Developing a Privacy Compliance Scale for IoT Health Applications

Kavenesh Thinakaran, Jaspaljeet Singh Dhillon*, Saraswathy Shamini Gunasekaran, Lim Fung Chen

College of Computer Science and Information Technology, Universiti Tenaga Nasional, Malaysia

Copyright©2018 by authors, all rights reserved. Authors agree that this article remains permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

Abstract Internet of things (IoT) is intensely gaining popularity in the healthcare industry. Though these systems are ubiquitous, pervasive and seamless, an issue concerning consumers' privacy remains debatable. There is an immaculate rise in terms of awareness amongst patients where data privacy is concerned. IoT-based health applications are more prone to privacy risks, and hence general privacy guidelines for health applications, in general, are not adequate. Often, privacy is oversights, causing consumers to lose interest from using an application continuously. In this paper, we propose a compliance scale modelling the privacy principles for privacy-aware novel IoT-based health applications. We have conducted an analytical review of privacy guidelines to derive at the essential principles required to develop and measure privacy-aware IoT health applications after discarding irrelevant principles, extracting repeating core principles, and merging relevant principles. A quantitative survey was deployed to empirically evaluate the proposed scale to finalize the principles based on their significance. The proposed compliance scale presents essential privacy principles to adhere in the development of novel IoT health applications. The proposed compliance scale would be significant for policymakers and applications developers to measure, better understand and respect the privacy principles of consumers towards novel IoT-based health applications.

Keywords Internet of Things, Privacy Framework, Requirements, Healthcare Applications

1. Introduction

Privacy can be conceptualised as the right to be left alone. It refers to the process of disclosing and mobilising one's personal data under certain conditions and safeguarding measures [1]. The distinction or overlap between 'privacy' and 'security' are subtle. While 'privacy' indicates freedom from unauthorised intrusion, 'security'

alludes to procedures or measures taken to ensure the safeguarding of privacy.

Privacy is a prominent issue for consumers in a globally connected network society [2]. The concern towards privacy risks is escalating as we are moving forward into a ubiquitous world, where more innovative self-care applications are being developed using a prominent technology widely known as the Internet of Things (IoT).

IoT is a convergence of smart devices that generate data through sensors to create new information and knowledge to boost human intelligence, efficiency and productivity to enhance the quality of life. It is a highly distributed and ubiquitous network of seamlessly connected heterogeneous devices integrated with the existing Internet and mobile networks. IoT paves the development of new intelligent health services which is made available anytime, anywhere, by anyone and anything. Healthcare is one of the most attractive applications for IoT [4] because it is designed to improve the efficiency, effectiveness, quality and cost of healthcare by enabling physicians to remotely monitor their patients as well as letting individuals manage their health at ease [5].

Unlike typical health applications that offer health-related services via smartphones and tablets, IoT-based health applications involve a collection of health tools and medical devices which require Internet connectivity [5]. They encompass a broad range of applications that provide health care services such as remote health monitoring, fitness programs, elderly care, electronic patient records, telemedicine, surgical simulations and so much more. The devices associated with this application often are wearable technology devices. Some other examples include headsets that measure brainwaves, clothes with sensing devices, BP monitors, glucose monitors, ECG monitors, pulse oximeters, sensors embedded in medical equipment, dispensing systems, surgical robots and device implants. Figure 1 illustrates an example of how IoT enables remote healthcare, in which health data of patients are transmitted to healthcare providers via wireless telecommunication devices for monitoring and treatment purposes. In a nutshell, these

applications have great potential for advance personalised connected healthcare, some of which has never been imagined before but are nevertheless possible via integration of diverse technologies. However, these applications are prone to unknown risks and issues.

