Privacy Value Modeling: A Gateway To Ethical Big Data Handling

Syeda Amna Sohail[1][0000-0001-8078-0411], Johannes Krabbe[2][0000-0003-1585-9304], Patrício de Alencar Silva[3][0000-0001-6827-1024], ,and Faiza Allah Bukhsh[4][0000-0001-5978-2754]

[1] University of Twente, 7522NB Enschede, The Netherlands
s.a.sohail@utwente.nl
[2]Medische Spectrum Twente, Medlon BV, 7500 KA Enschede, The Netherlands
j.krabbe@mst.nl
[3]Universidade Federal Rural do Semi-Arido – UFERSA, Mossoro, RN, Brazil
patricio.alencar@ufersa.edu.br
[4] University of Twente, 7522NB Enschede, The Netherlands
f.a.bukhsh@utwente.nl

Abstract. EU through General Data Protection Regulation, GDPR, stipulates to safeguard EU citizens fundamental rights by ensuring ethical, uninterrupted, big data sharing within and outside EU. Healthcare data is no exception to this. While dealing with big data, healthcare providers, Big Data Analysts(BDAs) and government bodies have collectively realized that patients values are to be prioritized for patients optimal value care and for an efficient healthcare system at large. To ensure patients value care, privacy, inter alia, is incorporated both by design within each domain's data base and by policy via international, pan-European and national laws and regulations. This also became viable by standardizing the Information Security Management System (ISMS) indicators for healthcare providers and regulators alike. Lack of standard respective metrics for each privacy assuring parameter, constrains privacy from becoming an objective value object for each value actor. Still, privacy can be seen transforming from being a subjective value for each value actor to a (subjective) value object in healthcare setup. To confirm this concept, this paper is based on two value models. Both models are built using E^3- value kit on the guidelines of Padlock Chain Model in a Dutch healthcare setting. First model is built to represent the current state of privacy protecting data/information sharing between patients and healthcare providers (from the patients perspective). Later, the focus is drawn upon the privacy assuring bilateral relationships between Lab (biobank and bio-depositary) and other key value actors. In future our endeavor will be to quantitatively measure privacy by design constituents i.e. Minimization, Enforcement and Transparency at the backdrop of privacy by policy (ISMS) indicators i.e. availability, integrity, confidentiality and accountability. Experts opinions are included to evaluate the viability of the model discussed for privacy-ensuring healthcare data sharing both on healthcare sector and on technical grounds.

Keywords: , Privacy Protection, E^3-value Model, Patients optimal-care.

1 Introduction

It is todays reality that all of us are intricately entangled via information based economy and are bound to face the repercussions of this rapid technological advancement (either good or bad). Information based economy has changed the way we govern, socialize, do research and business [1]. Correct use of big data, by implying apt data techniques, can enhance the possibilities of efficient and effective services and the quality goods provided [2]. However there are also concerns regarding the fair use of data [3,4]. Not only at the onset of data handling but each step in data pipeline can give vent to ethical issues pertaining to inaccuracy, inequality, non-transparency, intrusion [1]. Moreover today's world of ICT is so pervasive and ubiquitous that it is nearly impossible to identify that who is behind what [5]. However, this does not mitigate the importance of data pooling or in simple words data sharing. Data sharing is coordinated data pooling amongst organizations or nation states. This involves multiple monetary, temporal, language based, privacy and security oriented constraints. However, it is capable of giving vent to more impactful far reaching outcomes than the sum of respective separate outcomes [6]. Thus, Data sharing/data pooling is quintessential for the better insights across sectors and across nation states.

General Data Protection Regulation, GDPR [7] normative promises to ascertain socially responsible big data practices in the best interest of its citizens and in a way that it facilitates technologically driven businesses by pooling data across EU. Protecting privacy and improving the control over the personal info of EU's citizens are also of vital importance for EU's political drive. On the other hand, provision of sharing healthcare data across borders in EU is integral for collective healthcare advancement across EU. The latter is part of Articles 7-8 of Charter of Fundamental Rights of the European Union on the "respect for private and family life" and the "protection of personal data", respectively [8]. While passing through various data travel paths, to maintain patients privacy, GDPR, inter-alia, entails that patient data must only be used for research after patient's informed consent. Exception remains for quality control and improvement purposes. For some researchers [9]. Informed consent in addition to disintegrated healthcare providers, diversified governance structures, intricate legal and ethical pre requisites of each data subject collectively can potentially hinder the efficient data handling in EU. To counter this, an urge is felt to anchor those fast advancing technological tides in the best of social interest where policy, society and science aggroup [10].

