Privacy by Design Approach for eHealthcare System Architecture

Malgorzata Pankowska
Department of Informatics
University of Economics in Katowice
Katowice, Poland
pank@ue.katowice.pl

***Abstract*—Privacy engineering has recently attracted attention from professionals; therefore, current literature includes methodologies to support privacy modelling and system design. However, in order to ensure appropriate and successful implementation of these methodologies, it is important to develop business and system analyses focusing on privacy and security issues. The paper aims to identify privacy engineering requirements and conditions and model them for further holistic system architecture development in the eHealthcare context. The results show the demand to strongly focus on business architecture development for further mapping the privacy requirements into security systems.**

Keywords-Privacy; Security; Privacy by Design; Business Architecture; System Architecture; ArchiMate.

I. INTRODUCTION

Protection of data privacy is becoming a key challenge for most business entities. The discussions are now very intensive, particularly because of the General Data Protection Regulation (GDPR) [1] introduced in 2016 in European Union (EU) member countries. However, due to the big data and information, the GDPR recommendations are becoming popular in the digital space. Therefore, identifying key indicators for patient configured privacy policy in relation to eHealthcare personalized services is also very important and valid. Taking into account the existing literature, it is necessary to mention that information privacy refers mostly to the right to exercise control over the use of personal information. However, in this paper, we emphasize the need to develop a holistic approach for privacy requirements specification and modelling. The privacy by design approach, as well as Information Boundary Theory (IBT), and Communications Privacy Management Theory are used in discussion for this development. The privacy paradox is explained and the business architecture and system architecture models are presented. The paper is organized as follows. Firstly, background information regarding the privacy concepts is provided. Next, in Section 2, the literature review on Privacy by Design (PbD) approach is discussed. Further, in Section 3, the eHealthcare issues are presented as a certain context of privacy issues. Then, models of business architecture and system architecture in ArchiMate language are considered. This is followed by the discussion of results of the models' analysis. The conclusions cover implications and limitations of the work presented.

II. PRIVACY VS. SECURITY

Any information about an individual maintained and processed by an agency, including data on the individual's identity, i.e., names, social security number, personal identification number, parents' names, or biometric records is personal information and as such is usually linked to other medical, educational, financial, and employment information. In this context, privacy is an ability to control this information, because individuals are interested in keeping some of their personal information hidden from others.

According to de Souza et al. [2] privacy is a fundamental right guaranteed by the Universal Declaration of Human Rights, proclaimed by the United Nations General Assembly. Reference [3] includes a classification of different types of privacy:

- Personal privacy concerning the privacy of personal attributes.
- Informational privacy involving the protection of unauthorized access to information.
- Institutional privacy referring to the administration of organizational private data as well as strategic business information.

Burgoon et al. [4] assume a multidimensional approach and define privacy as the ability to control and limit physical, interactional, psychological, and informational access to a social group or just to its entity. For Solove [5], privacy is valued contextually, and it includes practices of information collecting, processing, dissemination and invasion. Information Boundary Theory (IBT) was formulated to explain the psychological processes individuals use to control the flows of private information. The theory proposes that consumers form physical or virtual informational spaces around them. The boundaries around the spaces play important roles in their willingness to reveal private information or not. Any attempt by an external party to cross these boundaries is perceived as an invasion. According to Communications Privacy Management Theory (CPMT), disclosure of private information renders people vulnerable to opportunistic exploitation, because the disclosed private information becomes co-owned by other parties. The boundary management mechanisms are developed to help people maximize the benefits of revealing private information while simultaneously reduce the risks of opportunistic behavior resulting from intrusive access.

