GDPR and Systems for Health Behavior Change: A Systematic Review

Eunice Eno Yaa Frimponmaa Agyei and Harri Oinas-Kukkonen

Faculty of Information Technology and Electrical Engineering

University of Oulu, Oulu 90570, Finland

{eunice.agyei, harri.oinas-kukkonen}@oulu.fi

Abstract

eHealth systems for behavior change need to cope with a wide variety of privacy requirements specified by governmental and other regulations. We conducted a systematic review of scientific articles. Analysis of the articles revealed General Data Protection Regulation (GDPR) compliant eHealth technologies, challenges posed by GDPR as well as early solutions for them. In addition, we highlight key GDPR issues to be considered when designing persuasive technologies.

Keywords: GDPR, eHealth, persuasive technology, persuasive features, behaviour change

Introduction

eHealth technology seeks to enhance health care delivery [1]. It enhances the efficiency of healthcare by reducing cost, improving the quality of care, and empowering stakeholders by making personal electronic records readily accessible to them. It also provides a mechanism for collaboration between patients, health workers, and technology providers, and thus educates and facilitates information exchange between health practitioners and healthcare centers.

Persuasive eHealth technologies such as Behaviour Change Support Systems (BCSS) help users change their behaviour over time [2]. Despite their usefulness, eHealth systems are prone to ethical issues pertaining to informed consent, privacy breaches, and equity issues regarding who can have access to the resources and the opportunities it has to offer [3]. Privacy and security are a cause for concern due to the sensitive and personal nature of health data. Without addressing privacy related issues, the rate of adoption and use of eHealth applications and systems could to a significant manner be negatively impacted [4].

Privacy of health data presents serious concerns when health records are electronic [5]. Maintaining the privacy of health data involves ensuring confidentiality, integrity, and availability of the data, as well as securing the collection, transmission, storage and processing of the data. It further involves securing the technology itself, educating and increasing the awareness of privacy and security breach issues, as well as complying with policies and regulations to keep the data secured [6]. Two well-known legislations that regulate the handling of data are the Health Insurance Portability and Accountability Act (HIPAA) and General Data Protection Regulation (GDPR) [7].

In this paper, the following research contributions are made: (1) analysis of the influence GDPR has on the privacy requirements of eHealth systems, (2) identification of challenges GDPR possess to the development of eHealth systems and how these requirements can be fulfilled, (3) highlight key issues for designing persuasive features of eHealth systems. The terms eHealth systems, applications and technologies are used interchangeably in this paper.

Background

Although eHealth projects and applications do not always perform as anticipated [8] [9], one important issue to consider is the resistance to change attitude of health professionals which stems from the lack of

reconciliation of their expectations and actual outcome of eHealth systems [8]. In the development of eHealth systems, attention is often given to the technical aspects leading to the neglect of the interdependencies that exist between the technology, people, and the environment to reap the full benefits of such systems [10]. This calls for the adoption of a comprehensive approach to the development of eHealth applications. One such approach is proposed by the Centre for eHealth Research and Disease Management (CeHRes) as the CeHRes Roadmap [10].

CeHRes Roadmap

The CeHRes Roadmap is an approach that serves as a guideline for eHealth development, implementation and evaluation. It adopts a holistic approach for the development of eHealth technologies using an iterative and dynamic 5-phase framework which encompasses participatory development, persuasive design techniques, and business modelling [10]. The phases of the framework are contextual inquiry, value specification, design, operationalization and summative evaluation. (1) Contextual Inquiry: The first phase focuses on gaining an in-depth understanding of the current state of the problem at hand, identifies and analyses the roles and needs of the various stakeholders who fall within the scope and context of the problem. (2) Value Specification: This phase involves the identification and elicitation of the specific benefits (values) of the technology based on stakeholder needs. These values can then be translated into end-user requirements. (3) Design: Here, the identification of user requirements of the system is followed by development mock-ups, prototypes, usability tests, technology development, and the addition of usability principles and persuasive features to the design are done [11]. (4) Operationalization: Plans regarding the operationalization of the technology are outlined. Concrete activities such as pilot programs, advocacies, and presentations are used to increase the awareness of the technology. (5) Evaluation: This phase involves a formative and/or summative assessment of the impact of the designed technology on the problem context and its stakeholders. Thus, the value added to the stakeholder's life should be apparent. The CeHRes Roadmap aids in the planning and execution of the development process of eHealth technologies and can be a valuable tool for the improvement of existing technologies.