For overall satisfaction of the patient, patient's trust upon the healthcare providers is quintessential. Trust being an integral part of any value model, has to persist between the value actors throughout the healthcare service for healthy outcomes. And to that end healthcare providers are moving from volume based fee-reimbursement healthcare model to value based, patient centric healthcare model [11]. This affirms the shift from exclusively monetary gains oriented healthcare to more value based healthcare system [12]. In a value based healthcare system, physical/tangible or first order value transactions between the value actors appear exactly the same as that of volume based healthcare but the latter contains qualitative intrinsic value as it equally values patients satisfaction along with patients health improvement [19]. Shared decision making, an integral part of value based healthcare model, inculcates that during a healthcare process from presentation of the ailment by the patients to the healthcare provider to his/her diagnosis, treatment and to healthcare outcome, each step is mutually decided between the provider and the patient for the latter's engagement, adherence, effective and efficient cost involving decision making and overall satisfaction [13]. Patients values, preferences and overall satisfaction is integral for the long lasting sustainability of the healthcare services [14]. The value based healthcare is largely practiced for more cost effective, quality assuring and more patient engaging health outcomes for the benefit of related stakeholders ranging from healthcare providers to the patient himself [15].

At organizational level Big Data Analysts BDA have diagnosed a number of values that are generally prioritized by healthcare providers while dealing with healthcare data [16]. Amongst those ten enumerated values, 4 of them are directly related to patients information security, namely personalized healthcare, patients value care risks, privacy protection, transparency while the rest 6 are related to the uninterrupted efficient healthcare data sharing. Though privacy protection is considered as the least valued organizational value by BDAs but it is well integrated in respective domain's systems in the form of Privacy by design/architecture. Privacy by architecture is system based which incorporates ISMS standard parameters in alignment with organization's objectives and goals. This takes place in three phases namely minimization, enforcement, and transparency [17]. On the other hand, Privacy by policy for organizations and individuals is the application of regulations, laws, policies and processes by which personal information is managed [18]. It is mainly related to privacy securing data processing of the data subjects. Its bi-product is Information Security Management System (ISMS) with availability, integrity, confidentiality and accountability as its standard indicators. First two indicators encompass "patients security" and the remaining two involve "patients privacy" which collectively come under the tag of Information Security [19]. Apt security measures are designed at administrative as well as at technical level to protect Information Security. Privacy by design and privacy by policy encourages the idea of treating privacy as a subjective value object as they set standardized indicators for value actors to offer and receive.

Value modeling bridges the gap between IT and organizational undertakings and that is what needed for this research. E^3-value toolkit is chosen for the purpose to highlight values of key stakeholder and their respective value transfers.

The paper comprises three sections. First section is based on the introduction, state of the art, problem statement and cause of the paper. Second section constitutes Privacy as a (subjective) value object, objective of using e^3-value model, first model using ontology of Padlock Chain Model, its discussion and then the second model using Padlock Chain Model ontology and its discussion, is followed by the limitation of the second model and conclusion in the end.

2 Privacy As A Value Object

Privacy is a fundamental human right [20] at European level (European Convention on Human Rights) [8] and also as per national constitutions and charters of rights. Idea of privacy is sometimes elusive and far reaching. From the right to be forlorn, to control over personal information, to the rights and responsibilities relating individuals and organizations with respect to their collection, execution, disclosure, and retention of personally identifiable information (PII) all come under the tag of privacy. Moreover, legally, privacy violations are reap with consequences where hefty compensations are to be faced as per GDPR, 2018. From Consumerism perspective, privacy is protected, apt use of the personal information of customers/data subjects, and the meeting of expectations of customers about its use. This may entail the idea of informed consent of the data subjects (consumers/customers) and the idea of patients respective notice and choice as per privacy by policy suggested by Spiekermann and Cranor [18]. Privacy has been an integral fundamental right which needs to be protected but is regarded as given less of an attention when dealt in big data handling, storage, processing, recovery and data retention [5,8]. Bigger data and better algorithms have gradually mitigated the significance of privacy breaches of individuals in favor of their informed consent [3]. If emerging technologies are to be classified with respect to their ethical issues, each one is diagnosed to have the prime issue of privacy protection [4]. Shift of autonomy and decision making is moving from individuals to technology [5]. Considering the importance of privacy assurance and the fears it entails, it is vital to first evaluate the current situation and then to entail measures to guarantee privacy protection by setting set standards for all stake holders with standardized indicators and their respective metrics.