 ISBN: 978-1-61208-732-0

In general, privacy is determined by the context, i.e., business environment, the individual value system and confidence awareness, which may encourage people to reveal their personal information. The value system constructs social patterns of all aspects of human interactions. Sherif et al. [6] argue that shared patterns of behaviours and interactions, cognitive constructs, and affective understandings are learned through a process of socialization. Privacy culture and security culture are defined as ideas, customs, habits, and social behaviours that help individuals to survive as a community. Cavoukian and Chibba [7] argue that while information security concerns protecting personal data through confidentiality, integrity, and availability control, privacy is about unlinkability, transparency, and intervenability assurance. Security is about how information is protected, but privacy is on how it is maintained and used.

Literature review reveals principles of data privacy assurance. The principles are hidden in theories, standards, and various regulations. Particularly important standards are as follows:

- The ISO 9241-210:2010 Ergonomics of human-system interaction Part 210: Human-centered design for interactive systems, which, as a framework for human-centered design processes, integrates different designs and developments appropriate in a particular context [8].
- The ISO/IEC 25010:2011 SQuaRE Systems and Software Quality Requirements and Evaluation, which is a standard that defines the system and software quality, which is highly focused on system's quality of use [8].
- The ISO/IEC 27034-3:2018 Information Technology - Application Security- Part 3: Application security management process, which is a part of standard series assisting organization in integrating security into the life cycle of their applications by providing frameworks and processes at the organization [10].
- The ISO/IEC 29100:2011 Information Technology - Security Techniques - Privacy Framework, applicable to individuals and organizations involved in the specification, procurement, architecturing, designing, developing, testing, maintaining, administering, and operating information and communication technology systems and services, where privacy controls are required for the processing of Personally Identifiable Information (PII) [11].
- The ISO/IEC 29147 - Information Technology - Security Techniques - Vulnerability Disclosure, which is a standard providing requirements and recommendations to vendors on the disclosure of vulnerabilities in products and services [12].

According to the last standard, privacy preferences are to be confronted with privacy safeguarding controls. The privacy principles included there concern data subject's consent and choice, purpose legitimacy and specification, collection limitation, data minimization, data use, retention and disclosure limitation, data accuracy and quality, data openness, transparency and notice, data subject's individual participation and access, accountability, information security, and privacy compliance. In May 25, 2018 the GDPR came in effect mandating data controllers and processors to emphasize transparency, security, and accountability of processed data. The GDPR specifies seven data protection principles that business organizations are to follow when collecting, processing, transferring, and storing individuals' personal data (Table 1). The Organization for Economic Co-operation and Development (OECD) [13] provided principles similar to the GDPR work (Table I). The regulations discussed above do not concern Privacy by Design (PbD) approach.

TABLE I. PRIVACY PRINCIPLES.

Privacy Standards		
Cavoukian Principles	***OECD Principles***	***GDPR Principles***
Proactive not Reactive	Collection Limitation	Storage Limitation
Privacy as the Default Setting	Data Quality	Accuracy
Privacy embedded into Design	Purpose Specification and Openness of Data Handling	Data Lawfulness, Fairness, and Transparency
Full Functionality	Use Limitation	Purpose Limitation
End to End Security	Security Safeguards	Integrity and Confidentiality
Visibility and Transparency	Accountability	Accountability
Respect for User Privacy	Individual Participation	Data Minimization

In 2011, Cavoukian published her Privacy by Design principles [14], which for years have been treated as the de facto standard in privacy protection (Table I). In Article 29, Data Protection Working Party, the proposed principles that should be respected in PbD approach are as follows:

- Choice and consent principle defining that data controllers and processors should describe choices suitable to the data subjects to obtain appropriate consents.
- Legitimate data use purpose specification and use limitations.
- Personal information and sensitive information lifecycle management to ensure minimization of data collection and all its use, just to the strictly specified, documented purposes.
- Accuracy and quality of data that is processed and utilized.
- Providing clear, accessible, transparent and accurate details about business organization privacy management program on how information is processed.
- Development of procedures to allow data subjects to withdraw the consent to use their personal data at any time.
- Establishing the requirements for data protection officers' responsibilities and actions.