General Data Protection Regulation (GDPR)

The data protection regulation which emphasizes on the need to protect citizens of the European Union (EU) from privacy and data breaches and the consequences of non-compliance was enforced in May, 2018 [12]. GDPR is famous for the penalties associated with non-compliance and the rights of data subjects such as privacy by design, breach notifications, right to be forgotten, right to access, and data portability which was not the case in previous legislations. In the event of a breach or non-compliance, an organization can incur a fine to the tune of 4% of its annual global turnover or 20 million euros (whichever is greater). GDPR requires the data of people living within the EU to be processed within the EU regardless of the location of the company. This means that any business entity that seeks to process the data of EU citizens must have a representative within the EU. Consent is another requirement of GDPR. GDPR demands user consent be clear, informative, accessible, written in clear and plain language, and easy to withdraw from. GDPR also specifies requirements for proper record keeping of internal data operations. The implementation of GDPR in eHealth systems brings new design requirements, responsibilities, and expenditures leading to significant impact on eHealth organizations [13]. In this paper, the CeHRes roadmap will be used to identify the influence GDPR has on the development of eHealth systems.

Methodology

A systematic review was conducted to identify GDPR implementations in eHealth systems using data from the following databases: Proquest, IEEE Xplore, Ebscohost, Web of Science, and ACM using the following keyword combinations: GDPR AND (ehealth OR e-health OR mhealth OR m-health OR 'electronic health'

OR ‘digital health’, OR ‘digital interventions’ OR ‘online interventions’ OR ‘ehealth interventions’ OR ‘mobile intervention’ OR ‘e-health intervention’ OR ‘mhealth intervention’ OR ‘m-health intervention’, OR ‘mobile health’ OR ‘mobile app’ OR ‘mobile application’).

A total of 213 articles were found, of which 168 unique articles were obtained after deduplication. The titles and abstracts were screened for keywords and articles that did not have any of the keywords were excluded. A total of 28 articles remained for further analysis. Further screening was performed to exclude articles that were not relevant to our objective. Articles included were directly or indirectly related to eHealth and GDPR. 5 articles were not relevant for this study and hence excluded. A total of 23 articles were analysed. These articles can be found as publications [8, 14-35] in the reference list of this paper.

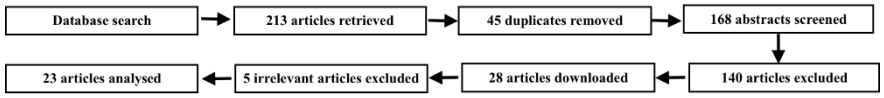

Fig 1. *Selection process*

Results

GDPR and characteristics of eHealth Roadmap

The CeHRes roadmap employs participatory approach, persuasive design and business modelling [10]. Quite naturally, not all the analysed studies utilised all these principles. However, a number of characteristics of the roadmap were found in various studies. Table 1 shows how the CeHRes Roadmap characteristics were evident in the analysed studies.

