc. of the 15th Int. Requirements Engineering Conf. (RE)*. IEEE, 2007, pp. 21–26.

[80] Eu-Jin Goh et al. "Secure indexes." In: *IACR Cryptology ePrint Archive* 2003 (2003). Available at: http://eprint.iacr.org/2003/216, p. 216.

[81] Oded Goldreich and Rafail Ostrovsky. "Software protection and simulation on oblivious RAMs". In: *Journal of the ACM (JACM)* 43.3 (1996), pp. 431–473.

[82] Philippe Golle, Jessica Staddon, and Brent Waters. "Secure conjunctive keyword search over encrypted data". In: *International Conference on Applied Cryptography and Network Security*. Springer. 2004, pp. 31–45.

[83] Kenneth W Goodman 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". In: *Journal of the American Medical Informatics Association* 18.1 (2011), pp. 77–81.

[84] V. Goudar and M. Potkonjak. "A Robust Watermarking Technique for Secure Sharing of BASN Generated Medical Data". In: *IEEE International Conference on Distributed Computing in Sensor Systems*. May 2014, pp. 162–170.

[85] Government Digital Service. *UK Government Digital Service Style Guide*. Last accessed in May 2018. 2018. URL: https://www.gov.uk/guidance/content-design/writing-for-gov-uk\#short-sentences.

[86] Jewel Greywoode et al. "Readability analysis of patient information on the American Academy of Otolaryngology–Head and Neck Surgery website". In: *Otolaryngology-Head and Neck Surgery* 141.5 (2009), pp. 555–558.

[87] Daniel Grunwell, Randike Gajanayake, and Tony Sahama. "The security and privacy of usage policies and provenance logs in an information accountability framework". In: *Proceedings of the Eighth Australasian Workshop on Health Informatics and Knowledge Management (HIKM2015)*. Vol. 164. Australian Computer Society. 2015, pp. 33–40.

[88] Mohamed Jacem Guezguez, Slim Rekhis, and Noureddine Boudriga. "A Sensor Cloud for the Provision of Secure and QoS-Aware Healthcare Services". In: *Arabian Journal for Science and Engineering* (2017), pp. 1–24.

[89] Sebastian Haas et al. "Aspects of privacy for electronic health records". In: *International Journal of Medical Informatics* 80.2 (2011). Special Issue: Security in Health Information Systems, e26 –e31. ISSN: 1386-5056.

[90] Gill Haddow et al. "'Nothing is really safe': a focus group study on the processes of anonymizing and sharing of health data for research purposes". In: *Journal of Evaluation in Clinical Practice* 17.6 (2011), pp. 1140–1146.

[91] Mohamed Ali Hajjaji, Abdellatif Mtibaa, and El bey Bourennane. *A Watermarking of Medical Image: New Approach Based On "Multi-Layer " Method*. 2011.

[92] Mohamed Ali Hajjaji et al. "A new system for watermarking based on the turbo-codes and wavelet 5/3". In: *13th International conference on Sciences and Techniques of Automatic control & computer engineering*. Tunisia, Dec. 2012.

[93] S.A. Hameed, H. Yuchoh, and W.F. Al-Khateeb. "A model for ensuring data confidentiality: In healthcare and medical emergency". In: *4th International Conference On Mechatronicsw*. May 2011, pp. 1–5.

[94] Soon Hwa Han et al. "Implementation of Medical Information Exchange System Based on EHR Standard". In: *Healthcare informatics research* (2010).

[95] M. Hansen. "Marrying Transparency Tools with User-Controlled Identity Management". In: *The Future of Identity in the Information Society*. Vol. 262. Springer US, 2008, pp. 199–220.

[96] Heather L. Harrell and Mark A. Rothstein. "Biobanking Research and Privacy Laws in the United States." In: *Journal of Law, Medicine & Ethics* 44.1 (2016), pp. 106 –127. ISSN: 10731105.

[97] Mohammad Zahidul Hasan, Md Safiur Rahman Mahdi, and Noman Mohammed. "Secure count query on encrypted genomic data". In: *arXiv preprint arXiv:1703.01534* (2017).

[98] H. Hedbom. "A Survey on Transparency Tools for Enhancing Privacy". In: *The Future of Identity in the Information Society*. Vol. 298. IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg, 2009, pp. 67–82.

[99] N. Henke, T. Kelsey, and H. Whately. "Transparency — the most powerful driver of health care improvement?" In: *Health International* (2011), pp. 64–73.

[100] Martin Henze et al. "A comprehensive approach to privacy in the cloud-based Internet of Things". In: *Future Generation Computer Systems* 56 (2016), pp. 701–718.

