SEMINAR
FÜR WIRTSCHAFTSINFORMATIK
UND SYSTEMENTWICKLUNG

Themasteller: Prof. Dr. Ali Sunyaev

Bachelorarbeit im Fach Information Systems

User Concerns with Information Security and Privacy of Patient-Centered Health IT Services

vorgelegt von:
Anders, Marco Manfred

Köln, April 2014

Table of Contents

Index of Illustrations

1. Introduction

1.1 Problem Definition

Patient-Centered Health IT-Services (PHS) are capable of storing medical data of patients and helping patients to become knowledgeable on their own health.[1] The focus of PHS always lies on the needs of the patient. Therefore patients always keep data sovereignty. However, this does not entirely prevent the chance of private information leaking to third parties, because the healthcare environment sometimes is obliged to disclose private information to others.[2] For example, if a patient is on sick leave his insurance needs to know why, in order to verify absorption of costs of the treatment. Nevertheless, private information of users should be treated as responsible as possible and be disclosed to others as few as possible, in order to prevent accidental, if not deliberate, misuse and its potential consequences.[3] Possible consequences are, for example, ”socio-economic repercussions”[4] that harm users or denial of insurance coverage.[5] The prevention of these consequences cannot be guaranteed for PHS, since the realization of the customized service requires the access of others to parts of that sensitive information. [6] Furthermore, PHS, as part of the web application technology which provides services over the internet, suffers additional information security and privacy dangers that can cause concerns of users.[7] For instance, the data clouds, in which the information of the users of the application and others is stored, are a valuable target for attacks, because they contain sensitive data of multiple entities.[8]
As a result it is desirable to help patients to identify possible risks that could arise if one discloses sensitive medical information. Thus, patients will be more capable of

[1] cf. for this and following two sentences Dehling and Sunyaev (2014, p. 1)

[2] cf. Appari and Johnson, M. Eric (2010, p. 290)

[3] cf. Appari and Johnson, M. Eric (2010, p. 284)

[4] cf. Appari and Johnson, M. Eric (2010, p. 290)

[5] cf. Appari and Johnson, M. Eric (2010, p. 285)

[6] cf. Laric, Pitta, and Katsanis (2009, pp. 97–98)

[7] cf. Subashini and Kavitha (2011, p. 6)

[8] cf. Kaufman (2009, p. 63)

estimating whether they want to entrust their private information to service providers, which yields them either the benefits of the customized service PHS offer, or the option to protect their privacy.[9] Furthermore, better knowledge of these concerns could help in vanquishing, or at least mitigating, some of those concerns, because known concerns will probably be easier to address. This would possibly lead to improvement of the quality of PHS by introducing new features or services that address these concerns.[10]

Information privacy and security concern research normally uses either the keyword information privacy concern, or the keywords security concerns or security risks.[11] Moreover, the concepts of information privacy and information security overlap each other, but the relationship between them is not researched yet.[12] Furthermore, it is not known whether individuals see them as distinct concepts at all.[13] Generally, the keyword information privacy concern is used far more often than information security concern. A lot of research focuses on the measurement of information privacy concern as a proxy for measuring users' perception of privacy, in order to further investigate its causes and consequences, with special interest on its influence on consumers' willingness to disclose information to organizations and/or websites.[14] Many of the causes and consequences have been found to have an influence on, or being influenced of information privacy concerns, but often the combination of results of different studies remain inconclusive due to contradictory results.[15]

---

[9] cf. Acquisti and Grossklags (2005, p. 7)

[10] cf. Dehling and Sunyaev (2014, p. 2)

[11] cf. Hong and Thong, James Y L (2013); Li (2011); van Deursen, Buchanan, and Duff (2013); Subashini and Kavitha (2011)

[12] cf. Ambrose and Basu (2012, p. 44)

[13] cf. Belanger, Hiller, and Smith (2002, p. 248)

