pHealth 2022
B. Blobel et al. (Eds.)

doi:10.3233/SHTI220968

Privacy and Trust in pHealth - Past, Present and Future

Pekka RUOTSALAINEN[a,1], Bernd BLOBEL[b,c,d]
[a] *Faculty of Information Technology and Communication Sciences (ITC), Tampere University, Finland*
[b] *Medical Faculty, University of Regensburg, Germany*
[c] *eHealth Competence Center Bavaria, Deggendorf Institute of Technology, Germany*
[d] *First Medical Faculty, Charles University of Prague, Czech Republic*

Abstract From beginning to today, pHealth has been a data driven service that collects and uses personal health information (PHI) for personal health services and personalized healthcare. As a result, pHealth services use intensively ICT technology, sensors, computers and mathematical algorithms. In past, pHealth applications were focused to certain health or sickness related problem, but in today they use mobile devices, wireless networks, Web-technology and Cloud platforms. In future, pHealth uses information systems that are highly distributed, dynamic, increasingly autonomous, multi-stakeholder data driven eco-system having ability to monitor anywhere person's regular life, movements and health related behaviours. Because privacy and trust are pre-requirements for successful pHealth, this development raises huge privacy and trust challenges to be solved. Researchers have shown that current privacy approaches and solutions used in pHealth do not offer acceptable level of privacy, and trust is only an illusion. This indicates, that today's privacy models and technology shall not be moved to the future pHealth. The authors have analysed interesting new privacy and trust ideas published in journals, and found that they seem to be effective but offer only a partial solution. To solve this weakness, the authors used a holistic system view to aspects impacting privacy and trust in pHealth, and created a template that can be used in planning and development future pHealth services. The authors also propose a tentative solution for future trustworthy pHealth. It combines privacy as personal property and trust as legal binding fiducial duty approaches, and uses a Blockchain-based smart contract solution to store person's privacy and trust requirements and service providers' promises.

Keywords Privacy, Trust, System view, Fiducial Duty, Privacy law, Smart Contract

Introduction

While being focused on personal health and services as well as personalized health and health care, pHealth presents a horizontal view to health care, eHealth and mHealth. Real life pHealth services and applications vary in size and interest. It can be a single sensor-based monitoring solution (e.g., heart rate monitoring), or it has a multi-dimensional view to person's health problems (e.g., support for independent living). From

[1] Corresponding Author. Pekka S. Ruotsalainen, DSc (Tech.), Adjunct professor, Research professor emeritus, Faculty of Information Technology and Communication Sciences (ITC), Tampere University, Kanslerinrinne 1, 33014 Tampere, Finland; Email:pekka.ruotsalainen@uta.fi

technological point of view, pHealth can appear as person's health problem focused application or as personal health system (PHS) that collects personal health information (PHI) using body sensors and wearables. Currently, it is increasingly part of a multi-stakeholder eco-system focusing on health management.

From past to today, information systems for healthcare and health have performed a meaningful development at conceptual, technological and information system levels. An important driver for this development has been the paradigm shift in health care, i.e., the transition from hospital centred and reactive healthcare to person-centred preventive and even predictive care [1]. In the past, health care information systems (e.g., hospital information systems) were institutional, local, siloed and static. In today, health care and health information systems are increasingly cross-organizational, communicative, networked ecosystems with data sharing capability.

During last 15 years, pHealth has underwent similar transition as health care. In the past, many of pHealth applications were local, focused on the use of certain body sensors and wearables to measure and analyse person's health and sickness related body functions. The goal was to support the management of person's health or illness, self-care and independent living. Nowadays, pHealth services use different kind of artifacts such as sensor, mobile devices, wireless networks, Web-technology and Cloud platforms for collecting, storing and processing PHI to support on-line personalized care and health management. Current pHealth services are also increasingly part of a multi-stakeholder eco-system.

At present, the collection of personally identifiable information (PII) takes place every day and everywhere when we are using networks, personal computers, smart phones and wellness devices. Our behavioural health related activities are tracked by the browser, and our e-mails can be read by applications or cookies invisibly injected by applications [2, 3]. Furthermore, PHI is not collected and processed only by regulated healthcare organizations and professionals, but also by commercial non-regulated health service providers, web service providers and social web applications. PHI is also shared and sold between them [4-7]. Researchers have observed that digital information systems are seldom designed with privacy in mind [8].

This situation has raised huge privacy and trust concerns. In today's health information systems, it is difficult or even impossible for a person to know what PHI is collected, used and disclosed by whom for what purposes, which privacy laws are deployed by the service provider, and how to maintain privacy in distributed ecosystems [7, 9-11]. In real life, it is almost impossible for the service user to prevent unnecessary data collection and to know to whom data is disclosed. Furthermore, security-based solutions widely used in current information systems are ineffective in privacy protection. Therefore, the assumption that a person can control the use of his or her personal information in the Internet and ecosystems is just an illusion. In fact, we simply do not have privacy [12].