	Number of studies (N=23)	% addressed
Contextual inquiry	22	95%
Value specification	22	95%
Design	16	70%
Operationalization	4	17%
Summative evaluation	4	17%

Table 1. Characteristics of studies (N=23)

Contextual inquiry

A vast majority of the articles (22 out of 23) provided a detailed analysis of the current healthcare provision as well as a thorough description of the problem context, the strengths and weaknesses of the existing healthcare provisions (eHealth system in use) in the light of privacy and GDPR. The remaining article (1 out of 23) only analysed an existing system against GDPR requirements. The nature of the analysis was such that the phases of the CeHRes framework were unobvious and hence the roadmap was non-applicable to it. Some of the problems identified in the studies were centered around data privacy [14][15][19][23][19][20][21], consent [21][25][31], ownership of user data [20][27], right to data portability [27], security [19], right to be forgotten [25][28], cyber insurance to cover eHealth assets [28], among others. Interestingly, only one article identified and analysed the stakeholders where surveys were used to collect privacy concerns of stakeholders which were then translated into user requirements [19].

Value specification

Privacy related values of the technology were identified and translated into requirements. A clear and specific goal as well as the associated values of the technology were evident in 22 out of the 23 articles analysed. The

values of the eHealth systems to be designed were clearly articulated by specifying the demands from the implementation context as well as how the set goals could be achieved. While some studies approached value identification from the stakeholder perspective [19], others sought to determine what could be improved or supported by means of an eHealth solution [14][15][29][31][33][18][23][25][27]. The identified privacy values thus formed the basis for the requirements of the design of the technology

Design

The output of the contextual inquiry and value specification phases translated into a unified modelling language diagram [24], conceptual designs [22][14], a high-fidelity prototype [17], and system architectures [31][25][18][19][29][20][16][23][15][30][28][32][26]. Persuasive features were identified from some of the studies. These include self-monitoring [16][18], personalization [29][31][17], reduction [26][23], rewards [26], reminders [29], and competition [29]. Gamification, a component of modern eHealth applications, which encompasses persuasive features was also identified [29]. Some of the studies went ahead to develop solutions [18][23][30][15][28] that solved the identified privacy issue (e.g. [21]) in the eHealth system.

Operationalization

A few studies (4 out of 23) implemented and tested their designs. Four studies piloted their eHealth technologies in different forms including in a real-world environment [18], a proof of concept [23], a field study [15], and an integration into an existing system [28].

Summative evaluation

Only a handful of studies (4 out of 23) evaluated their eHealth technologies. Evaluation of the eHealth technologies were based on the values specified [30]. Two studies assessed the impact on system stakeholders [23][18] , while another evaluated the accuracy of a deep learning model that underpinned their privacy policy extraction system [15].

GDPR and system requirements

eHealth technologies identified from the studies include web applications (e.g. [16]), Internet of Things (IoT) (e.g. [26]), cloud computing (e.g.[32]), artificial intelligence (AI) [24], mobile applications (e.g.[31]), big data [33], and blockchain-based solutions (e.g. [26]). These technologies varied in terms of application domain ranging from general solutions to specific solutions such as solutions tailored for monitoring heart conditions [31], well-being and fitness [7], human-disease infection [33], elderly care (e.g. [29]), and remote care [16].

Static healthcare data includes data that may not change during the lifetime of a person such as fingerprint and genome, whereas dynamic data includes data collected when a user engages in an activity (e.g. heartbeat rate) and the state of the user (e.g. blood test) [7]. Data is collected for an instance or continuously for both static and dynamic data depending on the purpose of the data collection and as such the frequency and size of the data collected, stored, and processed may require different methods and approaches. Typically, data is collected from web applications (e.g.[14]), mobile applications (e.g.[15]), IoT devices (e.g. [22]), or other health information systems [34], among others. These are stored on local or remote servers and/or cloud services.