[101] Mireille Hildebrandt. "Defining Profiling: A New Type of Knowledge?" In: *Profiling the European Citizen* (2008), pp. 17–45. DOI: 10.1007/978-1-4020-6914-7_2.

[102] A.A. Hossain et al. "Rapid Cloud Data Processing with Healthcare Information Protection". In: *IEEE World Congress on Services*. June 2014, pp. 454–455.

[103] J. Hu, H. Chen, and T. Hou. "A hybrid public key infrastructure solution (HPKI) for HIPAA privacy/security regulations". In: *Computer Standards and Interfaces* 32 (2010), pp. 274 –280. ISSN: 0920-5489.

[104] Vincent C Hu, David Ferraiolo, and D Richard Kuhn. *Assessment of access control systems*. US Department of Commerce, National Institute of Standards and Technology, 2006.

[105] Haiping Huang et al. "Private and secured medical data transmission and analysis for wireless sensing healthcare system". In: *IEEE Transactions on Industrial Informatics* 13.3 (2017), pp. 1227–1237.

[106] Thaís Bardini Idalino, Dayana Spagnuelo, and Jean Everson Martina. "Private Verification of Access on Medical Data: An Initial Study". In: *Data Privacy Management, Cryptocurrencies and Blockchain Technology*. Springer, 2017, pp. 86–103.

[107] IEEE Computer Society. *IEEE Standard for a Software Quality Metrics Methodology*. IEEE Standard 1061-1998. IEEE Computer Society, 1998. DOI: 10.1109/IEEESTD.1998.243394.

[108] International Organization for Standardization. *ISO 9241-11:1998 Ergonomic requirements for office work with visual display terminals (VDTs)*. Part 11: Guidance on usability. 2000.

[109] International Organization for Standardization. *ISO/IEC 27004 Information technology – Security techniques – Information security management – Monitoring, measurement, analysis and evaluation*. Tech. rep. ISO, 2016.

[110] International Organization for Standardization. *ISO/TS 18308:2004 Health informatics - Requirements for an electronic health record architecture*. 2004.

[111] Ryuji Ito. "ID-Link, an Enabler for Medical Data Marketplace". In: *Data Mining Workshops (ICDMW), 2016 IEEE 16th International Conference on*. IEEE. 2016, pp. 792–797.

[112] Mohammad Jafari et al. "Using Digital Rights Management for Securing Data in a Medical Research Environment". In: *Proceedings of the Tenth Annual ACM Workshop on Digital Rights Management*. 2010, pp. 55–60.

[113] M. Janic, J.P. 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.

[114] Yan-Feng Jiang et al. "Access control for rural medical and health collaborative working platform". In: *The Journal of China Universities of Posts and Telecommunications* 20 (2013), pp. 7–10.

[115] Jacob Jinil and G Valarmathi. "An enhanced TBAHIBE-LBKQS technique for privacy preservation in cloud". In: *International Journal of Computer Application* 6.5 (2016).

[116] Seny Kamara and Tarik Moataz. "Boolean Searchable Symmetric Encryption with Worst-Case Sub-linear Complexity". In: *EUROCRYPT (3)*. Springer, 2017, pp. 94–124.

[117] Cem Kaner and Walter P. Bond. "Software Engineering Metrics: What Do They Measure and How Do We Know?" In: *Proc. of the* 10*th* *Int. Symposium on Software Metrics*. IEEE, 2004. ISBN: 0-7695-2129-0. DOI: 10.1109/METRIC.2004.1357896. URL: http://kaner.com/pdfs/metrics2004.pdf.

[118] Duygu Karaoğlan and Albert Levi. "A Survey on the Development of Security Mechanisms for Body Area Networks". In: *The Computer Journal* (2013). DOI: 10.1093/comjnl/bxt077.

[119] Khushabu Kasabwala et al. "Readability assessment of patient education materials from the American Academy of Otolaryngology—Head and Neck Surgery Foundation". In: *Otolaryngology–Head and Neck Surgery* 147.3 (2012), pp. 466–471.

[120] Przemyslaw Kazienko Katarzyna Pasierb Tomasz Kajdanowicz. *Privacy-preserving Data Mining, Sharing and Publishing*. 2013.

[121] Murugesan Kavitha and T. K. Anjana. *Password Authentication Scheme Based On Shape and Text for Secure Sharing Of PHR Using ABE in Cloud*. 2013.

[122] Steven E Keller, Laurence G Kahn, and Roger B Panara. "Specifying software quality requirements with metrics". In: *System and Software Requirements Engineering* (1990), pp. 145–163.