Figure 1. Remote healthcare enabled via IoT (from [3])

Despite the benefits of leveraging IoT-based health applications, there are many challenges associated with its implementation. As an example, health data collected rapidly from various sources may significantly impact consumer's privacy. It may lead to potential widespread surveillance of individuals without their consent or knowledge [6]. In June 2015, a substantial privacy-violation attack occurred when malware comprising blood gas analysers gained access into hospital networks and in the process stole confidential data [7]. Apart from this, the open and interconnected environment of IoT supports the exchange of sensitive data like mental health, genetics, reproductive care and substance which are prone to privacy risks abuse. Furthermore, all online and offline activities are recorded and stored forever which may be prone to identity threats, location threats and data eavesdropping [8]. This raises concerns as to who will have access to this information and under what terms, conditions, and whether the public will be subjected to serious privacy infringement [9]. Recent breaches of health information underscore that the risks are real. In a 2006 study, when Americans were given some information about the advantages of and worries about online health information, 53% of them were worried about insurers gaining access to this health information, 56% were fretful about employers having access to their health information, 77% reported being very concerned about their health information being utilized for marketing tenacities whereas 80% of them stated that they are very concerned about identity theft or fraud [10]. Based on a recent poll conducted, one in six adults (17%) whom represents 38 million individuals confessed that they suppress their respective health information from their health providers due to concerns on how the medical data might be disclosed [11]. Therefore, adequate privacy guidelines must be incorporated from the outset in the design process of the health application itself.

Since IoT health applications are still in the early age of development, this is the critical window to be addressing

privacy requirements for IoT health-based applications. In a nutshell, the existing privacy scales and guidelines for health information is not comprehensive, consistent or sufficient. Eventually, this portrays a strong case on why is our study important. There are guidelines available for developers to design applications to safeguard the privacy aspects of consumers. Likewise, there are also the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health Act (HITECH) to enforce the privacy and protection of health information of consumers [12]. However, most of the guidelines available provide general privacy principles which may be insufficient to design novel IoT applications that deal with sensitive health information. We argue that IoT-based health applications are more susceptible to privacy risks and hence privacy guidelines for health applications in general are inadequate. Moreover, it is apparent that privacy is often overlooked, causing consumers to lose interest from using an application continuously. The emphasis of most research efforts is in the design of security guidelines or the combination of both the privacy and security frameworks. Hence, the prominent objective of this paper is to develop a privacy compliance scale to assist in the design of the IoT-based health applications. We have critically reviewed several privacy guidelines to identify the relevant principles to include in the scale. A quantitative survey was deployed to empirically evaluate the proposed scale to finalise the principles based on their significance.

2. Methodology

This study was prominently built upon two approaches: an analytical review and a quantitative survey. The first approach is constructed based on the primary two objectives, which are: (1) to identify the privacy requirements for IoT-based health application and (2) to develop a scale modelling the privacy requirements for IoT-based health applications. Therefore, we reviewed the literature focusing on privacy requirements in the context of IoT health applications and formulated the scale after discarding irrelevant principles, extracting repeating core principles, and merging relevant principles.

Well established models like the U.S. Office of National Coordinator (ONC) framework were the theoretical basis for the scale development. Addition to that, the second approach, a quantitative survey was deployed to empirically evaluate the proposed model to finalise the factors based on their significance. However, since there were inadequate studies with regards to privacy requirements of IoT-based health applications, the survey had to be built from scratch based on existing privacy guidelines. Thus, we conducted an expert review with total four experts two of them from the medical whereas another two from education field to ensure that statements included in the questionnaire were clear, comprehensible and mainly

interpreted correctly by the respondents. Expert reviews have “value in identifying question problems that result in lower survey data quality” [13]. The expert’s comments and feedback were used to improve the survey.