Theme	Problem	Implemented solution	Example Study
Privacy	privacy issues related to electronic health records such as data breaches	privacy by design model for managing electronic health records	Bincoletto, 2019. [14]
	issues related to readability of privacy policies of eHealth systems	a system to predict and extract privacy policies using privacy concerns of users	Chang et al. 2019 [15]
	privacy issues caused by data leakage in remote digital health interventions	an architecture that secures remote transmission of sensor data	El Jaouhari & Bouabdallah, 2018 [16]
	privacy issues in mHealth apps related to user-app interaction and transparency	integrating GDPR requirements into app visualizations to enhance transparency	Muchagata & Ferreira, 2018 [17]
	privacy issues associated with storing health records in the public cloud	tokenization architecture to remove sensitive information from health records and encryption of the data	Paavola & Ekqvist, 2017 [18]
Privacy/ Security	vulnerability of electronic healthcare infrastructure to privacy and cybersecurity threats	a GDPR compliant platform for managing and transferring eHealth data	Diaz-Honrubia et al., 2019 [19]
	privacy and security challenges related to IoT eHealth systems	an architecture for secured collection, storage and processing of data from IoT systems	Koutli et al., 2019 [29]
Ownership	the need to allow data subjects to control their own data	a GDPR controller to give full control of data to data subjects	Rhahla, Abdellatif, Attia, & Berrayana, 2019 [30]
Privacy/ Ownership	privacy challenges of healthcare data	use of blockchain to enable users control their data	Mohammad Hossein, Esmaeili, Dargahi, & others, 2019 [20]
Trust/ Ownership	trust issues emerging during the exchange of healthcare data between institutions	a federated blockchain application to enable trust and allow users to own, control and exchange their data	Koscina et al., 2019 [25]
	problems associated with ownership and control of health data	blockchain based data sharing systems to enable users to control and own their data	Zheng et al., 2018 [26]
Ownership/Data Portability	the need for patients to own and control their data and data should be in a format that support interoperability	a GDPR compliant blockchain application to give control to the user	Stan & Miclea, 2019 [27]
Consent	issues related to consent in eHealth systems	user-centered electronic consent system that incorporates data subject's rights	O'Connor et al., 2017 [22]
	the need for adequate management of consent in eHealth systems	consent management framework to enable users of eHealth systems manage their own consent	Hyysalo et al., 2016 [23]
Consent/ right to be forgotten	issues related to knowledge management in artificial intelligence eHealth systems	a way to unlink (remove) user data from training samples	Lutze, 2019 [24]
Insurance	data risks emerging from digital health data	a framework for risk assessment and insurance against risks	Hatzivasilis et al. 2019 [28]

Table 2. Problems related to GDPR and proposed solutions

The rights enjoyed by data subjects sit at the heart of GDPR with 19 out of the 23 articles reviewed addressing data subject rights. Nine articles discussed the right to access, five articles discussed the right to be forgotten, two articles addressed the right to rectification, three articles addressed data portability, while 18 articles addressed privacy by design. Interestingly, only one article addressed the issue of breach notifications. Clearly, there exist a need for a more solid and consolidated effort in implementing data subject rights in eHealth systems comprehensively to ensure compliance with GDPR requirements.

The enforcement of the GDPR poses a significant amount of challenges to eHealth systems. GDPR gives a new dimension to issues of security and privacy, putting the user at the center of it all, with additional requirements that eHealth systems need to comply with. Interestingly, we identified several challenges which we have classified into high-level themes. These high-level themes represent the areas from which the reviewed articles identified GDPR-related problems and to which they proposed solutions. Privacy is a theme

that a vast majority of the articles focused on. While some discussed privacy in eHealth systems in general, others were more specific, focusing on privacy of health data, privacy during data transmission and storage. Some of the themes however overlap with each other. A detailed description of the classification, the problems and challenges identified by the studies, and their suggested solutions can be found in Table 2.

GDPR and persuasion for behaviour change

Behaviour change support systems are developed with persuasive features that enable and support users change their behaviour over time. From our analysis, only two persuasive features in eHealth systems were identified that targeted behaviour change: personalization and self-monitoring [31][29]. Persuasion through personalization and self-monitoring is carried out based on the data of the information system. It is important that this data meets the GDPR requirements of the consent to collect, store and process data, the right to access data, the right to be forgotten, as well as privacy. These requirements must be properly incorporated into the design of behavioural change systems.