In this wake, the presence of both i.e. privacy by policy and privacy by architecture is highlighted. By modeling the value actors in an e^3-value model and by highlighting privacy as a (subjective) value object for the market segment of patients that can be offered and received as a value object along with some other tangible value activity. Privacy being a subjective term (varies as per ontological requirements/ priorities of each value actor) is not explicitly defined in each value transaction rather other physical and tangible services/products are depicted where the privacy as a (subjective) value object is always intrinsic. Still, Privacy can be deemed as a (subjective) value object as it satisfies four possible attributes to be called as a value object in padlock chain model. Privacy can be reckoned as a value object if it proves to have attributes given below. Below are the attributes with respective logic that proves privacy to be a (subjective) value object:

1. Business goal: Service-based Logic ascertains that patients are prioritized and so is their right over control of their data sharing.
2. Proof of Performance (POP): When healthcare services are regulated by Independent Regulatory Authorities.
3. Accreditation: when the services are accredited by standard authorities, in this case International Standard Organization (ISO) and Netherlands standard authority (NEN).
4. Exchanged against healthcare data/patients sensitive information: This is what expected by the patients.

Currently all above mentioned indicators are satisfied for the privacy to be considered as a value object but subjectively. Because the level of its measurement is only nominal(named indicators) but lags behind in ordinal(set order of priority), interval (proportionate order), ratio (quantitatively calculable) based measurements. The research aims to proceed step by step from nominal to ratio based measurement of privacy preservation within and amongst healthcare provider's information systems by focusing on lab as an epicenter. This paper is based on the first step in providing the ground for the privacy to be called as a value object, subjective though, to proceed further.

Privacy protection is expected by the patients from every domain that is directly or indirectly involved, in first data sharing and then data handling, that carries patients personal information. It is to keep in mind that when data securing sensitive personal information is collected, stored or accessed, different data protection requirements are met in different phases of data handling. Similarly different privacy issues arise at different stages of data handling and are handled differently as per organizational objectives and goals. As e^3-value model focusses more on the stakeholders and their respective priorities, similarly value based healthcare model prioritize patients for the benefit of all.

2.1 Objective behind using E^3-value model

E^{3-}value model can be an apt source to highlight certain very integral elements from the onset of this research in a conveniently understandable manner [21]. E^3-value model provides with the web of enterprises where value actors (stakeholders) are highlighted from the "creation, execution and consumption" of the value objects i.e. goods and services. In this value mode the first model will be shaped from the perspective of patients as a market segment interacting with other value actors at the onset of an ailment.

It becomes evident that "Who is offering what of value to whom and expects what in return?" In an ideal patients value care scenario, If a patient offers his/her sensitive personal info to other value actors, Privacy is a common factor which he expects in return along with other healthcare outcomes. As an element of consumerism, key stakeholders are ideally the data subjects and in this case the market segment of patients are selected to testify the postulates of privacy by policy (being an integral part of GDPR, 2018). Linear relationships make it evident that value actors who come in contact with one another for a period of time (generally with an ailment) and undergo value transfers of value objects are part of an ideal situation where they trust one another for the timely mutual satisfaction of their respective needs. So trust is a constant in e3-value model.

It is assumed that with e3-value model it will be easier to unravel the optimal value care which assures patients privacy with uninterrupted, pooling of medical data.

Following are the two models with their respective discussions, concept, scope, conclusion and references are in the end.

Both the models are built on the guidelines of Padlock Chain Model in Dutch healthcare setting. First Model is taken form the patients perspective, later, in second model, the focus is drawn between the privacy assuring bilateral relationship between Lab (biobank and bio-depositary) with other key stake holders in Dutch backdrop. Value actors are divided into four main heading that are following:

1. Principals: who wish to satisfy their prime need.
2. Agent: chosen by the principal to satisfy his/her prime need.
3. Regulator: bodies to regulate and give accreditations to the healthcare providers, if the latter manage to satisfy the pre requisites of being privacy preserving entities.
4. Third Party: instituted to assist and facilitate the agents but are not in direct contact with the principal.

Similarly these four main actors perform following four main activities.

1. Front-end activity (principal undergoes).
2. Counter response (Agent responds to the front end activity).

3. Regulation and giving accreditations to the health care providers (regulators and international and national standard organizations regulate and give accreditations).
4. Back-end activity (performed by third party).