The survey was administered for a month between January and February 2017. Along with the questionnaire, we attached a small write up about IoT health applications pertaining definitions and examples. Quantitative research emphasises on collecting numerical data to explain a particular question. A one to five rating scale was used a measure in the survey. Data was collected via an online survey that was developed using Survey Monkey. However, we also prepared a printed version to be distributed. Altogether we had 140 respondents for the study. However, only 128 responses were extracted and found useful the rest 12 were discarded due to skipped sections and irrelevant answers. Below is the online survey link which was distributed to potential respondents: <https://www.surveymonkey.com/r/kaveneshweb>. A copy of the questionnaire is attached in the appendix of this paper as well. Data analysis for this study was conducted via SPSS version 19. Descriptive analysis was performed to determine the demographic information of the respondents along together with descriptive information. Descriptive statistics are useful describe the basic features of the data and they provide simple summaries about the sample and the measures. Reliability test like Cronbach’s Alpha was also undertaken to assess the internal consistency of the questionnaire items. Cronbach’s alpha helps to determine if the test one has designed is accurately measuring the variable of interest [14]. Furthermore, Kaiser–Meyer–Olkin (KMO) and Bartlett’s Test was also conducted to determine the convenience in performing factor analysis. KMO & Bartlett’s test is a measure of sampling adequacy that is recommended to check the case to variable ratio for the analysis being conducted [15]. Last but not least, Exploratory Factor Analysis (EFA) was done to identify the underlying dimensions of privacy requirements. EFA helps summarize data regroup variables into a limited set of clusters based on shared variance so that relationships and patterns can be easily interpreted and understood [16]. Figure 2 below depicts a graphical representation of the approaches utilised in conducting the research.

3. Existing Privacy Guidelines

Identification of privacy requirements for IoT-based health applications is vital for developers to understand the expectations of consumers in ensuring confident and sustainable use of novel IoT applications. In this section, we review existing solutions that were aimed at preserving privacy in several areas. These solutions are presented in a chronological manner. Table 1 summarises privacy principles that are included in existing guidelines.

Aivaloglou, Gritzalis & Skianis [17] reported a set of requirements to design privacy-aware sensor networks.

The proposed Guideline was derived based on the understanding built upon privacy requirements and challenges in preserving privacy. This guideline presents five principles with an emphasis on sensor networks, which is the backbone to develop ubiquitous IoT-based solutions that are known to impose greater privacy risks.

In May 2008, the Center for Democracy & Technology released a comprehensive privacy and security framework to support the protection of health data [18]. This framework is a revised version of the framework that was released by the Markle Foundation in the project Connecting for Health [10]. The framework contains nine principles that are based on a mix of legislative action, regulation and industry commitment.

Figure 2. Research Design Process

A comprehensive framework governing the electronic exchange of individually identifiable health information was introduced by ONC for Health Information Technology [19]. In the development process of this ONC framework, various international, national, public, private sector and security principles were reviewed. A careful review and analysis of these principles were conducted by accommodating as much variation as possible keeping well in mind at the same time as to how they apply to electronic data. The ONC framework covers eight principles that serve as a guideline for public and private sector entities that hold or exchange electronic individual health-related data and help to guide the Nation’s adoption of health information technologies.

In the year 2014, Alqassem and Svetinovic [20] released

a taxonomy on security and privacy requirements for the IoT. The taxonomy presented quality attributes applied in an IoT smart grid scenario. The document provides support for more investigation of expected privacy and security vulnerabilities and threats about IoT. The presented four principles mainly cover the security aspects of IoT.

In recent times, AL-mawee [8] reported a survey on security and privacy issues in IoT healthcare applications in the context of disabled users. It presents a wide range of IoT based applications for the disabled. These presentations identified the respective security and privacy issues for the applications. Furthermore, the main solutions to these applications were discussed at length and prominent privacy and security requirements for the disabled were defined as well. This study presented a

guideline consisting of seven principles.

Recently, Porambage et al. [21] reported design guidelines for preserving privacy in IoT in general. The guidelines presented are applicable to govern privacy issues and concerns of different industries specifically for healthcare, smart homes, public safety and supply management. It provides insight into privacy requirements that should be integrated into the development of privacy guidelines, in our context, IoT-based health applications. The guidelines developed are based on examining the complementary pieces of technology or application-specific privacy guidelines and the IoT network attributes such as the technological aspects and legal regulations. It provides nine characteristics to be included when deploying an IoT privacy guideline.

Table 1. A Summary of Privacy Principles included in Existing Frameworks.