[123] Rajkumar Kettimuthu et al. “A Data Management Framework for Distributed Biomedical Research Environments”. In: *Proceedings of the 2010 Sixth IEEE International Conference on e-Science Workshops*. 2010, pp. 72–79. ISBN: 978-0-7695-4295-9.

[124] K. K. Kim et al. *Development of a privacy and security policy framework for a multistate comparative effectiveness research network*. 2013.

[125] Jason Tyler King, Ben Smith, and Laurie Williams. “Modifying without a trace: general audit guidelines are inadequate for open-source electronic health record audit mechanisms”. In: *Proc. of the 2^{nd} ACM SIGHIT Int. Health Informatics Symposium*. ACM. 2012, pp. 305–314.

[126] René F Kizilcec. “How much information?: Effects of transparency on trust in an algorithmic interface”. In: *Proceedings of the 2016 CHI Conference on Human Factors in Computing Systems*. ACM. 2016, pp. 2390–2395.

[127] Patty Kostkova et al. “Who owns the data? Open data for healthcare”. In: *Frontiers in public health* 4 (2016), p. 7.

[128] Steve Kremer, Mark Ryan, and Ben Smyth. “Election verifiability in electronic voting protocols”. In: *European Symposium on Research in Computer Security*. Springer. 2010, pp. 389–404.

[129] Kaoru Kurosawa. “Garbled Searchable Symmetric Encryption.” In: *Financial Cryptography*. Vol. 2014. 2014, pp. 234–251.

[130] Ralf Küsters, Tomasz Truderung, and Andreas Vogt. “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*. ACM, 2010, pp. 526–535.

[131] C Lakshmi et al. “Encryption and watermark-treated medical image against hacking disease – An immune convention in spatial and frequency domains”. In: *Computer Methods and Programs in Biomedicine* 159 (2018), pp. 11–21.

[132] Stephen Langella et al. “Sharing Data and Analytical Resources Securely in a Biomedical Research Grid Environment”. In: *JAMIA* 15.3 (2008), pp. 363–373.

[133] Ronald Lautenschläger et al. “A generic solution for web-based management of pseudonymized data”. In: *BMC medical informatics and decision making* 15.1 (2015), p. 1.

[134] Wonhyuk Lee et al. “A Virtualized Network Model for Wellness Information Technology Research”. In: *International Conference on IT Convergence and Security*. Dec. 2013, pp. 1–3.

[135] Julio Cesar Sampaio do Prado Leite and Claudia Cappelli. “Software Transparency”. In: *Business and Information Systems Engineering* 2 (2010), pp. 127–139.

[136] Guan-Chen Li et al. “Design of a secure and effective medical cyber-physical system for ubiquitous telemonitoring pregnancy”. In: *Concurrency and Computation: Practice and Experience* 30.2 (2018).

[137] Xiaobai Li and Jialun Qin. “Protecting Privacy When Releasing Search Results from Medical Document Data”. In: *Proceedings of the 51st Hawaii International Conference on System Sciences*. 2018.

[138] Yan Li, Changxin Bai, and Chandan K Reddy. “A distributed ensemble approach for mining healthcare data under privacy constraints”. In: *Information sciences* 330 (2016), pp. 245–259.

[139] David Liebovitz. "Meaningful EHR attributes for an era of accountability, transparency, shared decision making, and value assessment". In: *Journal of Legal Medicine* 34.1 (2013), pp. 43–53.

[140] Jianghua Liu, Xinyi Huang, and Joseph K. Liu. "Secure sharing of Personal Health Records in cloud computing: Ciphertext-Policy Attribute-Based Signcryption". In: *Future Generation Computer Systems* (2014).

[141] Weiran Liu et al. "Auditing Revocable Privacy-Preserving Access Control for EHRs in Clouds". In: *The Computer Journal* 60.12 (2017), pp. 1871–1888.

[142] Yupeng Liu, Yifei Chen, and Gwo-Hshiung Tzeng. "Identification of key factors in consumers' adoption behavior of intelligent medical terminals based on a hybrid modified MADM model for product improvement". In: *International journal of medical informatics* 105 (2017), pp. 68–82.

[143] S. Lohiya and L. Ragha. "Privacy Preserving in Data Mining Using Hybrid Approach". In: *Fourth International Conference on Computational Intelligence and Communication Networks*. Nov. 2012, pp. 743–746.

[144] Ahmed Lounis et al. "Healing on the cloud: Secure cloud architecture for medical wireless sensor networks". In: *Future Generation Computer Systems* 55 (2016), pp. 266–277.

[145] Yang Lu and Richard O Sinnott. "Semantic-Based Privacy Protection of Electronic Health Records for Collaborative Research". In: *Trustcom/BigDataSE, 2016 IEEE*. IEEE. 2016, pp. 519–526.