GDPR and Persuasive System Design

Persuasive System Design (PSD) is a model for designing and evaluating persuasive systems [35]. The PSD model specifies key issues that have the tendency to persuade a user. These include supporting the user to perform primary tasks of the eHealth system, supporting the interaction between humans and the system, supporting the credibility of the system and providing social support if necessary. Persuasion occurs via the content of the eHealth system, software features offered, the credibility of the system to function and privacy trust. For example, the content and software features have conflicting implications on the privacy of the user. Privacy issues are imperative because they act as barriers that influence the use of eHealth systems [5]. In Table 3, we summarize persuasive features according to support categories of the PSD model with examples of GDPR requirements and implementation for each.

Category	Example GDPR Requirement	Example GDPR Implementation
Primary task support	• Systems should protect the privacy of its users • Systems should allow users to control their own data • Systems should seek the consent of users when collecting and processing their data • Systems should limit data collection to what is needed for persuasion to be effective • Data collection and processing should be recorded for accountability	• The app limits the amount of data to what is needed for the functioning of the app • The app allows users to rectify incorrect information
Dialogue Support	• Systems should provide feedback in a way that does not reveal private or sensitive information	• The app displays important information but not information that compromises the privacy of the user • The app allows users to use pseudonyms or avatars instead of their real names
System credibility support	• Systems should demonstrate compliance with GDPR rules	• The app displays the contact details of the Data Protection Officer (DPO) to enable users to request information about their data • The app provides a means for users to configure privacy settings • The app shows the logo of privacy rules complied to
Social support	• Systems should preserve the privacy of users in social settings	• The app informs and seeks the consent of users before sharing data with other users

Table 1. Persuasive principles and GDPR requirements

Persuasive systems rely on user data such as goals, preferences, and lifestyle as well as objective data such as phone app usage, heart rate, etc. obtained from mobile and wearable device sensors [35]. The availability of such data enables persuasive systems to create and make better recommendations to users (e.g. to match the content with user preferences). Such user data is subject to GDPR requirements hence in building persuasive

systems, it is important to consider how the various data subject rights can affect the performance of the system (e.g. the right to be forgotten).

Often, software features in persuasive systems are tailored for user segments and hence not truly unique for an individual user [36]. Unique software features for an individual user would require personal data and may raise privacy concerns. The possibility of providing truly unique persuasive features to match an individual's preferences provides an interesting research opportunity but it is very complex [37]. Such features could perhaps sustain behaviour change and/or equip users to commit to their set goals. Such a feature is analogical to human gratitude when another human or creature demonstrates thoughtfulness. As we aim to closely mimic human ways in human-computer interaction, unique and meaningful persuasive features in eHealth systems cannot be overemphasized. Providing such unique features requires a large amount of user data and huge computational capabilities which may not be possible with the current fourth generation (4G) telecommunication networks. Perhaps the introduction of fifth generation (5G) and subsequent telecommunication networks could create this possibility. We call for research into individualized persuasive features and encourage debates on the perceived persuasiveness of unique features based on the preferences of an individual.

Discussion

Research has shown that privacy remains a concern for electronic health records produced from eHealth systems [38]. Persuasive strategies such as monitoring, tracking, and personalization affect the privacy of users. Not only is health data sensitive, it may also trigger placebo effect [39] and/or undesired outcomes which may lead to coercion [40] and falsification of information (by the user) [41]. These issues have the tendency to affect the efficiency of an eHealth application particularly for systems that offer personalization and recommendations. As such, the designers and developers of persuasive technologies should aim to protect the privacy of users as their own. This also applies to third party data collectors [42].