Guideline Code	G1	G2	G3	G4	G5	G6
Author	[17]	[18]	[19]	[20]	[8]	[21]
Objective of the guideline	To identify the requirements for privacy preserving sensor networks	To generate a comprehensive privacy and security guideline for e-health efforts	To establish a privacy framework for electronic health information exchange	To present a taxonomy on security and privacy requirements for IoT	To identify privacy requirements for IoT health based applications for the disabled	To develop a holistic privacy guideline for IoT
For IoT?	Yes	No	No	Yes	Yes	Yes
Privacy principles included	Data confidentiality, Protecting the communication's context User anonymity Ensuring data authenticity and integrity User data disclosure	Openness and transparency Purpose specification and minimization Collection limitation Use limitation Individual participation and control Data integrity and quality Security safeguards and controls Accountability and oversight Remedies	Individual access Correction Openness and transparency Individuals choice Collection, use and disclosure limitation Data quality and integrity Safeguards Accountability	Access control Data integrity Contextual Integrity Intrusion detection	Data ownership Disabled's permission for access to her data Disabled anonymity and pseudonymity Location privacy Maximizing locality of information Privacy provided devices Empathizing on privacy for application design	Openness, transparency and purpose specification Identify privacy Temporal and location privacy Query privacy Access control Interoperability Data minimization Accountability Security

4. Findings & Discussion

This study proposes a compliance scale modelling the privacy requirements for IoT-based health applications. Compliance scales presented in the preceding section are critically reviewed with respect to their suitability to aid the development of privacy-aware IoT-based health applications. The principles were evaluated using a list of pre-defined criteria. After that, essential privacy principles to govern for IoT-based health applications were derived. The following list describes the criteria used to gauge suitability of the existing guidelines for privacy-aware IoT health applications: (1) generalizability: to what extent is the guideline applicable to IoT-based health applications in general?, (2) ambiguity: is there any principle(s) that is ambiguous or similar but segmented into two different principles?, (3) relevance: are the principles relevant for IoT-based healthcare applications?, and (4) completeness: are the principles adequate to cater for IoT-based healthcare applications?

Our analysis of existing privacy guidelines reveals essential principles to adhere in an ideal privacy-aware application. Guidelines presented above are aimed at preserving privacy in specific areas. Out of the six the guidelines analyzed, four are related to IoT (i.e. G1, G4, G5 and G6), whereas G2 and G3 focus on preserving privacy in health data in general. Based on our review, there has not been much work done in the area of safeguarding privacy in IoT, and to the best of our knowledge, ours is the first study whose primary focus is on IoT-based health applications.

Results presented in Table 2 indicate that the guidelines reviewed in this paper are useful for their respective purposes, but isn't sufficient if they are to be used to govern IoT health applications. Based on the review, each of the reviewed guidelines has its strengths and limitations with regards to its suitability to govern privacy aspects of IoT health applications. However, G2, G3 and G6 require minimum modification if applied in our context. We also took notice that none of the above guidelines covers life-span of the collected data. The duration of storing health data might post a privacy concern. The data subjects should be informed about the period of storage of their data by the data users, and it is also the right of the data subjects to aware of the time of disposal of their health data.

Table 2. Guideline Evaluation Results

	G1	G2	G3	G4	G5	G6
Generalizability	x	√	√	√	x	√
Ambiguity	x	x	x	√	√	√
Relevance	√	√	√	x	√	x
Completeness	√	√	√	x	√	√

Table 3 illustrates the proposed privacy compliance scale. The included principles were carefully examined and incorporated from the guidelines above.

Table 3. Proposed Privacy Compliance Scale

Principle	Definition
<i>Access control</i>	Consumer health related information should only be accessible by authorized personnel. Limited access to consumer's health related information should be ensured.
<i>Anonymity</i>	The identity of the consumers using IoT-based health applications, device and system needs to be protected. Unlinkability must be ensured between the consumers and their health related data respectively. Identification and tracking of consumers should be impossible. Indistinguishability among consumers should be achieved
<i>Consent</i>	Before the collection of health related data, the consumer needs to be acknowledged on the details being collected. Clinicians or third parties may access the information only via the consent of the consumer. Data subject's consent is also needed for the duration of storing and disposal of the collected health data.
<i>Data disclosure</i>	Health consumer needs to be notified and aware of with whom his/her health data is being shared with. Once the user has clearly understood via a short notice with whom the data will be disclosed, then the collection process may take place. Consumer needs to be empowered whether to share his/her health related information to third parties or other entities.
<i>Data minimization</i>	The collection and storage of consumer's health data should be minimized to which that information is necessary to perform a service.
<i>Openness and transparency</i>	Consumers not only need to know the use of their health data but the manner of collection as well. The personnel who has access to it and where it resides should also be made loud and clear.
<i>Purpose specifications</i>	The purpose why the health data is being collected needs to be specified at the time of collection. The usage of data should be limited to that particular purpose stated in the beginning and if there is further use of it, the user should be notified from time to time.
<i>Safeguard and remedies</i>	Consumer's health data should be protected against risks for example unauthorized access, destruction, and etc. In the event it happens. The consumer should be notified regarding the breach and violation.
<i>Data life-span</i>	The duration of storing the health data collected. After the prescription, for how long the health data can be kept by the data user. If the health care data is no longer needed, it should be disposed of with the data subject's consent. If the data is required for further prescription, then the data subject's consent is needed for the extension of data storing duration.