 ISBN: 978-1-61208-732-0

- Development of security policies and supporting procedures.
- Implementation of monitoring, measuring and reporting procedures to provide sufficient regular privacy and security control.
- Preventing harms, reducing risk, and protecting vital interests of data subjects.
- Documenting the management policies and control cooperation with third party vendors and security outsourcing companies.
- Elaboration of documented personal data breach policies and supporting procedures that include requirements for notifications of appropriate supervisory authorities.
- Development of procedures concerning implementation technologies and PbD protection.
- Maintaining the policies and procedures to contact the appropriate supervisory authorities.

Nowadays, the PbD issue seems to be increasingly important, particularly because people commonly use Internet of Things (IoT) applications. An exemplary list of devices includes baby monitors, smart home assistants, connected safety-relevant products such as smoke detectors and door locks, smart cameras, TVs and speakers, wearable health trackers, connected home automation and alarm systems. The devices should be safe and secured. Safety is assumed to be a situation, in which people are protected from injury, but security is identified with a condition, where individuals are protected against the consequences of malicious acts. Taking into account the IoT common usage, security and privacy should be embedded in the IoT software application development. Privacy and security by design mean that basic security features are to be built into products and the consumer should learn how to secure their devices. The PbD and security by design ideas require methodological approaches and good practices guidelines. The Code of Practice for Consumer IoT Security [15] covers the following guidelines: password idiosyncrasy, vulnerability disclosure policy implementation, software updating, credentials protection, remote control, software integrity, personal data protection, system resilience, monitoring telemetry data, and making personal data easy to delete. So, the suggested PbD methodological approach is expected to emphasize the principles of response to customer needs, monitoring, learning and anticipation.

III. PRIVACY BY DESIGN - LITERATURE REVIEW

At first glance, the idea of PbD can be recognized as an approach that promotes privacy and data protection compliance from the start of data collecting and processing and maintains such protection in the whole information system lifecycle. Beyond that, it is expected to increase the awareness of privacy and decrease human vulnerabilities. Literature review confirms this attitude. The fundamental reviews have been done using the following tools: 1) IEEEXplore Digital Library [16], 2) AIS (Association of Information Systems) eLibrary [17], 3) ScienceDirect.com [18], 4) Google Scholar [19], 5) Sage Journals [20], 6) Scopus [21], and 7) Web of Science (WoS) research paper repository [22]. The numbers of publications found in these repositories were impressive, but incomparable. The maximum number of publications were presented in GoogleScholar, i.e., 3 340 200 papers, and the smallest on IEEEXplore Digital Libery, i.e., 2791 papers. The reviewed papers include considerations on combining the Privacy by Design concept with information system development methodologies. According to information from the surveyed repositories, lately, authors are working on privacy issues in big data methodologies, as well as in Internet of Things (IoT) application design and implementation. However, in years 2009-2019 , the volume of publications in Google Scholar is going down. Evident increase of growth rates happened in 2012-2014 for WoS publications. The literature review has been done at the beginning of 2019, therefore the minor volume of publications for this year has been registered. However, taking into account further research work on PbD approach in eHealthcare system modelling, this huge volume of papers was reduced to the list of publications in Table II.