[14] cf. Smith, H. Jeff, Dinev, and Xu (2011, p. 997); Malhotra, Sung S. Kim, and Agarwal (2004); Dinev and Hart (2006); Smith, H. Jeff, Milberg, and Burke (1996)

[15] cf. Li (2011, p. 454); Smith, H. Jeff et al. (2011, p. 998)

Recently, scholars have more often researched information privacy and security simultaneously in the healthcare environment.[16] Thereby, research focuses either on the development of new technologies in order to ensure privacy of patients, or on the enactment of the new regulation in the USA, the Health Insurance Portability and Accountability Act (HIPAA).[17] Additionally, mobile health applications are also an increasing field of interest, and this thesis will focus on the information privacy and security concerns of the mobile health application called PHS.

1.2 Objectives

The main objective of this thesis is to determine information security and privacy concerns of users with respect to PHS. This results in two partial objectives. First, to identify information security and privacy concerns of users regarding web sites, web applications and further software. Second, to identify characteristics regarding information security and privacy, which distinguish PHS from other web sites, web applications and further software.

With both partial objectives met, it is then possible to transfer the general concerns of users that were collected to the domain of PHS. To do that, the detected specific characteristics of PHS are applied to evaluate the general concerns of users regarding the domain of PHS.

2. Methods

2.1 Literature Review

At First, it was searched for articles in journals and conferences in the databases of ACM, EBSCO (Business source complete, Academic search complete and MEDLINE) and ABI/Inform. In EBSCO it was only searched for academic journals. In ABI/Inform it was only searched for scholarly journals and working papers. In ACM, no further restrictions were applied. It was searched for the keywords ((concern OR doubt OR worry OR "preferences") AND (privacy OR "Information Security") AND (ecommerce OR information OR online OR internet OR web OR application OR software OR

---

[16] cf. Appari and Johnson, M. Eric (2010); Agaku, Adisa, Ayo-Yusuf, and Connolly (2014); Ambrose and Basu (2012)

[17] cf. for this and following sentence Appari and Johnson, M. Eric (2010, p. 280)

service)). It was only searched in the title of articles, because additional search in the abstract lead to far too many articles unrelated to the subject of this thesis. The word "preferences" was only searched in plural, because it probably only appears in plural in articles relevant for this thesis, for example "User preferences" or "The users' preferences". The use of "Information Security" as fixed term instead of using "security" is due to the fact that it also yielded far too many articles unrelated to this thesis. It was documented for each database, how many articles were found and which articles were found in that database.
Using this method, 225 articles were found in total, which includes 116 in EBSCO, 93 in ABI/Inform, and 16 in ACM. Thereafter, articles that were written by anonymous and articles that were found more than once were sorted out. With this done, 144 articles remained.

2.2 General Information Privacy and Security Concerns of Users

Subsequently, the remaining articles were examined by its title. Articles that dealt with the organizational point of view of user concerns, they were often coupled with marketing aspects like for example purchase behavior, were sorted out. This was the most frequent reason for an article sorted out in this stage. Further common reasons for articles to be sorted out were that the article dealt with effects or influences that user concerns had on other things, or that the articles dealt with psychological aspects of privacy concerns. Reasons for articles to be kept include that they dealt with the user point of view of privacy concerns, that they included empirical research, or that they contained a medical aspect in the article.
Afterwards, articles were examined closely by using their abstract. In case of doubt the full text was skimmed through as well. Furthermore, during the execution of the step the articles were sorted into the categories "general user concerns" and "health related literature". In the end 21 articles remained. Of those, 16 were taken from ABI/Inform and 5 from EBSCO. It has to be mentioned though, that all duplicates were removed from EBSCO and ABI/Inform was taken as the primary database, therefore the numbers do not represent the importance of these databases for the literature review. It can only be concluded that EBSCO contained 5 articles ABI/Inform did not contain.