The quantitative study that was conducted to evaluate the scale was conducted with a sample consisting of 128 respondents from diverse backgrounds (mean age 26, SD = 8.22). Table 4 represents the demographic information of the respondents.

Table 4. Descriptive Information of the Respondents

Characteristics	n	%
Gender		
Male	69	51.56
Female	59	44.84
Highest Level of Education		
Primary	1	0.8
Secondary	2	1.6
Tertiary	125	97.7
Computer Skill Level		
Expert	17	12.5
Advanced	54	42.2
Intermediate	55	42.5
Novice	2	3.1
Medication taken by respondents		
Yes	95.3	122
No	4.7	6
Experience of Respondents using Health Application		
Yes	67	52.3
No	61	47.7
Frequency of Respondents Usage of Health Application		
5 days a week or more	2	1.6
1 - 4 days/ week	15	11.7
1 - 3 times a month	37	28.9
Less often than once a month	20	15.6
Never	54	42.2
Heard about Internet of Things		
Yes	72	56.3
No	56	43.8

The following section depicts the descriptive statistics on the variable of the study. Based on Table 4, the statistic interpretation is conducted which are adopted from Klein [22], and Table 5 reveals the overall mean score value and its respective status.

Table 4. Descriptive Statistics of the Variables

Mean Score	Interpretation
1.00 – 1.80	Strongly Disagree (SD)
1.81 – 2.60	Disagree (D)
2.61 – 3.40	Moderate Agree (MA)
3.41 – 4.20	Agree (A)
4.21 – 5.00	Strongly Agree (SA)

Table 5. Descriptive Statistics of the Variables

Dimensions	Overall mean score value	Overall mean status
Access Control	4.26	SA
Anonymity	4.23	SA
Consent	4.27	SA
Data Disclosure	4.28	SA
Data Minimization	4.24	SA
Openness and Transparency	4.29	SA
Purpose of Specifications	4.28	SA
Safeguard and Remedies	4.28	SA
Data Life Span	4.20	A

In summary, based on the analysis of the questionnaire, eight dimensions with three items respectively each tend to produce an overall mean status of 4.21 and above which depicts *Strongly Agree* except for the last dimension, *Data Life-Span*, with an overall mean of 4.20 which resulted in *Agree*.

Cronbach's alpha was utilised to measure internal consistencies especially when you have multiple Likert questions in a questionnaire that form a scale to determine whether the scale is reliable [23]. Therefore, Cronbach's Alpha test is conducted to confirm the validity of the questions prepared for a study. The Table 6 below illustrates the range of reliability of the Cronbach's Alpha.

Table 6. Mean Score for Reliability range of Cronbach's Alpha.

Cronbach's Alpha	Internal Consistency
$0.9 \leq \alpha < 0.8$	Excellent
$0.7 \leq \alpha < 0.8$	Good
$0.6 \leq \alpha < 0.7$	Acceptable
$0.5 \leq \alpha < 0.6$	Poor
$\alpha < 0.5$	Unacceptable

However, a higher coefficient does not always mean the degree of reliability is higher because the alpha is pretentious by the length of the test. For instance, in our study the length is short, therefore leaving the value of alpha small [22]. Therefore, if all the 27 items are combined as shown in Table 7 the degree of the alpha value increase compared to analyzing items per factor.