Concerning trust, the situation is not much better. From past to today, it has been expected that people blindly trust in service provider and in technology used (e.g., computers, mobile phones networks Clouds and data storages, and applications). According to Mc Knight et al. it is expected that a service user believes (typically without any proof) that structures such as guarantees, regulations, promises, legal recourse and procedures are in place (i.e., structural assurance), and that the environment is in proper order (i.e., situational normality) [13]. According to Ruotsalainen et al., this is unfortunately a wrong assumption, because in distributed and multi-stakeholder environments such as pHealth, it is almost impossible to know to whom and why to trust

[14]. Researchers have observed that in today's digital information systems not only privacy is an illusion, but also trust is only a belief [15].

In the future pHealth, the situation can be even more serious, because information systems used by pHealth will be highly distributed, dynamic, increasingly autonomous, data-driven multi-stakeholder ecosystems. Those systems have the ability to monitor anywhere person's regular life, movements and health related behaviours using smart sensors and surveillance systems, and to combine this multi-source information to personal Big Health Data that can support 5P medicine and pHealth in many ways. Personal Big Health Data can be used for different analysis, to calculate detailed personal health profiles, detect of changes in personal health and disease, to support continuous health management, and for the development of personal health devices and services. It can be also easily misused for other purposes. Researchers expect, that future pHealth will rely on Internet of Things (IoT) based data collection, advanced computer methods such as machine leaning (ML), artificial intelligence (AI) and deep learning (DL) [11, 16]. They all need the availability of Big Data. Future pHealth applications and services can also empower to better understand causes of diseases [17]. The development of pHealth does not stop with the collection and intelligent use of PHI. In the future, mobile manipulators will be also part of the pHealth ecosystem. As those manipulators have ability to navigate in space and manipulate objects, communicate with person and networks, and have autonomous capabilities, they have the potential to assist people in everyday tasks, for example in home [18].

In spite of the big promises of the future pHealth, the development can lead to a situation where for a person as the source of PHI and at the same time user of pHealth service, there is no privacy, and she or he has to trust blindly in technology providers' goodwill in the environment of insufficient regulations [11]. To find a way from the current unsatisfactory situation to future trustworthy and privacy-enabled pHealth, the authors have studied both privacy and trust challenges existing in today's pHealth services and information systems, and new privacy and trust approaches and solutions proposed by researchers. Based on findings got, the authors have formulated a summary of principles, architectural models, rules and technological artefacts which, when used as hole, have power to make future pHealth ethically acceptable, trustworthy, and at the same time support person's privacy needs.

1. Privacy and Trust Approaches and Challenges

As discussed in the introduction chapter, pHealth is sensitive, health data driven service or application. Therefore, high level of privacy and trust is a prerequisite for successful pHealth. Because pHealth applications and services are typically build over general ICT technology and services (e.g., the Internet, mobile networks and Cloud services), their privacy and trust challenges can be used as proxy for pHealth.

Information privacy and trust are dynamic, situational, context-depending and vague concepts without globally accepted definition [7, 19]. This makes it challenging to conceptualize them and to perform them by computer programs. Privacy is human and constitutional right [20], but not an absolute policy. In principle, privacy addresses the question "what would we like others to know of us". Privacy is also a regulatory concept. In western countries, privacy is for long understood as a personal right to protect individuals against something (e.g., against other's manipulation, control or surveillance),

and to prevent others from harmfully actions. Widely used privacy models include privacy as control, privacy as a commodity, privacy as property or contextual integrity, privacy as a concern and legal construct, risk-based privacy, and privacy as behavioural concept and social good [21, 22].

The principle of autonomy is one of cornerstones of privacy, i.e., to control when and by whom PHI is collected, and for what purposes it is used [22]. The concept of privacy as a commodity understands privacy as economic good that can be traded for other goods or services [23]. Privacy as a concern refers to individuals' anxiety regarding data collectors' and processors' practices in collection, using and sharing data. Privacy as a regulative (legal) construct tries to regulate the disclosure and use of information in a context, and to protect individuals [24]. The risk-based approach to privacy focuses on risk such as harm, caused by unnecessary data collection, misuse and disclosure, surveillance and behavioural manipulation [25]. The nature of privacy and the lack of availability of reliable information make the measurement of actual (objective) privacy challenging [26]. Therefore, different proxies such as perceived risks, service level agreements, external third-party seals, service provider's privacy policy documents, reputation, direct observations, and degree of compliance with laws or standards are widely used instead [7].

Despite privacy is a fundamental right, there is always a tension between public and commercial interest to collect and use of PHI on one side and person's need for privacy on the other side. According to Ruotsalainen et al., nowadays, industry sees increasingly personal information as raw material for products and services, and society as public good. Therefore, there exist conflicting interests between individual's need for privacy on one hand and the use of PHI for meaningful public benefits or for making profit on the other hand [11].