[146] R Manoj et al. "Hybrid Secure and Scalable Electronic Health Record Sharing in Hybrid Cloud". In: *Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2017 5th IEEE International Conference on*. IEEE. 2017, pp. 185–190.

[147] Glen Marshall. *RFC 3881 - Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications*. Request for Comments. Internet Engineering Task Force (IETF), 2004.

[148] M Marwan, A Kartit, and H Ouahmane. "Design a Secure Framework for Cloud-Based Medical Image Storage". In: *Proceedings of the 2nd international Conference on Big Data, Cloud and Applications*. ACM. 2017, p. 7.

[149] Rene Meis and Maritta Heisel. "Computer-Aided Identification and Validation of Intervenability Requirements". In: *Information* 8.1 (2017), p. 30.

[150] Rene Meis, Roman Wirtz, and Maritta Heisel. "A taxonomy of requirements for the privacy goal transparency". In: *International Conference on Trust and Privacy in Digital Business*. Springer. 2015, pp. 195–209.

[151] Ruslan Mitkov. *The Oxford handbook of computational linguistics*. Oxford University Press, 2005.

[152] Tarik Moataz and Abdullatif Shikfa. "Boolean symmetric searchable encryption". In: *Proceedings of the 8th ACM SIGSAC symposium on Information, computer and communications security*. ACM. 2013, pp. 265–276.

[153] N. Moe. *D:B-2.1 Workshop 1 Results (Requirements)*. Mar. 2013.

[154] Nazila Gol Mohammadi and Maritta Heisel. "A Framework for Systematic Analysis and Modeling of Trustworthiness Requirements Using i* and BPMN". In: *Int. Conf. on Trust and Privacy in Digital Business*. Springer. 2016, pp. 3–18.

[155] Manoranjan Mohanty, Pradeep Atrey, and Wei Tsang Ooi. "Secure Cloud-based Medical Data Visualization". In: *Proceedings of the 20th ACM International Conference on Multimedia*. Nara, Japan, 2012, pp. 1105–1108. ISBN: 978-1-4503-1089-5.

[156] Yves-Alexandre de Montjoye et al. "OpenPDS: Protecting the privacy of metadata through safeanswers". In: *PloS one* 9.7 (2014), e98790.

[157] Michael A Morris et al. "Reinventing Radiology: Big Data and the Future of Medical Imaging". In: *Journal of thoracic imaging* 33.1 (2018), pp. 4–16.

[158] Salwa A. K. Mostafa et al. "Wavelet packets-based blind watermarking for medical image management". In: *The open biomedical engineering journal* 4 (2010), pp. 93–98.

[159] Patrick Murmann and Simone Fischer-Hübner. "Tools for achieving usable ex post transparency: a survey". In: *IEEE Access* (2017).

[160] Glenford J Myers, Corey Sandler, and Tom Badgett. *The art of software testing*. John Wiley and Sons, 2011.

[161] Roderick Neame. *Effective sharing of health records, maintaining privacy: a practical schema*. 2013.

[162] Najmeh Mousavi Nejad, Simon Scerri, and Sören Auer. "Semantic Similarity based Clustering of License Excerpts for Improved End-User Interpretation". In: *Proceedings of the 13th International Conference on Semantic Systems*. ACM. 2017, pp. 144–151.

[163] Thomas Neubauer and Johannes Heurix. "A methodology for the pseudonymization of medical data". In: *International Journal of Medical Informatics* (2011), pp. 190–204.

[164] R. Nithiavathy. "Data integrity and data dynamics with secure storage service in cloud". In: *International Conference on Pattern Recognition, Informatics and Mobile Engineering*. Feb. 2013, pp. 125–130.

[165] I. Nwankwo, S. Hanold, and N. Forgo. "Legal and ethical issues in integrating and sharing databases for translational medical research within the EU". In: *IEEE 12th International Conference on Bioinformatics Bioengineering*. Nov. 2012, pp. 428–433.

[166] Office for Civil Right of the Department of Health and Human Services, USA. *Privacy, Security, and Electronic Health Records*. 2015.

[167] Office of the Privacy Commissioner of Canada. *Privacy Enhancing Technologies – A Review of Tools and Techniques*. https://www.priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/. Last accessed in August 2018. 2017.

[168] Online Computer Library Center, Inc. *Dewey Decimal Classification*. Last accessed in May 2016. URL: https://www.oclc.org/dewey/features/summaries.en.html.

[169] Open Source Initiative. *The Open Source Definition*. Last accessed in May 2016. URL: https://opensource.org/.