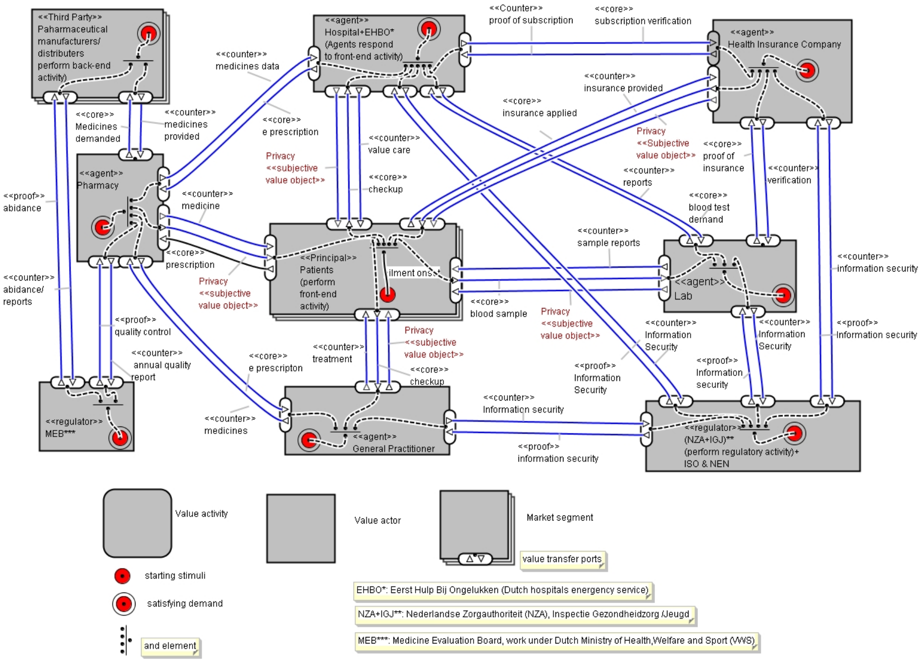
Aim is to analyze privacy protecting measures with simultaneous, uninterrupted, pooling of healthcare data across different domains of healthcare providers.

2.2 Model 1:

It is largely assumed that to draw an e^3-value model, physical or tangible value transactions are recommended as they are better wholly demonstrated which is in contrast to the qualitative value transactions such as, privacy, security, transparency, autonomy, confidentiality. As the latter ones are all respective terms and depend largely upon the purposes and requirements of the stakeholders involved. E^3-value model is opted in representing privacy from being a subjective value to a (subjective) value object in a value model as it satisfies all four attributes to become a value object (explained earlier in privacy as a value object) in an e^3-value model. Besides, It becomes easier to utilize e^3-value model for otherwise complex healthcare eco system as it focuses on linear inflow and outflow of the value transfers within a time frame between key value actors. Which makes it easier to locate the temporal and spatial transactions between the value actors involved in a value model and to diagnose the bottlenecks(if there are any) in performing effectively and efficiently a value transaction. In future, to quantitatively measure the value objects, indicators will provide us with the required parameters for the measurement and analysis of the value objects exchanged. For quantitatively measuring privacy for the healthcare providers each domain's implementation, enforcement and transparency (privacy by design) will be evaluated at the backdrop of ISMS indicator i.e. availability, integrity, confidentiality and accountability which are sub groups of patients security and patients privacy respectively and together form Patients information security as is prescribed by privacy by policy. See **Fig. 1**.

Discussion. The ontology is used to represent value network to match privacy protecting data base requirements while sharing sensitive healthcare data. It is based on Padlock Chain Model with focus on privacy protection [22]. In this model value actors are divided as per their roles i.e. principal, agent, regulators and third party actors. The principal at the onset of a prime need, delegates duty to the agent, who performs the duty in a confined period of time called contract [23]. Contracts that are outcome oriented are most efficient as they co-align the agents priorities with that of the principal regarding risk sharing. This gives vent to the rewards to the agents that emanate out of patients value care [23]. The Statement of Applicability (ISO 27001 Clause 6.1.3 d) is this link between the risk assessment and treatment and the implementation of information security. Similarly transparent information system also serves the principal as it reveals the agents undertakings form the beginning of the contract [23]. The Netherlands certified Transparency in Healthcare On 7 September 2015, according to the international ISO27001 and the Dutch NEN7510 standards for Information Security Management Systems (ISMS). This guarantees that Transparency in Healthcare (TiH) meets the highest standards for data security and regulatory compliance [24]. Some healthcare providers are on the lead in this then the rest. Hospitals usually make a transparency window with the patient for the satisfaction but rest of the providers including general practitioners lag far behind in this. Regulators are of two kinds. One kind covers the International Standard Organizations (ISO) and national standard organization