TABLE II. PRIVACY BY DESIGN FOR EHEALTHCARE

No	Paper	Research Results
1	[23]	Privacy patterns for Information System design are proposed and compared to ISO 29100 Privacy Framework principles
2	[24]	Practical approaches in designing IoT for data collection and data sharing within the health domain
3	[25]	Novel data linkage and anonymisation infrastructure in clinical study on chronic diseases in Scotland
4	[26]	Formal methodology for designing privacy mechanisms in pervasive healthcare applications
5	[27]	Analysis of legal difficulties surrounding the use of social networking for healthcare applications
6	[28]	Demonstration of why the implementation of PbD is a necessity in a number of sectors, where specific data protection concerns arise (biometrics, e-health, and video-surveillance)
7	[29]	Examining technological limits, ethical constraints and legal conditions of privacy by design, so as to prevent some misapprehensions of the current debate
8	[30]	In personal health monitoring, PbD approach implies that in some contexts like medication assistance and monitoring of specific health parameters one single automatic option is legitimate
9	[31]	Providing a critical reflection of the perceived privacy risks associated with social media recruitment strategy and the appropriateness of the risk mitigation strategies. Alignment with PbD. Discussion of the following: What are the potential risks and who is at risk? Is cancer considered "sensitive" personal information? What is the probability of online disclosure of a cancer diagnosis in everyday life? What are the public's expectations for privacy online?
10	[32]	This paper presents an analysis of personal e-health systems and identifies privacy issues as a first step towards a 'privacy by design' methodology and practical guidelines.

The paper presented in Table II reveal that researchers focus on combining the PbD approach with the healthcare system development methodologies and applications. The PbD approach is applied to mitigate privacy risk in online information systems and it is considered as a way for

protecting personal information. The reviewed research papers have revealed many questions for further investigation, particularly in social networks.

IV. eHEALTHCARE ARCHITECTURE MODELS INCLUDING PRIVACY BY DESIGN

Information Communication Technology (ICT) is incorporated into healthcare management programs enabling care personalization to an individual's needs. The patient-physician relationship system with more virtual interactions is possible to better coordinate care. The relationship systems are developed as formal support of the medical services, as well as informal communication in social networks. The European Group on Ethics in Science and New Technologies (EGE) [33] published an opinion on the ethical implications of new health technologies and individual participation. Therein, they have identified a set of risks. Patients' group focusing on particular diseases take greater responsibility for their health. They are voluntary involved and openly manifest using the online forums their private problems and data. They share symptoms, advices, opinions, and diagnoses. They use social media and internet forums to verify the quality of the professional healthcare as well as for ranking services and physicians. Internet and mobile applications enable them to avoid traditional medical services and develop self-diagnosing and self-treatment. This behavior implies that in some contexts, like medication assistance and monitoring, specific health parameters are revealed and individuals lose control on them. Although in the technical design professionals think about privacy in the aspect of problems of data collecting and security, the social networks people consider the privacy effects of communication on humans and they are open to exchange views in their own individual interests. The need to help themselves and to help others strongly stimulates them to reveal private data. According to Yoo et al. [34], privacy paradox is a phenomenon whereby individuals present strong privacy concerns, but they disclose their personal information. Within an individual's borders, people want to be free to self-determine what they want to reveal. On the other hand, society also has impact on defining these borders by accepting, supporting, tolerating, mocking or punishing. Unfortunately, some people see only the informational aspect without perceiving the consequences of privacy revealing for social relationship development. eHealthcare architecture modelling with respect to the PbD approach can be considered as a privacy engineering issue. The system architecture models proposed below are embedded in a specific healthcare context, particularly they concern the eHealthcare self-treatment, which as such is strongly based on the use of wearable devices, human behaviour monitors and smart assistants. In this paper, system architecture models are presented in the ArchiMate language [35]. Therefore, as it is in The Open Group Architecture Framework (TOGAF) [36] four architecture layers are defined. In the aspect of privacy management, the motivation layer is the most important. Here, perceived privacy risks, principles, constraints, stakeholders, their requirements, goals and values are to be identified and considered (Fig. 1).

Privacy risk is defined as a loss resulting from the negative outcomes and the possibility of an opportunistic behaviour of other parties. Privacy risk includes the misuse of private personal information or unauthorized access and theft [37]. In literature, privacy is perceived from the point of view of reputation loss and identity theft [38]. However, in opposition to that interpretation, private personal data is perceived as necessary to self-promotion. Privacy revealing actions are considered as good investments for individual and organizational development. In Fig. 1, the fundamental concepts of TOGAF motivation layer for eHealthcare self-management are presented.