[170] Vasilis Pappas et al. "Blind seer: A scalable private dbms". In: *Security and Privacy (SP), 2014 IEEE Symposium on*. IEEE. 2014, pp. 359–374.

[171] Michalis Pavlidis et al. "Trustworthy selection of cloud providers based on security and privacy requirements: Justifying trust assumptions". In: *Int. Conf. on Trust, Privacy and Security in Digital Business*. Springer. 2013, pp. 185–198.

[172] Roel Peeters and Tobias Pulls. "Insynd: Improved privacy-preserving transparency logging". In: *European Symposium on Research in Computer Security*. Springer. 2016, pp. 121–139.

[173] Michael Peters. *The Idea of Openness: Open Education and Education for Openness*. In *The Encyclopaedia of Educational Philosophy and Theory*, M. Peters, T. Besley, A. Gibbons, B. Žarnić, P. Ghiraldelli (eds.) 2010.

[174] Joshua Porter. "Testing the three-click rule". In: *User Interface Engineering* (2003).

[175] Oxford University Press. *Oxford Dictionaries*. Last accessed in May 2016. URL: http://www.oxforddictionaries.com/.

[176] William L. Prosser. "Privacy". In: *California Law Review* 48 (1960).

[177] Tobias Pulls, Roel Peeters, and Karel Wouters. "Distributed privacy-preserving transparency logging". In: *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*. ACM. 2013, pp. 83–94.

[178] Catherine Quantin et al. "The mixed management of patients' medical records: responsibility sharing between the patient and the physician". In: *Studies in health technology and informatics* 156 (2010), 189—200. ISSN: 0926-9630.

[179] Sk Md Mizanur Rahman et al. "Privacy preserving secure data exchange in mobile P2P cloud healthcare environment". In: *Peer-to-Peer Networking and Applications* 9.5 (2016), pp. 894–909.

[180] H. B. Rahmouni et al. *Privacy aware access controls for medical data disclosure on european healthgrids*. 2010.

[181] Hanene Boussi Rahmouni et al. "Privacy compliance and enforcement on European healthgrids: an approach through ontology". In: *Philosophical Transactions of the Royal Society of London A: Mathematical, Physical and Engineering Sciences* 368.1926 (2010), pp. 4057–4072.

[182] Jean Louis Raisaro et al. "MedCo: Enabling Privacy-Conscious Exploration of Distributed Clinical and Genomic Data". In: *4th International Workshop on Genome Privacy and Security (GenoPri 17)*. EPFL-CONF-232605. 2017.

[183] F. Raizaebagha, K. T. Win, and W. Susilo. "A systematic literature review on security and privacy of electronic health record systems: technical perspectives". In: *Health Information Management Journal* 44.3 (2015).

[184] Shruthi Ramdas and K Ankitha. "Advanced Protection for Patient Information in Medical Database". In: *International Journal of Computer Science and Mobile Computing* 6.6 (2017), pp. 478–488.

[185] Philip Raschke et al. "Designing a GDPR-Compliant and Usable Privacy Dashboard". In: *IFIP International Summer School on Privacy and Identity Management*. Springer. 2017, pp. 221–236.

[186] Pradeep Ray and Jaminda Wimalasiri. "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*. IEEE. 2006, pp. 4686–4689.

[187] Vulapula Sridhar Reddy and Barige Thirumala Rao. "A Combined Clustering and Geometric Data Perturbation Approach for Enriching Privacy Preservation of Healthcare Data in Hybrid Clouds". In: *International Journal of Intelligent Engineering and Systems* 11.1 (2018).

[188] Jenni Reuben, Leonardo A Martucci, and Simone Fischer-Hübner. "Automated Log Audits for Privacy Compliance Validation: A Literature Survey". In: *Privacy and Identity Management. Time for a Revolution?* Springer, 2016, pp. 312–326.

[189] Prashant Rewagad and Yogita Pawar. "Use of Digital Signature and Rijndael Encryption Algorithm to Enhanced Security of data in Cloud Computing Services". In: *IJCA Proceedings on Emerging Trends in Computer Science and Information Technology* 2 (Apr. 2012), pp. 5–7.

[190] A Martín del Rey, JL Hernández Pastora, and G Rodríguez Sánchez. "3D medical data security protection". In: *Expert Systems with Applications* 54 (2016), pp. 379–386.

[191] Fatemeh Rezaeibagha and Yi Mu. "Distributed clinical data sharing via dynamic access-control policy transformation". In: *International Journal of Medical Informatics* 89 (2016), pp. 25–31.