3. Definitions

PHS:

"Patient-Centered Health IT Services are scalable information systems that leverage information technology to support patients in managing and becoming knowledgeable on their own health; PHS are designed to fulfill patients' needs, do not have to incorporate requirements of care providers, and can be provided by anyone who can finance the required resources"[18]

4. Results

4.1 Literature Review

In 1890, privacy was first declared as a right when Warren and Brandeis called it the "right to be let alone"[19]. Today, information privacy is considered a subset of the concept of privacy in general, which generates increasing level of concern among people.[20] This is due to the advancing technology, which now makes it possible to store and analyze huge amounts of data.[21] Moreover, the use of internet in the field of information privacy emerged further concern about security.[22] For instance, outsiders have the opportunity to gain unauthorized access to private information of others by means of hacking. This led to blurring of the borders between the two fields of information security and privacy.[23] It is still unknown, in what way they are related to each other and additionally it is also still unknown, whether users of IT-services see a difference in those two concepts at all. Ackerman (2004) suggested that "security is necessary for privacy, but security is not sufficient to safeguard against subsequent use, to minimize the risk of […] disclosure, or to reassure users "[24]. Because even if security

---

[18] cf. {Dehling 2014 #4I: 1}

[19] cf. Warren and Brandeis (1890, p. 1)

[20] cf. Smith, H. Jeff et al. (1996, p. 167); Bélanger and Crossler (2011, p. 1018)

[21] cf. Dinev, Bellotto, Hart, Russo, and et al (2006, p. 63)

[22] cf. for this and following sentence Appari and Johnson, M. Eric (2010, p. 284)

[23] cf. for this and following sentence Belanger et al. (2002, pp. 247–248)

[24] cf. Ackerman (2004, p. 432)

is guaranteed, it is not guaranteed that organizations do not make bad decisions about subsequent use of information, which may lead to information privacy problems.[25] As a result of this and the fact that privacy itself cannot be measured, information privacy (and security) concerns are a field of interest for researchers in order to measure users' perception of privacy.[26] Information privacy concerns (IPC) are often referred to as "concerns about possible loss of privacy as a result of information disclosure to an online business" [27]. Others define IPC as "individual's subjective views of fairness within the context of information privacy"[28]. In order to measure the influence and the Perception of privacy, research about IPC usually focuses on the level of concern users feel, or the influence of privacy concerns on other variables, or vice versa, the influence of other variables on privacy concerns.[29] Examples for other variables are demographic factors, personality differences and willingness to provide personal information. Smith et al. (1996) developed the first framework to measure IPC named "Concern for Information Privacy", which consists of four dimensions:[30] Secondary use, improper access, errors and collection. Subsequently, more dimensional frameworks were developed (see chapter 4.2.1 for more detailed information). Hsu (2006) suggested that information privacy concern should rather be seen as a situational paradigm, like it had already been suggested for privacy itself, because IPC are dependent on outside factors like for example website category (e-commerce, government site and others).[31] The context dimensions, which are considered to have an influence, are domain of the research construct, time, location, occupation, culture, and rationale.[32] Xu et al. (2008)

---

[25] cf. Culnan (1995, p. 14); Smith, H. Jeff et al. (2011, p. 998)

[26] cf. Smith, H. Jeff et al. (2011, p. 997)

[27] cf. Xu, Dinev, Smith, and Hart (p. 4)

[28] cf. Malhotra et al. (2004, p. 337)

[29] cf. for this and following sentence Bélanger and Crossler (2011, p. 1020)

[30] cf. for this and following two sentences Bélanger and Crossler (2011, p. 1020); Smith, H. Jeff et al. (1996, p. 170)

[31] cf. Chiung-wen Hsu (2006, p. 571)

[32] cf. Smith, H. Jeff et al. (2011, p. 1002)

suggested an integrative view, by concentrating on how IPC are formed.[33] Their main determinant for IPC is "disposition to value privacy"[34], which is each individual's appreciation of privacy.[35]