A big privacy challenge is that today's ICT technology enables the collection, use and storage of extremely sensitive health-related information about person's life, health problems and behaviour. Modern sensors, microchips and computer technology, wearables and consumer level devices such as smart wrists have the ability to measure not only blood pressure, heart rate, quality of sleeping and social activities, but also personal training, emotions, mood, voice profile and daily life health behaviours. Furthermore, person's sweat, urea, breath gases, faces, or saliva can be measured and analysed as well. Smart-video-based facial recognition applications have the ability to analyse our emotions such as joy, sorrow and smiling. Furthermore, video surveillance systems in public spaces can monitor our social and health related behaviours. In the Web, there are tens of thousands health apps collecting and using PHI, and many people also self-disclose their personal health problems in social networks [19]. Currently, all this data is typically stored in the Web (e.g., in Clouds and platforms), and this enables the creation of a virtual personal Big Health Data repository. An additional privacy concern is that person's behavioural health data is systematically and hidden tracked by Web service providers, health apps and Web platforms. According to Dobkin et al., at least 77.4% of Websites globally track visitors' data and behaviour [27]. Zuboff has noted that behavioural tracking is not only used to measure body signals, but it covers also our physical and social behaviours and how we use information systems [28].

A big privacy concern is that PHI is increasingly used outside the regulated health care domain and by personal health wellness applications in the Web. Nowadays, PHI is not only used for health services, but also for social control, crime prevention, prevention of antisocial behaviours, to control humans' social life and behaviours, and to manipulate person's decisions.

Trust exists in the relationship between a trustor and trustee. It is widely understood as a social norm, subjective feature, psychological state, personal trait, and willingness to be vulnerable to other party's expected or unexpected actions without the ability to monitor or control them [29] Trust is needed in situations, where the trustor has insufficient information about the features and trust behaviours of the trustee [30].

Thrust can be a disposition, attitude, belief, expectancy, feeling willingness to trust, and perception based on own previous experiences or others' recommendations. It takes place between persons, but also between a person and a technical artifact (e.g., computer application or information system). Trust is necessary in situations where the trustor has insufficient information about the features and behaviours of the trustee [31]. Disposition (propensity) to trust is the tendency to trust others. Perceived trust is often only an opinion. Thrust can be also computational, i.e., based on measured features of the trustor and used information system [29]. Computational trust imitates the human notion of trust, and it is widely used to substitute mental trust models [30].

The lack of trust is a big problem when we are using computers, mobile phone networks, digital information systems, or the Internet and Web services. This environment is also a problem in pHealth, because its services are built over commercial digital technology. The user of pHealth service has not only to trust in a service provider, but also in invisible computer technologies, applications and algorithms. According to Mc Knight, trust in technology is often a belief that technology used is reliable, secure, and protects information privacy, and appropriate governance is established and enforced [32].

Currently, service providers and platform mangers often expect that the level of privacy the service user needs is a result of the balancing person's privacy needs against service provider's business objectives and requirements. Because the service provider is in real life often the stronger actor, this balancing means that the service provider's business benefits regularly override person's privacy needs. Therefore, the most practical solution for a person to maintain privacy is to reject the service, filter the amount of PHI he or she has willingness to disclosure or add noise to data [33]. In real life, stakeholders' privacy and trust features are seldom available, and the person has limited or no power for negotiation with the service provider to force her/him taking into account personal privacy needs. Instead, the service user is forced to accept service provider's privacy promises (policy) and trust manifesto in the form of a take-it-or-leave-it approach [27].

There are many other challenges. One is, that service providers are increasingly monetarizing personal information by selling collected PHI to other actors. Another problem is that the number of applications using PHI for secondary purposes in rapidly increasing. Examples of that include job recruiting, credit checks, the justice system, predictive policing, and determining health care for people**.** Furthermore, ML, AI and DL are used to analyse Big Health Data for providing personalized life style related proposals, health predictions, and context-aware profiles.

International organizations, regulators and governments have established both general and privacy laws, norms, standards, Golden Rules and health care specific acts to enable meaningful use of personal data, and to restrict unnecessary secondary use of PHI. Current privacy laws and guidelines are built on the principle of privacy as legal right, and a control as well as notice-and-choice approach [22]. From the person's point of view, privacy laws and Golden rules seem unfortunately to be weak compromises and in real life ineffective and not widely implemented by industry [24]. Laws also offer poor privacy in public spaces, and behavioural privacy is not protected [28].

A big problem from data subjects' and pHealth service users' point of view is that commercial service providers have low incentives to enforce strong privacy policies, and often they do not keep their privacy trust promises. Instead, they often fail to provide even basic privacy protection [34, 35]. Furthermore, researchers have shown that current security and control-based solutions have failed to guarantee privacy in distributed and dynamic digital environment, and many big Web actors and service providers simply do not worry of privacy laws [26, 37]. The result is, that the lack of reliable information of service provider's, networks and applications' privacy and trust features has leaded to situations where feeling or opinion is the only measure of privacy and trust in pHealth.