[192] Lillian Røstad. "An Initial Model and a Discussion of Access Control in Patient Controlled Health Records". In: *In Proc. of the 3rd International Conference on Availability, Reliability and Security*. Mar. 2008, pp. 935–942.

[193] P. Ruotsalainen et al. *Framework model and principles for trusted information sharing in pervasive health*. 2011.

[194] Stefan Sackmann, Jens Strüker, and Rafael Accorsi. "Personalization in privacy-aware highly dynamic systems". In: *Communications of the ACM* 49.9 (2006), pp. 32–38.

[195] Hare Ram Sah and G Gunasekaran. "Preserving Data Privacy with Record Retrieval using Visual Cryptography and Encryption Techniques". In: *Indian Journal of Science and Technology* 9.32 (2016).

[196] Muneeb Ahmed Sahi et al. "Privacy Preservation in e-Healthcare Environments: State of the Art and Future Directions". In: *Ieee Access* 6 (2018), pp. 464–478.

[197] Anam Sajid and Haider Abbas. "Data privacy in cloud-assisted healthcare systems: state of the art and future challenges". In: *Journal of medical systems* 40.6 (2016), p. 155.

[198] Samer Samarah et al. "An Efficient Activity Recognition Framework: Toward Privacy-Sensitive Health Data Sensing". In: *IEEE Access* 5 (2017), pp. 3848–3859.

[199] Kanthashree Mysore Sathyendra et al. "Identifying the provision of choices in privacy policy text". In: *Proceedings of the 2017 Conference on Empirical Methods in Natural Language Processing*. 2017, pp. 2774–2779.

[200] Hitoshi Satoh et al. "Teleradiology network system using the web medical image conference system with a new information security solution". In: *Proc. SPIE*. 2013.

[201] Klaus Schwab et al. *Personal Data: The Emergence of a New Asset Class*. Last accessed in April 2017. 2011. URL: `https://www.weforum.org/reports/personal-data-emergence-new-asset-class` (visited on 03/15/2017).

[202] Paul M. Schwartz. "Property, Privacy, and Personal Data". In: *Harvard Law Review* 117.7 (2004), pp. 2056–2128. ISSN: 0017-811X. DOI: 10.2307/4093335.

[203] I. Señor and J. Fernández-Alemán. "Security and privacy in electronic health records: A systematic literature review". In: *Journal of Biomedical Informatics* 46.3 (2013), pp. 541–562.

[204] Bhanumathi Selvaraj and Sakthivel Periyasamy. "A review of recent advances in privacy preservation in health care data publishing". In: *International Journal of Pharma and Biosciences* 7.4 (), pp. 33–41.

[205] O. Seneviratne and L. Kagal. "Enabling privacy through transparency". In: *Proc. of the 12th Annual International Conference on Privacy, Security and Trust*. July 2014, pp. 121–128.

[206] Oshani Seneviratne and Lalana Kagal. "Enabling privacy through transparency". In: *Privacy, Security and Trust (PST), 2014 Twelfth Annual International Conference on*. IEEE. 2014, pp. 121–128.

[207] Wong Kok Seng, R.B. Besar, and F.S. Abas. "Collaborative Support for Medical Data Mining in Telemedicine". In: *2nd Information and Communication Technologies*. Vol. 1. 2006, pp. 1894–1899.

[208] Zonyin Shae and Jeffrey JP Tsai. "On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine". In: *Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on*. IEEE. 2017, pp. 1972–1980.

[209] Elaine Shi et al. "Multi-dimensional range query over encrypted data". In: *Security and Privacy, 2007. SP'07. IEEE Symposium on*. IEEE. 2007, pp. 350–364.

[210] Johanneke Siljee. "Privacy transparency patterns". In: *Proceedings of the 20th European Conference on Pattern Languages of Programs*. ACM. 2015, p. 52.

[211] Niharika Singh et al. "Healthcare data privacy measures to cure & care cloud uncertainties". In: *Signal Processing, Computing and Control (ISPCC), 2017 4th International Conference on*. IEEE. 2017, pp. 402–407.

[212] Ben Smith. "Systematizing security test case planning using functional requirements phrases". In: *Proc. of the 33^rd^ Int. Conf. on Software Engineering*. ACM. 2011, pp. 1136–1137.

[213] Mukalel Bhaskaran Smithamol and Sridhar Rajeswari. "Hybrid solution for privacy-preserving access control for healthcare data". In: *Advances in Electrical and Computer Engineering* 17.2 (2017), pp. 31–39.

[214] A. Solanas, A. Martinez-Balleste, and J.M. Mateo-Sanz. "Distributed Architecture With Double-Phase Microaggregation for the Private Sharing of Biomedical Data in Mobile Health". In: *IEEE Transactions on Information Forensics and Security* 8.6 (June 2013), pp. 901–910.