When divided by sector of research, the majority of articles deals with e-commerce and marketing, but there is also a growing number of articles with medical background. [36] This might be due to the fact that in the medical environment the field of IPC comprises additional complications when compared to other domains of PHS. To begin with, the information present in healthcare industry generally is perceived more sensitive than in other domains.[37] This is due to the fact that disclosure of information might negatively affect social acceptance, employment opportunities, or individual relationships, which are key areas of daily life.[38] Examples for such highly sensitive information are HIV status, diseases, psychiatric care, and physical abuse.[39] Therefore, the perceived risk is a lot higher than in other domains and possible consequences are more severe.[40] This might go as far as patients initially refusing disclosure of information and as a result not receiving treatment.[41] Additionally, in other domains the relationship between service provider and the recipient of the service is two-dimensional, consisting of buyer and seller.[42] However, in healthcare it is normally a tripartite relationship. If the patient is insured, which is most commonly the case, the buyer splits into the insurance and the patient, making the relationship consist of three parties. As a matter of fact there is a good chance that more than three parties are involved, for example a hospital or a

---

[33] cf. Xu et al. (p. 4)

[34]cf. Xu et al. (p. 6)

[35] cf. Xu et al. (p. 6)

[36] cf. Smith, H. Jeff et al. (2011, pp. A10)

[37] cf. Chiung-wen Hsu (2006, p. 577)

[38] cf. Laric et al. (2009, p. 94)

[39] cf. Rindfleisch (1997, p. 94)

[40] cf. Rohm and Milne (2004, p. 1001)

[41] cf. Rindfleisch (1997, p. 94)

[42] cf. for this and following two sentences Laric et al. (2009, p. 96)

pharmacy as a fourth party.[43] This complicates the relationship even further and creates new possible spots for privacy leaks or privacy breaches, because there are more people involved who might be curious about some information. Furthermore, they might accidently disclose information; for example, an e-mail sent to the wrong address. Furthermore, the private information in healthcare is potentially interesting for other people or companies in order to improve their decision making; for instance, for employers that consider hiring a new employee in order to estimate period of disruption due to sickness, or a potential sexual partner might want to know whether the other person has sexually transmitted diseases.[44]

4.2 General Information Privacy and Security Concerns of Users

This chapter first addresses the following questions: "How can an information privacy concern be defined?", "How can an information security concern be defined?", and "What do information privacy concern and information security concern have in common?" Then, it is examined what variables have an influence on information privacy (and eventually security) concern or are influenced by information privacy (and eventually security) concern?" Subsequently, the impact of information type on information privacy and security concern is examined. Finally, empirical data on information privacy and security concerns is given.

4.2.1 Frameworks for Information Privacy Concerns

The first article, which was written in order to establish a framework to detect and measure IPC, was written by Smith et al. in 1996.[45] The name of the framework is "Concern For Information Privacy" (in the following referred to as "CFIP"). In 2004, Malhotra et al. introduced a new framework named "Internet Users' Information Privacy Concerns" (in the following referred to as "IUIPC"). These are the two most used frameworks by studies. In addition, Xu et al. recently developed "Mobile Users' Information Privacy Concerns" (in the following referred to as "MUIPC").[46] All

---

[43] cf. for this and following two sentences Laric et al. (2009, p. 97)

[44] cf. Laric et al. (2009, p. 101); Appari and Johnson, M. Eric (2010, p. 284)

[45] cf. for this and following three sentences Bélanger and Crossler (2011, p. 1040)

[46] cf. Heng Xu, Sumeet Gupta, Mary Beth Rosson, and John M. Carroll (p. 1)

mentioned frameworks use the seven-point likert scale to measure the amount of agreement the person questioned has towards each questioned item with “1” being strongly disagree and “7” being strongly agree.[47]