Table 7. Cronbach's Alpha

Dimensions	Number of Items	Cronbach's Alpha	Status
Access Control	3	0.702	Good
Anonymity	3	0.784	Good
Consent	3	0.754	Good
Data disclosure	3	0.800	Excellent
Data minimization	3	0.797	Good
Openness and Transparency	3	0.802	Excellent
Purpose of Specifications	3	0.788	Good
Safeguard and Remedies	3	0.828	Excellent
Data life-span	3	0.748	Good

Therefore, all the nine dimensions produced adequate status to support all the dimensions. KMO is conducted to calculate individual and multiple variables. Besides that, it is utilised to present the ratio of the squared correlation between variables to the squared partial correlation between variables. The KMO statistic ranges between 0 and 1. A value close to 1 indicates that patterns of correlations are relatively compact and so factor analysis should yield distinct and reliable factors. Kaiser [24] recommends accepting values higher than 0.5 as barely

acceptable. Therefore, values beneath this ought to lead you to either gather more information or reexamine which factors to incorporate. Whereas values between 0.5 and 0.7 are mediocre, values between 0.7 and 0.8 are good, values between 0.8 and 0.9 are great, and values above 0.9 are superb [25]. Bartlett's test tests the null hypothesis that the original correlation matrix is an identity matrix. Therefore, values beneath 0.05 are highly significant. For these data, Bartlett's test is considered highly significant [25].

Table 8. KMO and Bartlett's Test

Kaiser-Meyer-Olkin Measure of Sampling Adequacy.		.919
Bartlett's Test of Sphericity	Approx. Chi-Square	2908.454
	df	351
	Sig.	.000

Addition to that the result for KMO and Bartlett's test

also produced adequacy of 0.919 (refer to Table 8) which is more than sufficient. Leaving that aside, EFA was conducted on 27 items related to nine dimensions to extract, merge and discard the final dimensions. Table 9 shows the developed privacy compliance scale for IoT health applications with standard labels (Strongly Disagree to Strongly Agree, ranging from 1-5) and the codes that were used in the EFA. The pattern matrix of the EFA is presented in Table 10. The common extraction method was used which is the principle component analysis with the use of promax rotation method to make the output more understandable. The results suggested that all the nine dimensions remain since they keep most of the original value. No items were removed or merged to cross relation or strong relations among each other. Therefore, the pattern matrix supports all the dimensions to be included in the final scale.

Table 9. The Privacy Compliance Scale for IOT Health Applications

Principles	Statements	Coding
<i>Access Control</i>	I would be concerned on the accessibility of my health data in the IoT health application.	AC1
	The IoT health application should not expose my health data to everyone.	AC2
	Only authorized personnel should have access to my health data in the IoT application.	AC3
<i>Anonymity</i>	It is important that my identity remain anonymous within the IoT application.	AN1
	The IoT health application should not enable non-authorized personnel to establish a link between me and by health data regarding who is described by a given dataset.	AN2
	Identification and tracking of my whereabouts should not be impossible via the IoT health application.	AN3
<i>Consent</i>	I need to be acknowledged on the details being collected via the IoT health application.	CO1
	Nobody can have access to my health data unless, provided that I have given n my consent in prior.	CO2
	My consent is needed for the duration of storing and disposal of my health related data.	CO3
<i>Data Disclosure</i>	I need to be notified and aware of with whom my health data is being shared with via the IoT health application.	DD1
	The collection process may take place once I have clearly understood via a short notice with whom the data will be disclosed.	DD2
	I need to be empowered whether to share my health data to third parties or other entities via the IoT health applications.	DD3
<i>Data Life-Span</i>	I need to know for how long the health data can be kept by the IoT-application.	DLF1
	If my health data is no longer needed, it should be disposed.	DLF2
	My health data should only be disposed with my consent.	DLF3
<i>Data Minimization</i>	The collection and storage of my health data should be minimized to perform a service in the IoT health application.	DM1
	Unnecessary collection of health or personnel data should be avoided at all times therefore only the necessary information should be extracted to perform a service in the IoT health application.	DM2
	My health data should be collected for the specified purpose and should be obtained by lawful and fair manner.	DM3
<i>Openness and Transparency</i>	I need to be clear about the usage of my health data that is captured via the IoT health application.	OT1
	I need to know the manner of collection and where my health data resides.	OT2
	I need to know who will have access to my health data.	OT3
<i>Purpose of Specifications</i>	The purpose why my health data is being collected via the IoT health application should be specified at the time of collection.	PS1
	The usage of data should be limited to the particular purpose stated at the outset.	PS2
	If my health data is going to be used for other purposes then what was indicated at the initial, I should be notified from time to time.	PS3
<i>Safeguard and Remedies</i>	My health data should be protected against all possible risks such as unauthorized access and destruction.	SR1
	My health data should be safeguarded especially in terms of storage, use and disclosure of health information.	SR2
	In the event if a breach takes place, I should be notified regarding the breach and violation soonest possible.	SR