This systematic review was conducted to identify the requirements of GDPR in eHealth systems and technologies particularly those that persuade users. The results obtained shows that lingering privacy concerns can be addressed when GDPR requirements are factored in the design and development of eHealth systems. The study confirms that there is a relationship between privacy and GDPR requirements. Although GDPR presents a tall list of requirements which may seem overwhelming or even impossible to implement, we beg to differ. We argue this can be simplified if developers carefully analyse the data required for persuasive software features, identify the privacy issues and address them with the corresponding GDPR requirement (See examples in Table 3). This analysis should be carried out at the onset of the software project. Using approaches such as the CeHRes Roadmap as a guide, the privacy concerns of stakeholders can be identified in the contextual inquiry phase. Privacy values can be specified and incorporated into the design and development of the eHealth system. Also, privacy requirements of the technology such as frequency of data collection, storage and data processing activities (e.g. anonymization, encryption) must be specified and incorporated into the design and development of the system. The knowledge obtained from privacy concerns of stakeholders and privacy requirements of the system can be useful information for crafting meaningful and informed privacy policies. After the development, concrete plans must be made to test and prepare the system for use. The plan must include benchmarks which will be used to assess the functionality, privacy and security aspects of the system by stakeholders in the evaluation phase. We advocate involving stakeholders as much as possible from the contextual inquiry phase through to the evaluation phase of the CeHRes Roadmap or any similar holistic eHealth development framework. This will help address the privacy concerns of users and fulfil the requirements of privacy legislations like GDPR.

Notwithstanding, some GDPR requirements such as the right to be forgotten [27] and accountability requirement [43] for artificial intelligence (AI) based technologies may be challenging to implement [44][45]. While a data subject can request to be forgotten, this request can also be rejected based on public interest.

These critical issues must be factored into the design. New fields of research such as explainable AI [45] seek to make transparent the AI. This is a step in the right direction to ensure transparency and accountability of 'AI-powered' eHealth systems. It can therefore be assumed that adherence to GDPR requirements in eHealth technologies will significantly increase trust and transparency between developers of eHealth applications and its users which may ultimately affect its adoption and use.

Conclusion

In this study, we investigated how GDPR is implemented in eHealth systems as addressed in literature. The relevance of a holistic approach to the development of eHealth systems cannot be overemphasized especially when it addresses privacy concerns of stakeholders and fulfils GDPR requirements. As the literature review shows, there is a missing anchor in terms of the implementation of data subject rights. Only a few studies extensively addressed data subject rights in the reviewed papers. To address such shortcomings, we advocate an all-encompassing agenda that will empower and enable both researchers and practitioners to work together to guarantee compliance of eHealth systems to GDPR requirements. This can be done by ensuring that not only privacy but also data subject rights, and system evaluation become a fundamental value anchored in eHealth systems; particularly behaviour change systems and persuasive technologies.

The need for a human-centric viewpoint to the implementation of GDPR is yet to be exhaustively discussed within the scope of eHealth systems. We hope that our study is in itself a call to action concerning these issues.

References

[1] H. Oh, C. Rizo, M. Enkin, and A. Jadad, "What is eHealth (3): a systematic review of published definitions," *J. Med. Internet Res.*, vol. 7, no. 1, p. e1, 2005.

[2] H. Oinas-Kukkonen, "A foundation for the study of behavior change support systems," *Pers. ubiquitous Comput.*, vol. 17, no. 6, pp. 1223–1235, 2013.

[3] G. Eysenbach, "What is e-health?," *J. Med. Internet Res.*, vol. 3, no. 2, p. e20, 2001.

[4] D. Slamanig and C. Stingl, "Privacy aspects of ehealth," in *2008 Third International Conference on Availability, Reliability and Security*, 2008, pp. 1226–1233.

[5] K. Raychaudhuri and P. Ray, "Privacy challenges in the use of eHealth systems for public health management," in *Emerging Communication Technologies for E-Health and Medicine*, IGI Global, 2012, pp. 155–166.

[6] T. Sahama, L. Simpson, and B. Lane, "Security and Privacy in eHealth: Is it possible?," in *2013 IEEE 15th International Conference on e-Health Networking, Applications and Services (Healthcom 2013)*, 2013, pp. 249–253.

[7] C. Braghin, S. Cimato, and A. Della Libera, "Are mHealth Apps Secure? A Case Study," *2018 IEEE 42nd Annu. Comput. Softw. Appl. Conf.*, vol. 02, pp. 335–340, 2018.