(NEN) that give accreditations to the healthcare providers after finding them in compliance with the former. The other kind is of Agencies like Inspectie Gezondheidzorg / jeugd (IGJ) that keep an oversight and have powers to ask the healthcare providers for compensations if found non-abiding [25]. IGJ works along with governmental independent regulatory authority, Nederlandse ZorgAuthoriteit (NZA). NZA offers least regulation and facilitates competition in highly disintegrated Dutch healthcare market [28]. That ranges from large number of health insurance companies, to private/semi-private hospitals, from numerous pharmacies to labs. Patients are mostly open to whichever hospital, general practitioner, pharmacy or health insurance they wish to choose from.



<<Third Party>> Paharmaceutical manufacturers/ distributers perform back-end activity)
<<agent>> Hospital+EHBO* (Agents respond to front-end activity)
<<Counter>> proof of subscription
<<core>> subscription verification
<<agent>> Health Insurance Company
<<counter>> medicines data
<<core>> Medicines demanded
<<counter>> medicines provided
<<core>> e prescription
<<counter>> insurance provided
<<core>> insurance applied
Privacy <<Subjective value object>>
<<core>> proof of insurance
<<counter>> verification
<<counter>> value care
Privacy <<subjective value object>>
<<core>> checkup
<<counter>> reports
<<core>> blood test demand
<<agent>> Pharmacy
<<proof>> abidance
<<counter>> medicine
<<counter>> sample reports
<<core>> prescription
<<Principal>> Patients (perform front-end activity)
ilment ons
<<agent>> Lab
<<counter>> information security
<<counter>> abidance/ reports
Privacy <<subjective value object>>
<<core>> blood sample
Privacy <<subjective value object>>
<<proof>> quality control
Privacy <<subjective value object>>
<<counter>> Information Security
<<counter>> Information Security
<<proof>> Information security
<<counter>> annual quality report
<<core>> e prescripton
<<counter>> treatment
<<core>> checkup
<<proof>> Information Security
<<proof>> Information security
<<counter>> Information security
<<regulator>> MEB***
<<counter>> medicines
<<agent>> General Practitioner
<<regulator>> (NZA+IGJ)** (perform regulatory activity)+ ISO & NEN
<<proof>> information security
Value activity
Value actor
Market segment
value transfer ports
starting stimuli
satisfying demand
and element
EHBO*: Eerst Hulp Bij Ongelukken (Dutch hospitals energency service)
NZA+IGJ**: Nederlandse Zorgauthoriteit (NZA), Inspectie Gezondheidzorg /Jeugd
MEB***: Medicine Evaluation Board, work under Dutch Ministry of Health,Welfare and Sport (VWS)

Fig. 1. Padlock Chain Model with privacy as a (subjective) value object.

During value transfers, for patients, there is an outflow of data carrying personal sensitive info of the patient to the domain specific healthcare provider such as General Practitioner, pharmacy, hospital + EHBO, lab (biobank and bio repository) and health insurance company and expected inflow of the privacy as a (subjective) value object from the respective domain as per their security systems. For better insight one of the key healthcare providers are to be analyzed as the framework is represented in second model to evaluate the privacy protecting bilateral relationships between lab (biobank and biorepository) and other key stakeholders see model 2 below (from enterprises perspective), see Fig. 2.