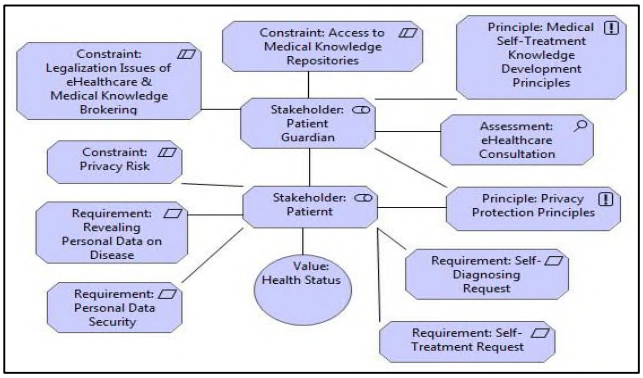

Figure 1. eHealthcare Self-Treatment Architecture Model: Motivation Layer in ArchiMate.

The next TOGAF layer is Archimate Business Layer, which includes the specification of fundamental business concepts, i.e., business partners, processes, services, functions, and objects (Fig. 2). Particularly, the process of control is to be embedded in most privacy regulations, so it is used to operationalize privacy.

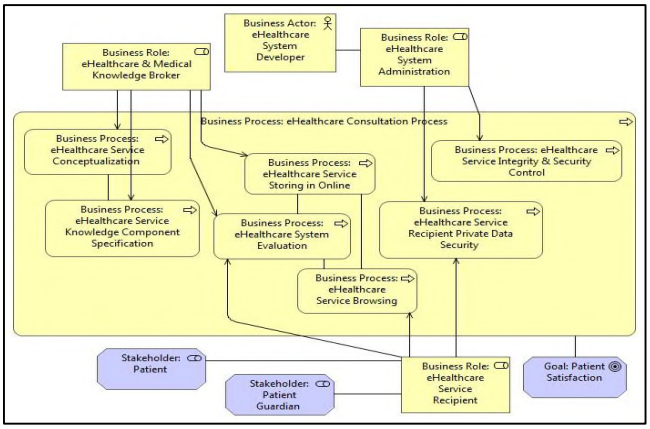

Figure 2. eHealthcare Self-Treatment Architecture Model: Business Layer in ArchiMate.

The eHealthcare consultation process comprises on the one side actions to reveal data, on the other side to hide and protect them. Therefore, basically, to prevent a privacy breach event the following activities are required [39]:

- Monitor of the event trigger generation.
- Notice of event triggers to privacy stakeholders.

- Blocking leakages to avoid personal data flows to the wrong hands.
- Security of delivery channel - encryption.

Anonymity, pseudonymization, unlinkability, and confidentiality prevent individual privacy from revealing i.e., breach of confidentiality. That process decomposition is presented in Fig. 3. Although in some cases "less identification means more privacy" [40], however, sometimes less data, but discovering critical data can lead to violation of privacy.

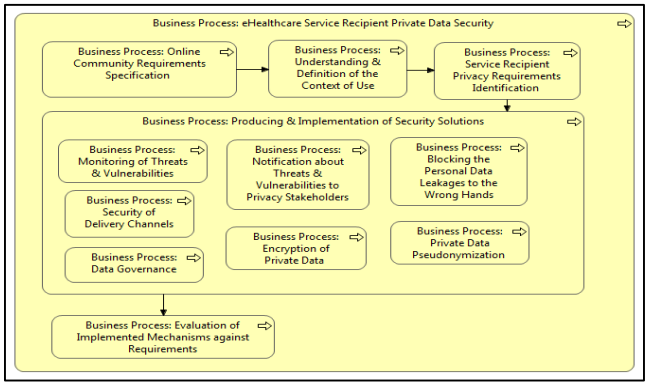

Figure 3. eHealthcare Self-Treatment Architecture Model: Recipient Private Data Security Process in ArchiMate.