From a personal point view, the current situation concerning privacy and trust in digital information systems is unsatisfactory, and when thinking of future highly distributed, dynamic and increasingly autonomous pHealth, the situation will be even more challenging. The use of AI, ML and DL, especially if raw PHI is used, generates privacy challenges such as the possibility of data reconstruction, and difficulties to support person's privacy policies, erasing of data and realizing the right to be forgotten [38]. Extensive collection of detailed PHI, health tracking and the creation of Big Health Data repositories can lead to total loss of autonomy and increased behavioural, social and political control, behavioural manipulation and discrimination, routinely monitoring of personal health and wellness in work and public places, and finally the commodization of PHI [11]. The authors state that better privacy and trust solutions than what is used now are indispensable for future pHealth. They should take into account person's and service user's privacy and trust concerns and enable them to know what PHI is collected, used and shared? Furthermore, persons need reasons to trust in the implementation and efficiency of laws and regulations, in service providers' and technology providers' privacy policies, features and behaviours, and in information systems as a whole. In the future pHealth, it should be clear, who is the owner of our PHI in different contexts, and what is the impact of data collection, and how data is used and shared by different apps. The data subject shall also have the possibility to measure (or estimate) using reliable data, what is the actual level of privacy and trust in pHealth information system.

2. New Privacy and Trust Approaches and Technological Solutions

Researcher have not only studied privacy and trust challenges existing in today's pHealth, but also proposed new approaches and solutions for privacy and trust to be used in future distributed information systems. Some of them are quite radical and require a paradigm change and new laws, but others rely on currently used privacy and trust models, and propose only architectural, mathematical and functional solution, Table 1, [29].

Balkin has proposed a concept of information fiduciary [39]. According to Balkin, a fiduciary (person or organization) has special obligations of loyalty and care toward another person and the responsibility not do harm. Fiduciaries must also act in the interests of another person. This means, that for example a fiduciary must accept and implement person's privacy needs. Because powerful organizations, such as online service providers and cloud companies, regularly collect, analyse, use, sell, and distribute personal information, Balkin suggested that they should be understood as information fiduciaries toward their customers and users of their digital services [39]. According to Barret, an information fiduciary model can strengthen protections for privacy, equality, and autonomy in the digital age [40]. According to Dobkin, the principle of information

fiduciary should be a legally imposed as duty [27]. Fiduciary relationship as legal duty is also a trust builder. For Mayer, trust in fiduciary relationships is based on the professional's competence and integrity [41].

Table 1 Examples of new privacy and trust models and solutions

Concept of information fiduciary as duty	New concept
Privacy as trust	New way to understand privacy
Personal information as property Privacy as intellectual property	Defines data ownership and new property rules A radical philosophical approach
Privacy as trust and legal binding fiducial duty	Expands trust as legal binding duty model
Computational privacy and trust	Uses available information and mathematical methods
Person controlled use of PHI	Proposal based on the use of cryptography
Cryptographic models	Blockchain Smart contract Patient controlled use of PHI
Data protection by encryption	Differential privacy Homomorphic
Privacy risk analysis-based approach (EU-GDP)	Part of the EU-GDPR act
New information architecture	Edge architecture

For Waldman, privacy in information sharing context is a social construct based on trust [22]. He has proposed a new way to understand privacy as Privacy as Trust approach that is not bound to the concepts of control, choice, autonomy, or seclusion. It a radical concept that presents a principal movement from the right to privacy to trust. According to Waldman, privacy as trust creates a fiduciary relationship between data subject and users. In this approach, a private context is also a trusted context [22].

Ritter et al., have proposed regulating digital information as a new class of property under current legislation. In this approach, rights of ownership for digital data establishes control of its use [42]. According to Samuelson, current laws do not give individuals the full right to control the use and disclosure of personal data. The informational property rights approach empowers individuals however to negotiate with organizations and firms the ways data is used [43]. Ruotsalainen et al. have proposed to use the Privacy as Property approach in such way that it enables a person to define personal privacy policies [11].

It is also possible to combines approaches and solutions shown in Table 1. Ruotsalainen et al. have made a solution that combines privacy as personal property model, trust as fiducial duty, legally binding smart contract, and Blockchain-based repositories for contracts [7]. In this approach, legally binding duties prevent big companies to set their own privacy standards. Instead, it defines a digital service level agreement the service provider must follow [11].

In the case, reasonable information of service providers' and information systems' privacy features is available, the data subject or service user can use mathematical methods to calculate the level of privacy and trust in an information system. Ruotsalainen et al., have used a Fuzzy Linguistic method to calculate the Merit of Service (Fuzzy attractiveness rating) for the whole ecosystem, where PHI is collected, processed, and shared [30].

The model of person-controlled use of PHI is based on the idea that a person has full control over operations with own PHI (e.g., the person grants or rejects granular access to the record storing PHI in a context). For access control, the person has to generate a private-public-key pair. The encrypted data is typically stored using Blockchain technology [44]. Yue et al. have proposed a Blockchain solution that enables the patient to own, control and share own data securely without violating privacy [45].

Cryptographic techniques such as encryption, differential privacy, or k-anonymity are widely used for anonymous communication and in data analysis. New encryption methods such as fully homomorphic encryption and differential privacy can be used to anonymize data. New homomorphic encryption allows calculations with the data without decryption, that way offering a strong solution for privacy [46].

A contractual agreement such as service level agreement (SLA) is one of strongest methods to guarantee service level and quality. Legally binding SLA is typically made performed between organizations, but it is not offered to pHealth customers [47]. Smart contracts are computer programs that automatically execute the terms of a contract in transparent and auditable manner. One of its features is that it can be executed by a network of mutually distrusted nodes without the need of a trusted authority [48]. For integrity, availability and non-repudiation of the contract, the content of a smart contract can be stored in a Blockchain. That kind of smart contract can be used by a person to publish personal privacy policies for all users of his or her PHI [29].