2.3. Model 2:

Laboratories (Biobanks and biorepositories) play a pivotal role to facilitate healthcare data sharing. Samples and data collected from them pave the way for valuable health research. Efficient sharing and pooling of this data is an important prerequisite for advancements in biomedical science [9]. In this wake, data curation is integral initially, for first hand data based insights and later for future reference to rightly anticipate and derive. With increased access to and collective databases from multiple sources, better insights from records of patient data in the form of data catalogues is achievable. In this respect, apprehension resides regarding "where the data goes to", "by whom it is used" and "for what purpose" which, so far, had not been dealt aptly [29]. To simplify the understanding of this rather complex value network padlock chain model provides linear and easily comprehensible model to start with. This model represents labs bilateral relationship with other key value actors in privacy protecting, healthcare data sharing. Here again, as is evident from the model below, actors are distributed as per their respective goals and are named as principal, with prime need, agent, who is assigned to fulfil the prime need, third party, who performs duties to facilitate the agent but is not in direct contact with the principal and regulator, who regulates and gives accreditations to healthcare providers if found abiding. All these actors do value transactions as front end activity, counter activity, back end activity and regulation respectively. They make use of their respective "privacy by design" parameters instilled in their respective data bases. Simultaneously, Privacy by policy is ensured by International and national standard organizations along with domain specific national regulatory authority. Informed consent plays an important role in completing the privacy preserving healthcare data sharing within and across healthcare providers. Labs are obliged to take informed consent of the patients before taking their bio samples or to collect their sensitive data. There is a big loophole as the informed consent in labs is based upon an opt out procedure instead of being an opt in procedure. This means that patients can opt out of becoming data subjects for further scientific studies or clinical trials if they explicitly say so. Else they are considered to be confirming to the terms and conditions of becoming data subjects for both clinical trials and clinical studies. Once granted informed consent, the lab's processing of patients data is also subjected to further scrutiny and justly so [25][26].

Discussion: Informed consent serves as a starting point for both, "privacy by design" and "privacy by policy". But it is shown as a part of privacy by policy in model 2 (see below) because it is obligatory upon lab (biobank and biorepository) to take informed consent at the onset of the patients interaction with the lab or at the beginning of the contract. Rest of the privacy preserving procedures serve as succeeding steps to informed consent.

International and national standard organizations/ NGOs play significant role in setting standard ISMS parameters for Dutch privatelab in Dutch healthcare setting.

Non-governmental organizations (NGOs) like Interna-tional Organization for Standardization (ISO) and NEN, Dutch Network of standardi-zation bounds labs to follow privacy by policy rules and regulations. ISO, an interna-tional federation of national standards bodies from 164 countries including NEN, facil-itates standardization processes to support the international exchange of goods and ser-vices. NEN is the Dutch network within the Netherlands for development of standardsand their respective application nationally and internationally. These NGOs along with regulator and the informed consent context allows labs to instill privacy in their value network by policy.