[215] Jiseong Son et al. "Dynamic access control model for privacy preserving personalized healthcare in cloud environment". In: *Technology and Health Care* 24.s1 (2016), S123–S129.

[216] Dawn Xiaoding Song, David Wagner, and Adrian Perrig. "Practical techniques for searches on encrypted data". In: *Security and Privacy, 2000. S&P 2000. Proceedings. 2000 IEEE Symposium on*. IEEE. 2000, pp. 44–55.

[217] Dayana Spagnuelo, Cesare Bartolini, and Gabriele Lenzini. "Metrics for Transparency". In: *Data Privacy Management and Security Assurance: 11th International Workshop, DPM 2016 and 5th Int. Workshop, QASA 2016, Heraklion, Crete, Greece, September 26-27, 2016, Proceedings*. Cham: Springer International Publishing, 2016, pp. 3–18. ISBN: 978-3-319-47072-6. DOI: 10.1007/978-3-319-47072-6_1.

[218] Dayana Spagnuelo, Cesare Bartolini, and Gabriele Lenzini. "Modelling Metrics for Transparency in Medical Systems". In: *International Conference on Trust and Privacy in Digital Business*. Springer. 2017, pp. 81–95.

[219] Dayana Spagnuelo, Cesare Bartolini, and Gabriele Lenzini. "Qualifying and Measuring Transparency (A Medical Data System Use Case)". In: *Computers & Security* (2018). **Under review; Submitted in August 2018**.

[220] Dayana Spagnuelo, Ana Ferreira, and Gabriele Lenzini. "Accomplishing Transparency within the General Data Protection Regulation". In: *5th International Conference on Information Systems Security and Privacy*. **To appear**. 2018.

[221] Dayana Spagnuelo and Gabriele Lenzini. "Patient-Centred Transparency Requirements for Medical Data Sharing Systems". In: *New Advances in Information Systems and Technologies*. Ed. by Álvaro Rocha et al. Cham: Springer International Publishing, 2016, pp. 1073–1083. ISBN: 978-3-319-31232-3. DOI: 10.1007/978-3-319-31232-3_102.

[222] Dayana. Spagnuelo and Gabriele Lenzini. *Security on medical data sharing (a literature review)*. http://hdl.handle.net/10993/23241. Mar. 2015.

[223] Dayana Spagnuelo and Gabriele Lenzini. "Transparent Medical Data Systems". In: *Journal of Medical Systems* 41.1 (2016), p. 8. ISSN: 1573-689X. DOI: 10.1007/s10916-016-0653-8.

[224] Grzegorz Spyra, William J Buchanan, and Elias Ekonomou. "Sticky policies approach within cloud computing". In: *Computers & Security* 70 (2017), pp. 366–375.

[225] Philip B Stark and David Wagner. "Evidence-based elections". In: *IEEE Security & Privacy* 10.5 (2012), pp. 33–41.

[226] J. Stevovic et al. "Compliance aware cross-organization medical record sharing". In: *IFIP/IEEE International Symposium on Integrated Network Management*. May 2013, pp. 772–775.

[227] Kieran Sullivan, Jim Clarke, and Barry P. Mulcahy. "Trust-terms Ontology for Defining Security Requirements and Metrics". In: *Proc. of the 4th Eur. Conf. on Software Architecture: Companion Volume*. ECSA '10. Copenhagen, Denmark: ACM, 2010, pp. 175–180. ISBN: 978-1-4503-0179-4.

[228] Richard Berntsson Svensson, Tony Gorschek, and Björn Regnell. "Quality Requirements in Practice: An Interview Study in Requirements Engineering for Embedded Systems". In: *Requirements Engineering: Foundation for Software Quality*. Vol. 5512. LNCS. Springer-Verlag, 2009, pp. 218–232. ISBN: 978-3-642-02049-0. DOI: 10.1007/978-3-642-02050-6_19.

[229] Paul C Tang and David Lansky. "The missing link: bridging the patient–provider health information gap". In: *Health Affairs* 24.5 (2005), pp. 1290–1295.

[230] T. Tashiro et al. "Practice and Experience of Building a Medical Application with PERMIS-based Access Control Mechanism". In: *The Sixth IEEE International Conference on Computer and Information Technology*. Sept. 2006, pp. 71–71.

[231] Takahito Tashiro et al. "Architecture of authorization mechanism for medical data sharing on the grid". In: *Studies in health technology and informatics* 120 (2006), 358—367.