The Data Governance process emphasized in Fig. 4 is assumed to include activities to appropriate data provenance, accuracy, lawfulness, fairness, transparency, integrity, and accountability. Implementation of all these processes is not common, however, it should be considered as obligatory. Even the knowledge broker's role is difficult, but in the interests of patients and their life protection, this role is needed. In the TOGAF framework, the next two layers cover software and hardware architecture modelling (Fig. 4).

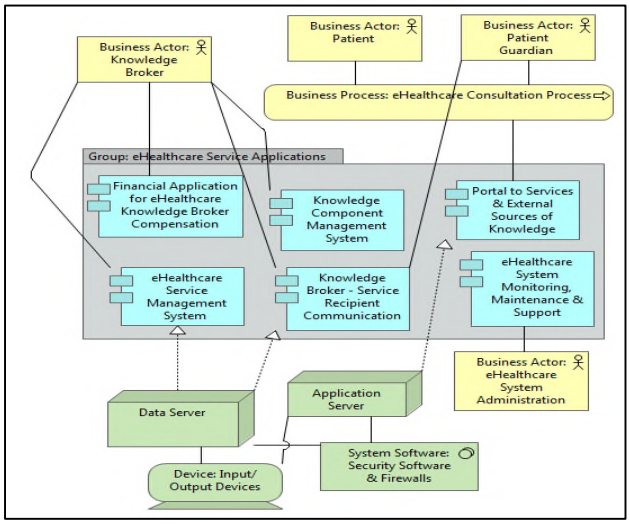

Figure 4. eHealthcare Self-Treatment Architecture Model: Software and Hardware Layers in ArchiMate.

Technologies like firewalls and access control filters are implemented to ensure the security of information assets, but they cannot provide enforcement of acceptable use policies, because of the users, who make decisions on the usage of confidential data and documents.

V. CONCLUSION

The Privacy by Design approach makes the application or information system more reliable from the personal data management point of view. Following literature review, we conclude that the PbD approach is implemented in software development methodologies. However, in this paper, the holistic approach to privacy management is proposed. Therefore, the system architecture modelling is presented. The TOGAF architecture models for motivation, business, software and hardware layers are included in Figures. The ArchiMate language and modelling tool were used. In this paper, privacy is discussed as a social category and issue, which is determined by personal data subjects. Beyond that, there are solutions developed for personal data protection. The fundamental processes of data security are also presented in ArchiMate language in this paper. The architecture modelling can be further considered as an introduction to application development. The limitation of the presented analysis results from the weaknesses of the applied tool, i.e., ArchiMate. On the one hand, it is suitable for modelling motivation and explaining preferences, but, on the other hand ArchiMate is not integrated with other software engineering tools.

REFERENCES

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 and repealing Directive 95/46/EC (General Data Protection Regulation). [Online]. Available from: https://eur-lex.europa.eu/ 2019.07.20

[2] P. C. de Souza and C. Maciel, "Legal Issues and User Experience in Ubiquitous Systems from a Privacy Perspective," in Human Aspects of Information Security, Privacy, and Trust, T. Tryfonas and I. Askoxylakis, Eds. Cham: Springer, pp. 449-460, 2015.

[3] J. M. Kizza, Ethical and Social Issues in the Information Age. New York: Springer, 2013.

[4] J. K. Burgoon, R. Parrot, B. A. LePoire, D. L. Kelley, J. B. Walther, and D. Perry, "Maintaining and restoring privacy through communication in different types of relationship," Journal of Social and Personal Relationships, Volume 6, pp. 131-158, 1989.

[5] D. J. Solove, "Conceptualizing privacy," California Law Review, 90, pp. 1087-1156, 2002.

[6] E. Sherif, S. Furnell, and N. Clarke, "An Identification of Variables Influencing the Establishment of Information Security Culture," in Human Aspects of Information Security, Privacy, and Trust, T. Tryfonas and I. Askoxylakis, Eds. Cham: Springer, pp. 436-448, 2015.