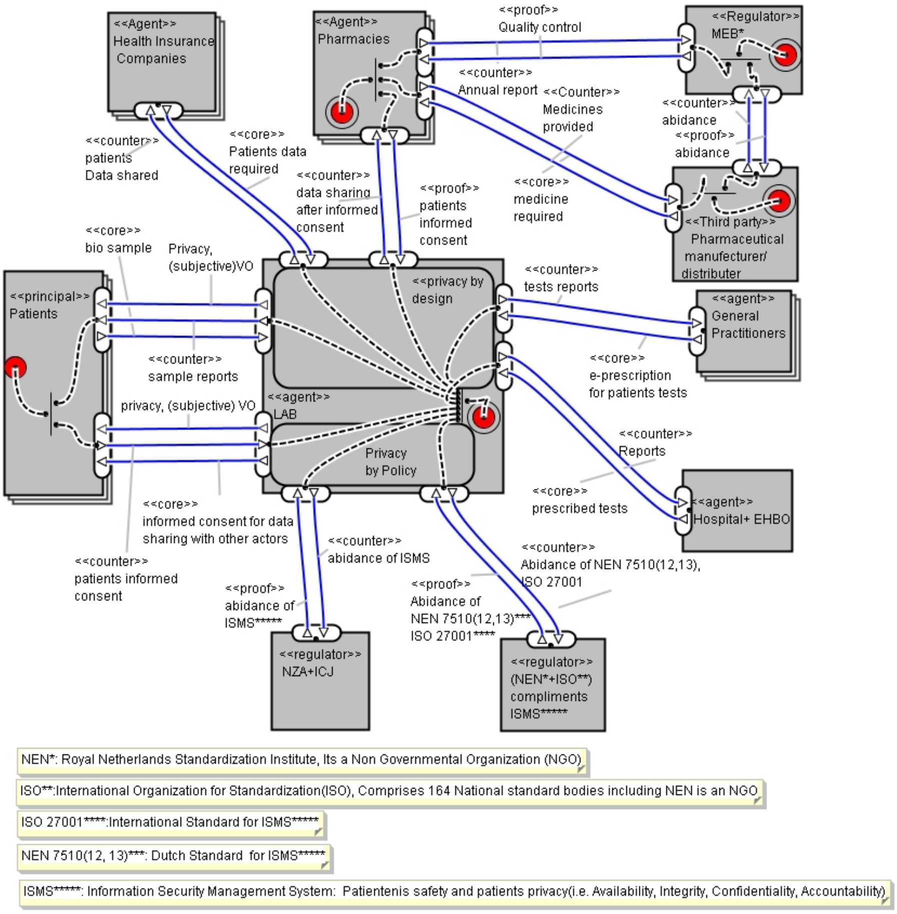

<<Agent>>
Health Insurance Companies
<<Agent>>
Pharmacies
<<proof>>
Quality control
<<Regulator>>
MEB*
<<counter>>
Annual report
<<Counter>>
Medicines provided
<<counter>>
abidance
<<proof>>
abidance
<<counter>>
patients Data shared
<<core>>
Patients data required
<<counter>>
data sharing after informed consent
<<proof>>
patients informed consent
<<core>>
medicine required
<<Third party>>
Pharmaceutical manufecturer/ distributer
<<core>>
bio sample
Privacy, (subjective)VO
<<principal>>
Patients
<<privacy by design
<<counter>>
tests reports
<<agent>>
General Practitioners
<<counter>>
sample reports
<<core>>
e-prescription for patients tests
privacy, (subjective) VO
<<agent>>
LAB
Privacy by Policy
<<counter>>
Reports
<<core>>
prescribed tests
<<agent>>
Hospital+ EHBO
<<core>>
informed consent for data sharing with other actors
<<counter>>
abidance of ISMS
<<counter>>
Abidance of NEN 7510(12,13), ISO 27001
<<counter>>
patients informed consent
<<proof>>
abidance of ISMS*****
<<proof>>
Abidance of NEN 7510(12,13)*** ISO 27001****
<<regulator>>
NZA+ICJ
<<regulator>>
(NEN*+ISO**) compliments ISMS*****
NEN*: Royal Netherlands Standardization Institute, Its a Non Governmental Organization (NGO)
ISO**:International Organization for Standardization(ISO), Comprises 164 National standard bodies including NEN is an NGO
ISO 27001****:International Standard for ISMS*****
NEN 7510(12, 13)***: Dutch Standard for ISMS*****
ISMS*****: Information Security Management System: Patientenis safety and patients privacy(i.e. Availability, Integrity, Confidentiality, Accountability)

Fig. 2. Lab's bilateral privacy protecting data sharing with other key stake holders.

While talking about value objects and their transfers, generating point or the source of the value objects matters a lot. For example when a patient goes to the biobank or lab for a blood test, results are generated from the lab making lab a source generating point for related information or data. There the power of the patient reduces in favor of the decision making of the lab management in regard of the inflow and outflow of that information. Simultaneously privacy by policy takes precedence to further the interest of patients as data subjects. Tackling of that information largely depends upon the lab or in other words upon the privacy protecting ontologies of lab.

Limitation: The second model lags behind in providing comprehensive and over encompassing analysis comprising multiple stakeholders at a time with their intrinsic privacy protecting values. So overall a disintegrated modeling or value network is doable in this regard.

Conclusion: The paper provides with the ontologies both from patients perspective and from the organizations(lab) perspective to maintain an equilibrium in safeguarding individuals fundamental rights while not ignoring the goals and objectives of the organizations. Given models provides the basis for further research in first analyzing the standard parameters from nominal to ratio based measurements to provide with the standard metrics for key stake holders to confirm the transfer of privacy as an objective value object within healthcare.