[8] C. Granja, W. Janssen, and M. A. Johansen, "Factors determining the success and failure of eHealth interventions: systematic review of the literature," *J. Med. Internet Res.*, vol. 20, no. 5, p. e10235, 2018.

[9] T. Greenhalgh and J. Russell, "Why do evaluations of eHealth programs fail? An alternative set of guiding principles," *PLoS Med.*, vol. 7, no. 11, p. e1000360, 2010.

[10] J. E. W. C. van Gemert-Pijnen *et al.*, "A holistic framework to improve the uptake and impact of eHealth technologies," *J. Med. Internet Res.*, vol. 13, no. 4, p. e111, 2011.

[11] L. van Gemert-Pijnen and M. Span, "CeHRes roadmap to improve dementia care," *Handb. Smart Homes, Heal. Care Well-Being*, pp. 133–146, 2017.

[12] "GDPR Archives - GDPR.eu." [Online]. Available: https://gdpr.eu/tag/gdpr/. [Accessed: 10-Feb-2020].

[13] X. Shao and H. Oinas-Kukkonen, "How Does GDPR (General Data Protection Regulation) Affect Persuasive System Design: Design Requirements and Cost Implications," in *International Conference*

on Persuasive Technology, 2019, pp. 168–173.
[14] G. Bincoletto, “A Data Protection by Design Model for Privacy Management in Electronic Health Records,” in *Annual Privacy Forum*, 2019, pp. 161–181.
[15] C. Chang, H. Li, Y. Zhang, S. Du, H. Cao, and H. Zhu, “Automated and Personalized Privacy Policy Extraction Under GDPR Consideration,” in *International Conference on Wireless Algorithms, Systems, and Applications*, 2019, pp. 43–54.
[16] S. El Jaouhari and A. Bouabdallah, “A Privacy Safeguard Framework for a WebRTC/WoT-Based Healthcare Architecture,” in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, 2018, vol. 02, pp. 468–473.
[17] J. Muchagata and A. Ferreira, “Translating GDPR into the mHealth Practice,” *2018 Int. Carnahan Conf. Secur. Technol.*, pp. 1–5, 2018.
[18] J. Paavola and J. Ekqvist, “Privacy Preserving and Resilient Cloudified IoT Architecture to Support eHealth Systems,” in *Interoperability, Safety and Security in IoT*, Springer, 2017, pp. 134–143.
[19] A. J. Diaz-Honrubia *et al.*, “An overview of the CUREX platform,” in *2019 IEEE 32nd International Symposium on Computer-Based Medical Systems (CBMS)*, 2019, pp. 162–167.
[20] K. Mohammad Hossein, M. E. Esmaeili, T. Dargahi, and others, “Blockchain-based privacy-preserving healthcare architecture,” 2019.
[21] R. L. B. Neame, “Privacy protection in personal health information and shared care records,” *J. Innov. Heal. Informatics*, vol. 21, no. 2, pp. 84–91, 2014.
[22] Y. O’Connor, W. Rowan, L. Lynch, and C. Heavin, “Privacy by design: informed consent and internet of things for smart health,” *Procedia Comput. Sci.*, vol. 113, pp. 653–658, 2017.
[23] J. Hyysalo, H. Hirvonsalo, J. J. Sauvola, and S. Tuoriniemi, “Consent Management Architecture for Secure Data Transactions.,” in *ICSOFT-EA*, 2016, pp. 125–132.
[24] R. Lutze, “Digital Twins in eHealth – : Prospects and Challenges Focussing on Information Management,” in *2019 IEEE International Conference on Engineering, Technology and Innovation (ICE/ITMC)*, 2019, pp. 1–9.
[25] M. Koscina, D. Manset, C. Negri, and O. P. Kempner, “Enabling trust in healthcare data exchange with a federated blockchain-based architecture,” 2019.
[26] X. Zheng, R. R. Mukkamala, R. Vatrapu, and J. Ordieres-Mere, “Blockchain-based personal health data sharing system using cloud storage,” in *2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom)*, 2018, pp. 1–6.
[27] L. Stan, O. P., & Miclea, “New Era for Technology in Healthcare Powered by GDPR and Blockchain,” in *In 6th International Conference on Advancements of Medicine and Health Care through Technology;*, 2019, pp. 311–317.
[28] G. Hatzivasilis *et al.*, “Cyber Insurance of Information Systems,” in *2019 IEEE 24th International Workshop on Computer Aided Modeling and Design of Communication Links and Networks (CAMAD)*, 2019, pp. 1–6.
[29] M. Koutli *et al.*, “Secure IoT e-Health Applications using VICINITY Framework and GDPR Guidelines,” in *2019 15th International Conference on Distributed Computing in Sensor Systems (DCOSS)*, 2019, pp. 263–270.
[30] M. Rhahla, T. Abdellatif, R. Attia, and W. Berrayana, “A GDPR Controller for IoT Systems: Application to e-Health,” in *2019 IEEE 28th International Conference on Enabling Technologies: Infrastructure for Collaborative Enterprises (WETICE)*, 2019, pp. 170–173.
[31] U. Mustafa, E. Pflugel, and N. Philip, “A Novel Privacy Framework for Secure M-Health Applications: The Case of the GDPR,” in *2019 IEEE 12th International Conference on Global Security, Safety and Sustainability (ICGS3)*, 2019, pp. 1–9.
[32] R. Ducato, “Cloud computing for s-health and the data protection challenge: Getting ready for the General Data Protection Regulation,” in *2016 IEEE International Smart Cities Conference (ISC2)*, 2016, pp. 1–4.
[33] P. Kostkova, “Disease surveillance data sharing for public health: the next ethical frontiers,” *Life Sci. Soc. policy*, vol. 14, no. 1, p. 16, 2018.
[34] M. Sousa *et al.*, “OpenEHR Based Systems and the General Data Protection Regulation (GDPR),” *Build. Cont. Knowl. Ocean. Data Futur. Co-Created EHealth*, 2018.