A Blockchain is a time-stamped series of records that is managed by a cluster of computers not owned by any single entity. In it, data blocks are bound to each other using cryptographic technology [49]. Blockchain offers advantages such as anonymity, decentralized trust, confidentiality and integrity of documents, authentication and non-repudiation of data. To enable control of actions, data transactions are signed by the owner using a private key [49]. For privacy, encryption is needed. Blockchain technology is increasingly used not only in commerce but also in health care.

In Edge Computing, cloud services are moved to the network edge [50]. Edge consists of human-controlled devices such as PCs, smart phones, IoT devices, personal health devices and local routers [51]. From a privacy point of view, its benefit is that sensitive personal data is located in the edge, and the control of trust and secure data flow belongs to it.

3. System View to Privacy and Trust in pHealth

As discussed in earlier chapters, future pHealth is increasingly part of a highly distributed and dynamic multi-stakeholder information system that uses intensively AI, ML and DL for detailed personal health analysis. It can also share PHI and results with other partners across contexts and jurisdictions. Stakeholders of the network have typically different business and privacy policies as well as trust features. These features of next generation pHealth indicate, that traditional control- and protection-based privacy solutions are insufficient, and belief or promises based trust will not work. Researchers have proposed

a big variety of solution from encryption to new privacy approaches (Chapter 3), but none of them is a silver bullet. The authors state, that instead of a single method or solution (e.g., encryption of PHI) for privacy and trust a holistic system view is needed. It takes into account privacy and trust models used by stakeholders, features of the environment, stakeholders', information systems and applications' privacy and trust features, sensitivity of data collected and used, and data subject's or service user's personal privacy and trust needs. Based on findings made by researchers, the authors have developed a template with seven views, that can be used in developing trustworthy and privacy enabled information system for next generation pHealth (Table 2). For each view, actions and tentative solutions are also shown. While the representation of an ideal system meeting all the aforementioned requirements has been developed by the authors and meanwhile standardized as ISO 23903 [52] as well as in related security and privacy standards such as ISO 22600 [53], ISO 21298 [54], or HL7 Privacy and Security Logical Data Model – Release 1 [55], the establishment and enforcement of the related governance is still an open issue.

Because ethics is the cornerstone of information privacy and privacy laws, it should be the starting point for the template. Ethics tries to explain what is good or bad behaviour in a situation. The authors proposed for future pHealth the use of a combination of consequentialism that is focused to consequences to a person caused by the collection, use and disclosure of PHI, and utilitarianism that means that PHI should available to improve population's health [7].

To be successful, future pHealth seems to require new legislation. The authors propose that the ownership of PHI, information and personal health behaviours must be defined unambiguously at the level of law. Furthermore, the authors state, that a person should be the owner of his or her PHI. All stakeholders in pHealth (e.g., service providers, data collectors and users) should have legal duty to publish reliable information concerning their privacy and trust features and behaviours, as well as privacy and trust features of their information systems. It is also necessary to strengthen the position of a person in such a way that it can always be aware of what, how and by whom PHI is collected and used.

Table 2 Privacy and trust views and solutions for future pHealth

View	Details	Proposed Action	Possible solution
Concepts	Ethics, privacy and trust model	Analysis of ethical principles, privacy policies and trust promises used by participating stakeholders (e.g., in Business models)	-Consequentialism -Privacy as personal property -Trust as fiducial duty -Computational privacy
	Consequences of the use of PHI	Analysis of consequences of data collection to the DS	
Environment	Laws, standards, golden rules	-Regulatory analysis - Creation of new laws	-Law to force service providers and IS developers to publish their privacy and trust features

			- Law to strengthening the role of a person -Law to restrict hidden collection of PHI
Stakeholders	Business and privacy policy Privacy and trust features	Policy analysis	Disclosure of stakeholder's privacy and trust features in standardized form
Information system	-IS Architecture Privacy and trust challenges information systems -PHI retention	-Selection of suitable architecture -Regulatory compliance analyses -Analysis of security and privacy risks	-Edge computing -Blockchain architecture -Federated computing -Communication privacy by encryption -Privacy and trust agents
Service or application	-Design methods -Privacy and trust tools	-Use of privacy as default method -Implementing of privacy and trust services	-Access limitation (attribute-based access control), audit trails data minimization and filtering, adding noise to data -Data vanish method -Notification to the DS of PHI collection -Federated data analysis -Federated learning
DS (in the role of service user)	-Person's position and power -Person's privacy needs -Reason to trust -Benefit and harm -Level of privacy and trust	-Creating own privacy policy -Collect privacy and trust attributes -Decision why to trust	-Service/application to -measure level of privacy and trust - Calculate the actual level of privacy and trust - Make a Smart contract
Data and sensors	-Integrity and reliability of sensors and data -Privacy management	Point-to-point raw data encryption at sensor level	Lite encryption methods

The person should be also be aware and informed of personal behavioural data collected in public places and hidden by applications. Furthermore, a person as the owner of PHI should have tools to define own privacy policies and rules. Here, the aforementioned standards could come into play. Organizations offering "free of charge pHealth applications", which collect PHI and behavioural data, should also have the responsibility to offer similar paid application without health data and behavioural tracking.