[7] A. Cavoukian and M. Chibba, "Start with Privacy by Design in All Big Data Applications," in Guide to Big Data Applications, S. Srinivasan, Ed. Heidelberg: Springer, pp.29-48, 2018.

[8] International Organization for Standardization. *ISO 9241-210:2010 Ergonomics of human-system interaction, Part 210: Human-centered design for interactive systems.* [Online]. Available from: https://www.iso.org/ 2019.06.11

[9] International Organization for Standardization. *ISO/IEC 25010:2011 SQuaRE Systems and Software Quality Requirements and Evaluation.* [Online]. Available from: https://www.iso.org/ 2019.06.11

[10] International Organization for Standardization. *ISO/IEC 27034-3:2018 Information Technology - Application Security-Part 3: Application security management process.* [Online]. Available from: https://www.iso.org/ 2019.06.11

[11] International Organization for Standardization. *ISO/IEC 29100:2011 Information Technology -Security Techniques - Privacy Framework.* [Online]. Available from: https://www.iso.org/ 2019.06.11

[12] International Organization for Standardization. ISO/IEC 29147 - Information Technology - Security Techniques - Vulnerability Disclosure. [Online]. Available from: https://www.iso.org/ 2019.06.11

[13] S. Anderson, "Privacy by Design: An Assessment of Law Enforcement Drones," A thesis submitted to the Faculty of the Graduate School of Art and Sciences of Georgetown University, Washington, DC, 2014

[14] A. Cavoukian, "Privacy by design. The 7 foundational principles in Privacy by Design. Strong privacy protection—now, and well into the future, 2011. [Online]. Available from: https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf 2019.03.20

[15] Department for Digital, Culture, Media & Sport. *Code of Practice for Consumer IoT Security*. 2018 [Online]. Available from: https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security 2019.06.11

[16] IEEEXplore Digital Library. [Online]. Available from: https://ieeexplore.ieee.org/Xplore/home.jsp 2019.03.10

[17] Association of Information Systems AIS eLibrary. [Online]. Available from: https://aisel.aisnet.org/ 2019.03.10

[18] ScienceDirect.com. [Online]. Available from: https://www.sciencedirect.com/ 2019.03.10

[19] GoogleScholar. [Online]. Available from: https://scholar.google.pl/ 2019.03.10

[20] Sage Journals. [Online]. Available from: https://journals.sagepub.com/ 2019.03.03

[21] Scopus [Online]. Available from: https://www.scopus.com/home.uri 2019.02.02

[22] Web of Science (WoS). [Online]. Available from: https://clarivate.com/products/web-of-science/ 2019.02.02

[23] M. Aljohani, K. Hawkey, and J. Blustein, "Proposed Privacy Patterns for Privacy Preserving Healthcare Systems in Accord with Nova Scotia's Personal Health Information Act," in Human Aspects of Information Security, Privacy, and Trust, T. Tryfonas, Ed. Cham: Springer, pp. 91-102, 2016

[24] Y. O'Connor, W. Rowan, L. Lynch, and C. Heavin, "Privacy by Design: Informed Consent and Internet of Things for Smart Health," The 7th International Conference on Current and Future trends of Information and Communication Technologies in Healthcare (ICTH2017), Procedia Computer Science, 113, 2017, pp. 653-658. [Online]. Available from: www.elsevier.com/locate/procedia 2019.02.20

[25] R. O. Sinnott, O. Ajayi, and A. J. Stell, "Data Privacy by Design: Digital Infrastructures for Clinical Collaborations," 2009. [Online]. Available from: https://minerva-access.unimelb.edu.au/handle/11343/28791 2019.02.23

[26] S. Moncrieff and S. Venkatesh, "A framework for the design of privacy preserving pervasive healthcare," ICME 2009. [Online]. Available from: https://www.researchgate.net/publication/221262735 2019.02.20