[35] H. Oinas-Kukkonen and M. Harjumaa, “Persuasive systems design: Key issues, process model, and system features,” *Commun. Assoc. Inf. Syst.*, vol. 24, no. 1, p. 28, 2009.
[36] H. Oinas-Kukkonen, “Personalization Myopia: A Viewpoint to True Personalization of Information Systems,” in *In Proceedings of the 22nd International Academic Mindtrek Conference (pp. 88-91). ACM.*, 2018.
[37] W. P. Klasnja, Predrag, Sunny Consolvo, “How to evaluate technologies for health behavior change in HCI research.,” in *conf*, 2011.
[38] M. Meingast, T. Roosta, and S. Sastry, “Security and privacy issues with health care information technology,” in *Annual International Conference of the IEEE Engineering in Medicine and Biology - Proceedings*, 2006, pp. 5453–5458.
[39] R. J. Beun *et al.*, “Improving Adherence in Automated e-Coaching A Case from Insomnia Therapy,” 2016.
[40] R. Cheng, “Persuasion Strategies for Computers as Persuasive Technologies.”
[41] E. M. Raybourn *et al.*, “Data privacy and security considerations for personal assistantsfor learning (PAL),” in *International Conference on Intelligent User Interfaces, Proceedings IUI*, 2015, vol. 29-March-2015, pp. 69–72.
[42] J. Davis, *Design Methods for Ethical Persuasive Computing*. .
[43] S. Wachter, B. Mittelstadt, and L. Floridi, “Transparent, explainable, and accountable AI for robotics,” 2017.
[44] P. Guarda, “Essays ‘Ok Google, am I sick?’: artificial intelligence, e-health, and data protection regulation.”
[45] W. Samek, T. Wiegand, and K.-R. Müller, “Explainable Artificial Intelligence: Understanding, Visualizing and Interpreting Deep Learning Models,” Aug. 2017.