Federated learning (FL) is a learning model that tries to address the problem of data governance and privacy by enabling ML from non-co-located data. ML offers a way to preserve user's privacy by decentralizing data from the central server to end-devices [56]. In an FL solution, the data controller not only defines its own privacy policies, but also controls data access and has the ability to revoke it [57]. Those features make FL a good tool for future pHealth. It is also necessary that pHealth applications (especially AI, ML and DL applications) support the principle of forgetting and enable data erasure. Encryption as default principle should be used everywhere where it is possible (e.g., homomorphic encryption or differential privacy). The authors state, architectural

solutions such as Blockchain-based information systems, Edge architecture and Federated Learning offer and strong encryption offer increased privacy compared to in today widely used Cloud based solutions, and therefore they are proposed to be used in future pHealth.

4. Discussion

Researchers have shown that, despite information privacy and high level of trust are prerequisites for successful pHealth, current privacy approaches and solutions do not offer acceptable level of privacy, so trust is just an illusion. This means that current privacy models and technology used cannot be moved to the future pHealth. According to the authors, to make future pHealth trusted and supporting privacy, a holistic system view is needed. In this paper, the authors have presented a seven-view privacy and trust template, and new privacy and trust concepts, architectural and technological solutions for future pHealth.

The authors state that without adapting new ways to understand privacy and trust, and creating new laws, which strengthen the position of a person, it is almost impossible to guarantee privacy and trustworthiness in future pHealth. The authors see, that current laws such as the EU-GDPR, that rely on privacy as notice and choice concept (aka consent) as well as on privacy risk analysis will no work in future environment [58-60]. Furthermore, according to Kerasidou et al., until today, policy-makers and technology developers have failed to provide people reasons to trust and left users of digital networks and services vulnerable. People are simply expected to blindly trust in companies' fairness and promises [61]. Thinking the future, the worst solution is only to wait for new laws and regulations, fair industrial self-regulation, and global harmonization of ways privacy and trust are understood. Instead, developers of next generation pHealth information systems, applications and services should create a holistic view on the system of systems based on a system-theoretical, context-aware, architecture-centred, ontology-based and policy-driven approach as standardized in ISO 23903, start to use the privacy and trust as default principle, and privacy and trust approaches and solution discussed in this paper.

References

[1] Codagnone C. Reconstruction the Whole: Present and Future of Personal Health Systems, PHS 2020, 2009, images/stories/pdf/phs2020-book-rev16082009.pdf.

[2] Rose C. Ubiquitous Smartphones, Zero Privacy, Review of Business Information Systems – Fourth Quarter 2012 Volume 16, Number 4.

[3] Wei Z, Zhao B, Su J. PDA: A Novel Privacy-Preserving Robust Data Aggregation Scheme in People Centric Sensing System, International Journal of Distributed Sensor Networks, Volume 2013, Article ID 147839, 9 pages, Hindawi Publishing Corporation, http://dx.doi.org/10.1155 /2013/147839.

[4] Trifan A, Oliveira M, Oliveira JH. Passive Sensing of Health Outcomes Through Smartphones: Systematic Review of Current Solutions and Possible Limitations, JMIR Mhealth Uhealth 2019; 7(8): e12649) doi: 10.2196/12649.

[5] DeSmet A, De Bourdeaudhuij I, Chastin S, Crombez G, Maddison R, Gardon G. Adults' Preferences for Behavior Change Techniques and Engagement Features in a Mobile App to Promote 24-Hour Movement Behaviors: Cross-Sectional Survey Study, JMIR Mhealth Uhealth 2019; 7(12): e15707) doi: 10.2196/15707.