[27] J. B. Williams and J. H. Weber-Jahnke, "Social networks for health care: Addressing regulatory gaps with privacy-by-design," Eighth International Conference on Privacy, Security and Trust, 2010, pp. 134-143. [Online]. Available from: https://ieeexplore.ieee.org/xpl/mostRecentIssue.jsp?punumber=5564352 2019.03.20

[28] A. Romanou, "The necessity of the implementation of Privacy by Design in sectors where data protection concern arise," Computer Law & Security Review, Volume 34, Issue 1, February 2018, pp. 99-110.

[29] U. Pagallo, "On the Principle of Privacy by Design and its Limits: Technology, Ethics and the Rule of Law," in European Data Protection: In Good Health? S. Gutwirth, R. Leenes, P. DeHert, Y. Poullet, Eds. Dordrecht: Springer, pp. 331-346, 2012.

[30] A. Nordgren, "Privacy by Design in Personal Health Monitoring," Health Care Analysis, 23, pp. 148-164, 2015.

[31] J. L. Bender, A. B. Cyr, L. Arbuckle, and L. E. Ferris, "Ethics and privacy implications of using the internet and social media to recruit participants for health research: A privacy-by-design framework for online recruitment," Journal of Medical Internet Research, Volume 19, Issue 4, April 2017, [Online]. Available form: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5399223/ 2019.03.20

[32] G. Drosatos, P. S. Efraimidis, G. Williams, and E. Kaldoudi, "Towards Privacy by Design in Personal e-Health System," Proceedings of the BIOSTEC 2016 Conference - Volume 5: HEALTHINF. SCITEPRESS – Science and Technology Publications, 2016. p. 472-477. [Online]. Available from: https://eprints.lancs.ac.uk/id/eprint/79489/ 2019.03.15

[33] European Group on Ethics in Science and New Technologies (EGE), The ethical implications of new health technologies and citizen participation, Opinion of the European Group on Ethics in Science and New Technologies to the European Commission, Brussels, 2015. [Online]. Available from: https://ec.europa.eu/research/ege/index.cfm?pg=reports 2019.03.18

[34] Ch. W. Yoo, H. J. Ahn, and H. R. Rao, "An Exploration of the Impact of Information Privacy Invasion," Thirty Third International Conference on Information Systems, Orlando 2012, AIS/ICIS, pp. 2260-2278. [Online]. Available from: https://www.semanticscholar.org/paper/An-Exploration-of-the-Impact-of-Information-Privacy-Yoo-Ahn/6569055fc719f57b2492b35531f987edfaa18cd8 2019.03.19

[35] Archi – Open Source ArchiMate Modelling. [Online]. Available from: https://www.archimatetool.com/ 2019.02.02

[36] W. Engelsman, H. Jonkers, and D. Quartel D. "Supporting Requirements Management in TOGAF and ArchiMate," February 2010. [Online]. Available from: http://www.opengroup.org 2015.03.01

[37] H. Xu, T. Dinev, H. J. Smith, and P. Hart, "Examining the Formation of Individual's Privacy Concerns: Toward an Integrative View," ICIS 2008 Proceedings, 6 2008. [Online]. Available from: http://aisel.aisnet.org/icis2008/6 2019.03.20

[38] K. E. Greenaway, Y. E. Chan, "Designing a Customer Information Privacy Program Aligned with Organizational Priorities," MIS Quarterly Executive, September, 12:3, pp. 137-150, 2013.

[39] S. Chen and A-M. Williams, "Grounding Privacy-by-Design for Information Systems" . PACIS 2013 Proceedings. 2013. [Online]. Available from: http://aisel.aisnet.org/pacis2013/107 2019.03.24

[40] G. Ben Ayed, Architecting User-Centric Privacy-as-a-Set-of-Services, Digital Identity-Related Privacy Framework, Cham: Springer, 2014.