References

1. van der Aalst W.M.P.: Responsible Data Science: Using Event Data in a “People Friendly” Manner. In: Hammoudi S., Maciaszek L., Missikoff M., Camp O., Cordeiro J. (eds) Enterprise Information Systems. ICEIS. Lecture Notes in Business Information Processing, vol 291, 3-28, Springer, Cham (2016).
2. van der Aalst, W.M.P., Bichler, M. & Heinzl, A.: Responsible data science. Bus Inf Syst Eng 59(5), 311–313 (2017).
3. Fairfield, J., Shtein, H.: Big Data, Big Problems: Emerging Issues in the Ethics of Data Science and Journalism. Journal of Mass Media Ethics 29(1), 38-51 (2014).
4. Stahl, B.C., Write, D.: Ethics and Privacy in AI and Big Data: Implementing Responsible Research and Innovation. In: IEEE Security & Privacy, vol. 16, no. 3, pp. 26-33 (2018).
5. Stahl, B.C., Timmermans, J., Flick, C.: Ethics of Emerging Information and Communication Technologies on the implantation of RRI. Science and Public Policy 44(3), 369-381 (2017).
6. Carrillo-Larco, R.M., Miranda, J.J., Kengne, A.P.: Data pooling efforts in Africa and Latin America. Lancet Global Health 5(1):e37 (2017).
7. GDPR Homepage, https://eugdpr.org/ last accessed 2019/11/17.
8. Eur-lex.europe EU Law homepage, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:31995L0046 last accessed 2019/11/17.
9. Simell, B.A. et al.: Transnational access to large prospective cohorts in Europe: Current trends and unmet needs. New Biotechnology 49, 98-103 (2019).
10. Reber, B.: RRI as the inheritor of deliberative democracy and the precautionary principle. Journal of Responsible Innovation 5(1), 38-64 (2018).
11. Kamal, R.N., Lindsay, S.E., Eppler, S.L.: Patients Should Define Value in Health Care: A Conceptual Framework. The journal of hand surgery 43(11), 1030–1034 (2018).
12. Reis, J.S., Silva, P.A., Bukhsh, F.A., Castro, A.F.: Configuring value networks based on subjective business values. In: Datamanagement & Biometrics (eds.) CEUR workshop proceedings, 2239, pp.158-170 (2018).
13. Lee, E.O., Ezekiel, J., Emanuel, M.D.: Shared Decision Making to Improve Care and Reduce Costs. The New England Journal of Medicine 368(1), 6-8 (2013).
14. Panvelker, P.N., Armour, C., Rose, J., Saini, B.: Patients' value of asthma services in Australian pharmacies: the way ahead for asthma care. In the journal of asthma 49(3): 310-316 (2012).
15. Butzer, J.F., Kozlowsky, A.J., Virva, R.: Measuring value in post acute care. Archives of Physical Medicine and Rehabilitation 100(5), 990-999 (2019).
16. Galetsi, P., Katsaliaka, K., Kumar, S.: Values, challenges and future directions of big data analytics in healthcare. A systematic review. Social Science & Medicine 241, 112533 (2019).
17. Kung, A., Freytag, J.C., Kargl, F.: Privacy-by-design in its applications. In: IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks, pp 1-6. Lucca, (2011).
18. Spiekermann, S., Cranor, L.F.: Engineering Privacy. IEEE Transactions on Software Engineering 35(1), 67-82 (2009).

19. Åhlfeldt R.M., Huvala I.: Patient Safety and Patient Privacy When Patient Reading Their Medical Records. In: Saranto K., Castrén M., Kuusela T., Hyrynsalmi S., Ojala S. (eds) Safe and Secure Cities. Communications in Computer and Information Science, 450. Springer, Cham (2014).
20. UN Homepage/Universal declaration of human rights, https://www.un.org/en/universal-declaration-human-rights/ last accessed 2019/11/17.
21. Fatemi, H., van Sinderen, M., Wieringa, R.,: E3value to BPMN Model Transformation. In: IFIP International Federation for Information Processing, L.M. Camarinha-Matos et al. (Eds.): PRO-VE 2011, IFIP AICT 362, pp. 333–340 (2011).
22. Avelino, J.G., de Silva, P.A., Bukhsh, F.A.: Towards Green Value Network Modeling: A Case from the Agribusiness Sector in Brazil. In: Panetto H., Debruyne C., Hepp M., Lewis D., Ardagna C., Meersman R. (eds) On the Move to Meaningful Internet Systems: OTM 2019 Conferences. Lecture Notes in Computer Science, vol 11877. Springer, Cham (2019).
23. Eisenhardt, K.M.: Agency Theory: An Assessment and Review: A systematic review. The Academy of Management Review 14(1), 57-74 (1989).
24. Transparency in Health Care Homepage, http://www.tihealthcare.nl/en last accesses 2019/11/30.
25. Critselis, E.: Impact of the General Data Protection Regulation on Clinical Proteomics Research. PROTEOMICS–Clinical Applications, 13(2), 1800199 (2019).
26. Garattini, C., Raffle, J., Aisyah, D. N., Sartain, F., & Kozlakidis, Z.: Big data analytics, infectious diseases and associated ethical impacts. Philosophy & technology, 32(1), 69-85 (2019)
27. IGJ Homepage, https://english.igj.nl/ last accessed 2019/11/30
28. NZA Homepage, https://www.nza.nl/ last accessed 2019/11/30
29. Consoli, S., Recupero, D.R., Petkovic, M.: Data Science for Healthcare, Methodologies and Applications. 1st Ed. Springer, Cham Switzerland (2019).