[232] Danan Thilakanathan et al. "A Platform for Secure Monitoring and Sharing of Generic Health Data in the Cloud". In: *Future Gener. Comput. Syst.* (June 2014), pp. 102–113. ISSN: 0167-739X.

[233] Adrian Thorogood and Ma'n H Zawati. "International Guidelines for Privacy in Genomic Biobanking (or the Unexpected Virtue of Pluralism)". In: *The Journal of Law, Medicine & Ethics* 43.4 (2015), pp. 690–702.

[234] Ye Tian et al. "A Fast Search Method for Encrypted Medical Data". In: *IEEE International Conference on Communications Workshops*. June 2009, pp. 1–5.

[235] Yue Tong et al. "Cloud-assisted mobile-access of health data with privacy and auditability". In: *IEEE Journal of Biomedical and Health informatics* 18.2 (2014), pp. 419–429.

[236] TrustArc. *Enterprise Privacy & Data Governance Practices Certification Assessment Criteria*. https://www.trustarc.com/products/enterprise-privacy-certification/. Last accessed in October 2018. 2018.

[237] M. Turilli and L. Floridi. "The ethics of information transparency". In: *Ethics and Information Technology* 11.2 (2009), pp. 105–112.

[238] Axel Van Lamsweerde et al. *Requirements engineering: from system goals to UML models to software specifications*. John Wiley & Sons, 2009.

[239] Verizon. *2018 Data Breach Investigations Report*. https://www.verizonenterprise.com/verizon-insights-lab/dbir/. Last accessed in October 2018. 2018.

[240] P. M. Vieira-Marques et al. "Secure Integration of Distributed Medical Data Using Mobile Agents". In: *IEEE Intelligent Systems* 6 (Nov. 2006), pp. 47–54.

[241] Gianluigi Viscusi, Carlo Batini, and Massimo Mecella. "Information systems for eGovernment: A quality-of-service perspective". In: Springer-Verlag, 2010. Chap. 7, pp. 127–144.

[242] P. de Vlieger et al. "Sentinel e-health network on grid: developments and challenges". In: *Stud Health Technolol Inform* 159 (2010).

[243] Zhijie Wang et al. "Efficient attribute-based comparable data access control". In: *Computers, IEEE Transactions on* 64.12 (2015), pp. 3430–3443.

[244] Samuel D Warren and Louis D Brandeis. "The right to privacy". In: *Harvard Law Review* (1890), pp. 193–220.

[245] Brent R Waters et al. "Building an Encrypted and Searchable Audit Log." In: *NDSS*. Vol. 4. 2004, pp. 5–6.

[246] D. Weerasinghe and R. Muttukrishnan. "Secure Trust Delegation for Sharing Patient Medical Records in a Mobile Environment". In: *7th International Conference on Wireless Communications, Networking and Mobile Computing*. Sept. 2011, pp. 1–4.

[247] Daniel J Weitzner et al. "Information accountability". In: *Communications of the ACM* 51.6 (2008), pp. 82–87.

[248] Edgar A Whitley and Nadja Kanellopoulou. "Privacy and Informed Consent in Online Interactions: Evidence from Expert Focus Groups." In: *ICIS*. Citeseer. 2010, p. 126.

[249] Chathurika Wickramage, Tony Sahama, and Colin Fidge. "Anatomy of log files: Implications for information accountability measures". In: *e-Health Networking, Applications and Services (Healthcom), 2016 IEEE 18th International Conference on*. IEEE. 2016, pp. 1–6.

[250] Shomir Wilson et al. "The creation and analysis of a website privacy policy corpus". In: *Proceedings of the 54th Annual Meeting of the Association for Computational Linguistics (Volume 1: Long Papers)*. Vol. 1. 2016, pp. 1330–1340.

[251] Qi Xia et al. "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments". In: *Information* 8.2 (2017), p. 44.

[252] Qi Xia et al. "MeDShare: Trust-Less Medical Data Sharing Among Cloud Service Providers via Blockchain". In: *IEEE Access* 5 (2017), pp. 14757–14767.

[253] Yang Yang et al. "Lightweight sharable and traceable secure mobile health system". In: *IEEE Transactions on Dependable and Secure Computing* (2017).

[254] Christina Zarcadoolas. "The simplicity complex: exploring simplified health messages in a complex world". In: *Health promotion international* 26.3 (2011), pp. 338–350.

[255] Huiqi Zhao. "Framework Research on Privacy Protection of PHR Owners in Medical Cloud System Based on Aggregation Key Encryption Algorithm". In: *Revista de la Facultad de Ingeniería* 32.15 (2017).

[256] Christian Zimmermann. "A categorization of Transparency-Enhancing Technologies". In: *arXiv preprint arXiv:1507.04914* (2015).