Table 10. Pattern Matrix of Exploratory Factor Analysis

	1	2	3	4	5	6	7	8	9
AC1	.877								
AC2	.854								
AC3	.748								
AN1		.706							
AN2		.561							
AN3		.998							
CO1			.827						
CO2			.499						
CO3			.416						
DD1				.887					
DD2				.672					
DD3				.657					
DLF1					.756				
DLF2					.677				
DLF3					.823				
DM1						.850			
DM2						.349			
DM3						.301			
OT1							.727		
OT2							.686		
OT3							.729		
PS1								.415	
PS2								.557	
PS3								.636	
SR1									.697
SR2									.586
SR3									.741

The final scale (refer to Appendix) was formulated upon discarding irrelevant requirements, extracting repeating core principles, and merging relevant principles. It is anticipated that this scale will be useful for developers to better understand the privacy requirements of consumers towards novel IoT-based health applications and would enable them to develop privacy-aware IoT health applications.

5. Conclusion and Future Work

There have been inadequate studies with regards to privacy requirements of IoT-based health applications. We have studied existing privacy guidelines in deriving suitable principles that are salient to develop privacy-aware IoT-based health applications. Results indicate the *access control*, *anonymity*, *consent*, *data disclosure*, *data life-span*, *data minimization*, *openness and transparency*, *purpose of specifications*, and *safeguard and remedies* are essential principles to be respected in designing a privacy-aware

health application. The derived principles make up a scale that would be useful for policymakers and applications developers to better understand and measure the privacy requirements of consumers towards IoT-based health applications. Due to the time constraint, we did not try the scale with an actual IoT health application. However, we provided an overview on IoT health applications which was complemented with a diagram to illustrate how it works. Future research could embark on the validation of the proposed framework with an actual IoT health application.

REFERENCES

- [1] Ruback, T. (2015). Understanding the Differences between Privacy and Security Online. Retrieved from <https://www.ghostery.com/intelligence/business-blog/privacy/understanding-the-differences-between-privacy-and/>
- [2] Smith, H. J., Dinev, T. & Xu, H. (2011). Theory and Review Information Privacy Research: An Interdisciplinary Review. MIS Quarterly Information Privacy Research, 35(4), 989–1015. Retrieved from <http://pal.ist.psu.edu/MISQ.pdf>
- [3] Ianace P. (2015). Internet of Things, Remote Healthcare, One Example. Retrieved from <https://www.linkedin.com/pulse/delivering-iot-promise-one-example-pete-ianace> [accessed Aug 20 2018].
- [4] Pang, Z. (2013). “Technologies and architectures of the Internet of Things (IoT) for health and well-being” M.S. Thesis, Dept. Electron Comput. Syst., KTH-Roy. Inst. Technol., Stockholm, Sweden.
- [5] Islam, S. M. R., Kwak, D., Kabir, H., Hossain, M., & Kwak, K.-S. (2015). The Internet of Things for Health Care: A Comprehensive Survey. Access, IEEE, 3, 678–708. <http://doi.org/10.1109/ACCESS.2015.2437951>
- [6] Oriwoh, E., Sant P., & Epiphaniou, G. (2013). Guidelines for internet of things deployment approaches—the thing commandments. Procedia Computer Science, Vol 21, pp. 122–31.
- [7] Darlene Storm. (2015). MEDJACK: Hackers hijacking medical devices to create backdoors in hospital networks. Retrieved from <http://www.computerworld.com/article/2932371/cybercrime-hacking/medjack-hackers-hijacking-medical-devices-to-create-backdoors-in-hospital-networks.html>
- [8] Al-mawee, W. (2012). Privacy and Security Issues in IoT Healthcare Applications for the Disabled Users a Survey. Retrieved from http://scholarworks.wmich.edu/cgi/viewcontent.cgi?article=1661&context=masters_theses
- [9] Medaglia, C. M., & Serbanati, A. (2010). “An overview of privacy and security issues in the internet of things”, In Proc. of 20th Tyrrhenian Workshop on Digital Communications, Italy, pp. 389-395.
- [10] Markle Foundation. (2008) Common Framework for networked personal health information: Overview and