[6] Rose C. Ubiquitous smartphones, Zero Privacy. Rev Bus Inf Syst. 2012; 16: 187–92. doi: 10.19030/rbis.V16i4.7438.
[7] Ruotsalainen P, Blobel B. Health Information Systems in the Digital Health Ecosystem—Problems and Solutions for Ethics, Trust and Privacy, Int. J. Environ. Res. Public Health 2020; 17(9): 3006; doi:10.3390/ijerph17093006.
[8] Gupta P, Akshat Dubey A. E-Commerce-Study of Privacy, Trust and Security from Consumer's Perspective. Int. J. Comput. Sci. Mob. Comput. 2016; 5: 224–232.
[9] Solove DJ. The End of Privacy?, Scientific American October 2008, DOI: 10.1038/ scientificamerican 0908-100.
[10] Rubinstein IS. Big Data: The End of Privacy or a New Beginning? International Data Privacy Law. 2013; 3(2), Oxford University Press.
[11] Ruotsalainen P, Blobel B. Privacy s Dead – Solutions for Privacy-Enabled Collections and Use of Personal Health Information in Digital Era. Stud Health Technol Inform. 2020; 273: 63-74. doi:10.3233/SHTI200616.
[12] Taviani HT, Moor JM. Privacy Protection, Control of Information, and Privacy-Enhancing Technologies. ACM SIGCAS Comput. Soc. 2001; 31: 6–11.
[13] McKnight DH, Choudhury V, Kacmar C. Developing and Validating Trust Measures for e-Commerce: An Integrative Typology, In: Davis GB (Ed.), The Blackwell Encyclopedia of Management. Vol. 7 Management Information Systems, Malden, MA: Blackwell, pp. 329-331.
[14] Ruotsalainen P, Blobel B. How a Service User Knows the Level of How a Service User Knows the Level of Privacy and to Whom Trust in pHealth Systems? Stud. Health Technol. Inf. 2021; 285: 39–48.
[15] Rubenfield J. The End of Privacy. Stanford Law Review. Oct. 2008; 61(1): 101-162.
[16] Sharma S, Chen K, Sheth A. Towards Practical Privacy-Preserving Analytics for IoT and Cloud-Based Healthcare Systems, IEEE Internet Computing January 2018; DOI: 10.1109/MIC.2018.112102519.
[17] Raghupathi W, Raghupathi V. Big data analytics in healthcare: Promise and potential. Health Inf Sci Syst. Febr. 2014; 2: 3.
[18] Cabrera ME, Bhattacharjee T, Dey K, Cakmak M. An Exploration of Accessible Remote Tele-operation for Assistive Mobile Manipulators in the Home, 2021 30th IEEE International Conference on Robot & Human Interactive Communication (RO-MAN), 978-1-6654-0492-1/21, 2021 IEEE, DOI: 10.1109/RO-MAN50785.2021.9515511.
[19] Joinson A, Houghton DJ, Vasalou A, Marder BL. Digital Crowding: Privacy, Self-Disclosure, and Technology. In Privacy Online; Springer Science and Business Media LLC: Berlin, Germany, 2011; pp. 33–45
[20] WHO Universal Declaration of Human Rights, http://www.un.who.org/en/universal-declaration-human-rig.
[21] Marguilis ST. Privacy as a Social Issue and Behavioral Concept. J. Soc. Issues 2003; 59: 243–261.
[22] Waldman AE. Privacy as Trust. Cambridge University Press, ISBN 978-1-316-63694-7, DOI:10.1017/978136888667, United Kingdom 2018.
[23] Smith H.J, Dinev T, Xu H. Information privacy research: An interdisciplinary review. MIS Q. 2011; 35: 989–1015.
[24] Zwick D. Models of Privacy in the Digital Age: Implications for Marketing and E-Commerce; University of Rhode Island: Kingston, RI, USA, 1999; https://www.researchgate.net/profile/ Nikhilesh-Dholakia/publication/ 236784823_ Models_ of_privacy_in_the_digital_age_Implications _for_ marketing_and_e-commerce/links/0a85e5348ac5589862000000/Modelsof-privacy-in-the-digital-age-Implications-for-marketing-and-e-commerce.pdf?origin=publication_detail.
[25] Bhatia J, Breaux TD. Empirical Measurement of Perceived Privacy Risk. ACM Trans. Comput.-Hum. Interact. 2018; 25: 1–47.
[26] Dinev T, Xu H, Smith JH, Hart P. Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. Eur. J. Inf. Syst. 2013; 22: 295–316.
[27] Dobkin A. Information fiduciaries in Practice: data privacy and user expectations, BERKELEY TECHNOLOGY LAW JOURNAL 2018 Vol. 33:1; DOI: https://doi.org/10.15779/Z38G44HQ8.
[28] Zuboff S. The Age of Surveillance Capitalism, Public Affairs, ISBN 9781781256855.
[29] Ruotsalainen P and Blobel B. Transformed Health Ecosystems Challenges for Security, Privacy, and Trust. Front. Med. 2022; 9:827253. doi:10.3389/fmed.2022.827253.
[30] Ruotsalainen P, Blobel B, Pohjolainen S. Privacy and Trust in eHealth: A Fuzzy Linguistic Solution for Calculating the Merit of Service. J. Pers. Med. 2022; 12: 657. https:// doi.org/10.3390/jpm12050657.
[31] Beldad A, de Jong M, Steehouder M. How shall I trust the faceless and the intangible? A literature review on the antecedents of online trust. Comput. Hum. Behav. 2010; 26(5): 857–869, DOI:10.1016/j.chb.2010.03.013.
[32] McKnight DH. Trust in Information Technology. In: Davis GB (Ed.). The Blackwell Encyclopedia of Management 2005, Vol. 7 Management Information Systems, Malden, MA: Blackwell, pp. 329-331.