- principles. Connecting for Health. Retrieved from <https://www.markle.org/sites/default/files/CF-Consumers-Full.pdf>
- [11] American Psychological Association. (2015). Paying With Our Health. Retrieved from <https://www.apa.org/news/press/releases/stress/2014/stress-report.pdf>
- [12] Blumenthal, D. (2010). Launching HITECH, *N. Engl. J. Med.*, vol. 362, no. 5, pp. 382–385
- [13] Olson, K. (2010). An Examination of Questionnaire Evaluation by Expert Reviewers, *Field Methods*, Vol. 22, Issue 4, pp. 295 - 318.
- [14] Stephanie (2014). Cronbach's Alpha: Simple Definition, Use and Interpretation, *Statistics How To*, <http://www.statisticshowto.com/cronbachs-alpha-spss/> [accessed Aug 20 2018].
- [15] Binjrajka, R. (2012). Factor Analysis-KMO-Bartlett's Test & Rotated Component Matrix, *Business Analytics*, <http://badmforum.blogspot.com/> [Accessed Aug 20 2018].
- [16] Yong, A. G, & Pearce S. (2013). A Beginner's Guide to Factor Analysis: Focusing on Exploratory Factor Analysis. *Tutorials in Quantitative Methods for Psychology*, Vol. 9(2), pp. 79-94.
- [17] Aivaloglou, E., Gritzalis, S., & Skianis, C. (2006). Requirements and Challenges in the Design of Privacy-aware Sensor Networks. Retrieved from <http://ieeexplore.ieee.org/document/4150864/>
- [18] Center for Democracy & Technology. (2008). Comprehensive privacy and security: Critical for health information technology. White paper. Retrieved from <https://www.cdt.org/files/healthprivacy/20080514HPframe.pdf>
- [19] Office of the National Coordinator for Health Information Technology, U.S. Department of Health and Human Services. The nationwide privacy and security framework for electronic exchange of individually identifiable health information, Dec. 2008. Retrieved from <https://www.healthit.gov/sites/default/files/nationwide-ps-framework-5.pdf>
- [20] Alqassem, I. & Svetinovic D. (2014). A taxonomy of security and privacy requirements for the Internet of Things (IoT), *IEEE International Conference on Industrial Engineering and Engineering Management*, pp. 1244-1248.
- [21] Porambage, P., Ylianttila, M., Schmitt, C., Kumar, P., Gurtov, A., & Vasilakos, A. V. (2016). The Quest for Privacy in the Internet of Things. *IEEE Cloud Computing*, 3(2), 36-45. doi:10.1109/mcc.2016.28
- [22] Klein, P. G. (2008). The Make-or-Buy Decisions: Lessons from Empirical Studies. *Handbook of New Institutional Economics*, pp. 435-464
- [23] Tavakol, M. & Dennick, R. (2011). Making sense of Cronbach's alpha. *International Journal of Medical Education*. 2011;2:5355. Doi:10.5116/ijme.4dfb.8dfd.
- [24] Kaiser, H. F. (1974). An index of factorial simplicity. *Psychometrika*, 39, 31–36.
- [25] Hutcheson, G. D., and Sofroniou, N. (1999). *The Multivariate Social Scientist: an introduction to generalized linear models*. Sage Publications