[33] Richards N, Hartzog W. Taking Trust Seriously in Privacy Law. Stanf. Tech. Law Rev. 2016; 19: 431.
[34] Huckvale K, Prieto JT, Tilney M, Benghozi P-J, Car J. Unaddressed privacy risks in accredited health and wellness apps: A cross-sectional systematic assessment. BMC Med. 2015; 13: 214.
[35] Papageorgiou A, Strigkos M, Politou E, Alepis E, Solanas A, Patsakis C. Security and Privacy Analysis of Mobile Health Applications: The Alarming State of Practice. IEEE Access 2018; 6: 9390–9403.
[36] Ruotsalainen P, Blobel B. Trust—Essential Requirement and Basis for pHealth Services. Stud Health Technol Inform. 2017; 237: 25–33.
[37] O'Connor Y, Rowan W, Lynch L, Heavin C. Privacy by Design: Informed Consent and Internet of Things for Smart Health. Procedia Comput. Sci. 2017; 113: 653–658.
[38] Al-Rubaie M, Chang JM. Privacy Preserving Machine Learning: Threats and Solutions, IEEE Security and Privacy Magazine 2018; 17(2): 49-58.
[39] Balkin JM. Information Fiduciaries and the First Amendment, UC Davis Law Review, April 2016; 49(4).
[40] Barrett L. Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries. Seattle University Law Review 2019; 42(1): 1057-1113.
[41] Mayer RC, Davis JH, Schoorman FD. An Integrative Model of Organizational Trust. Acad. Manag. Rev. 1995; 20: 709–734. Available online: http://www.jstor.org/stable/258792.137-154.
[42] Ritter J, Mayer A. Regulating Data as Property: A New Construct for Moving Forward. Duke Law Technol. Rev. 2018, 16, 220–277. Available online: https://scholarship. law.duke. edu/dltr/ vol16/iss1/7].
[43] Samuelson P. Privacy As Intellectual Property? Stanford Law Review, November 2000; 52(5). DOI:10.2307/1229511.
[44] Li M, Yu S, Zheng Y, Ren K, Lou W. Scalable and Secure Sharing of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. IEEE Transactions on Parallel and Distributed Systems, January 2013; 24(1): 131-143.
[45] Yue X, Wang H, Jin D, Li M, Jiang W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control, Journal of Medical Systems 2016; Volume 40, Article number 218.
[46] Gursels S. Privacy and Security Can you engineer privacy? Communications of the ACM, August 2014, VOL. 57, No.8.
[47] Ruotsalainen P, Blobel B. Digital pHealth – Problems and Solutions for Ethics Trust and Privacy. Stud Health Technol Inform. 2019; 261: 31-46. doi:10.3233/978-1-61499- 975-1-31
[48] Uriarte RB, Zhou H, Kritikos K, Shi Z, Zhao Z, De Nicola R. Distributed service-level agreement management with smart contracts and blockchain. Concurrency Computat Pract Exper. 2020;e5800, https://doi.org/10.1002/cpe.5800
[49] Rosic A. What is Blockchain Technology? A Step-byStep Guide for Beginners. Journal of Chemical Information and Modeling, 2013, https:// blockgeeks.com/guides/what-is-blockchain-technology.
[50] Cao X, Tang G, Guo D, Li Y, Zhang W. Edge Federation: Towards an Integrated Service Provisioning Model. IEEE/ACM Transactions on Networking 2020; 28(3): 1116-1129. arXiv:1902.09055v3 [cs.NI] , https://doi.org/10.48550/asZiv.1902.09055.
[51] Lopez GP, Montresor A, Epema D, Datta A, Higashino T, Iamniychi A, Barcellos M, Felber P, Riviere E. Edge-centric computing: Vision and Challenges. ACM SIGCOMM Computer Communication Review 37 October 2015; 45(5): 1116-1129.
[52] International Organisation for Standardisation. ISO 23903:2021 Health informatics – Interoperability and integration reference architecture – Model and framework. ISO: Geneva; 2021.
[53] International Organisation for Standardisation. ISO 22600:2014 Health informatics – Privilege management and access control (Part1-3). ISO: Geneva; 2014.
[54] International Organisation for Standardisation. ISO 21298:2017 Health informatics – Functional and structural roles. ISO: Geneva; 2017.
[55] HL7 International. ANSI/HL7 Privacy and Security Logical Data Model, Release 1. HL7: Ann Arbor; 2021.
[56] Mothukuri V, Parizi RM, Pouriyeh S, Huang Y, Dehghantanha A, Srivastava G. A survey on security and privacy of federated learning Future Generation Computer Systems, February 2021; 115: 619-640, https://doi.org/10.1016/j.future.2020.10.007 0167-739X].
[57] Rieke et al, The future of digital health with federated learning. Digital Medicine 2020; 3: 119; https://doi.org/10.1038/s41746-020-00323-1.
[58] EU-GDPR. Available online: htpps://eur-lex.europa.eu/legal-content/EN/TXT/?uri= CELEX%3A02016R0679-2016950&qid=1532348683434
[59] Gerber N, Reinheimer B, Volkamer M. Investigating People's Privacy Risk Perception. Proc. Priv. Enhancing Technol. 2019; 3: 267–288.
[60] Mitchell VM. Consumer perceived risk: Conceptualizations and models. Eur. J. Mark. 1999; 33: 163–195.

[61] Kerasidou CX, Kerasidou A, Buscher M, Wilkinson S. Before and beyond trust: reliance in medical AI, . Journal of Medical Ethics Published Online First: 23 August 2021. doi: 10.1136/medethics-2020-107095