4.2.1.1 Concern For Information Privacy

The “Concern For Information Privacy” (CFIP) framework consists of 15 items divided into four dimensions.[48] The dimensions are “Collection”, “Unauthorized Secondary Use”, “Improper Access” and “Errors”. The dimension “Collection” contains four items and measures how much people are concerned about organizations collecting private data from them.[49] “Unauthorized Secondary Use” consists of four items and deals with the concerns of users, that data is collected for some reason with their knowledge and approval, but is then also used for another purpose, for example an e-commerce company, which sends ordered goods to their customers, needs the address and name of their customers to send them the ordered articles. If they used this information to send their customers advertising without asking them for permission previously it would be unauthorized secondary use. This secondary use would be internal because the data was collected and used by the same company. If the data had been sold to another company and they had sent advertisement to the first companies’ customers, this would be external. External unauthorized secondary use usually concerns customers more than internal.[50] “Improper access” consist of three items and deals with the users’ concerns, that their data is accessible to individuals that do not need access to their data. Furthermore, it does not matter for what reason people have access to the data. Therefore, this dimension can be related to information security. The dimension “Errors” consist of four items and measures the concerns of users, that data collected about them is incorrect.

---

[47] cf. Malhotra et al. (2004, p. 351); Smith, H. Jeff et al. (1996, p. 186); Heng Xu et al. (p. 5)

[48] cf. for this and following sentence Smith, H. Jeff et al. (1996, p. 170)

[49] cf. for this paragraph Smith, H. Jeff et al. (1996, pp. 171–173)

[50] cf. Tolchinsky et al. (1981, p. 311)

4.2.1.2 Internet Users' Information Privacy Concerns

The Internet Users' Information Privacy Concern (IUIPC) framework consists of 10 items divided into three dimensions.[51] The dimensions are "Awareness", "Control" and "Collection". The dimension "Collection" is similar to its namesake in the CFIP-framework. The dimension "Control" refers to an individuals' concern to lose control about their information. If their data is used in any way they do not comply with, they want to have the option to change this state. For example if a company collects and uses data without the users' knowledge, the user has no control, because he cannot influence the companies' actions in any way. The given example also includes the dimension "Awareness", because this dimension is dedicated to making people aware of what is done. In this example they are not informed what is done and thus, they are not aware of it. "Awareness" and "Control" are often correlated as one can see in the example. "Collection" consists of four items, "Awareness" and "Control" each consist of three items.[52]

4.2.1.3 Mobile Users' Information Privacy Concerns

The Mobile Users' Information Privacy Concerns (MUIPC) framework consists of nine items, which are divided equally into the dimensions "Surveillance", "Intrusion" and "Secondary Use".[53] The MUIPC-framework focuses more on apps and smartphones. The dimension "Secondary Use" equals the dimension of the same name in the CFIP-framework, whereas the other two dimension are new concepts. "Surveillance" deals with the perceived surveillance of users, because it is widely known that the new technologies, like smartphones in cooperation with apps collect data. In addition, they are capable to collect a lot more data than computers, because data from one person is a lot more concentrated on a smart phone. Thereby, users feel that vendors always keep an eye on them and that raises their concern. The dimension of "Intrusion" deals with the perceived possibility that others invade someone's privacy. The possible invasion makes the people affected feel uncomfortable, because they feel the intruder has the option to decide what to do with their data. It does not matter whether it really happens. It is enough that the possibility of this is present. This dimension also contains a

---

[51] cf. for this paragraph Malhotra et al. (2004, pp. 338–339)

[52] cf. Li (2011, p. 459)

[53] cf. for this paragraph Heng Xu et al. (pp. 4–5)

connection to security, like the dimension of "Improper Access" of the CFIP-framework, because malware is able to execute exactly this invasion.

Although every framework has its own emphases, they all overlap each other in certain areas as displayed earlier.[54] Further researches about frameworks related to IPC include Stewart and Segars in 2002, Dinev and Hart in 2004 and Buchanan et al. in 2007.

4.2.2 Framework for Information Security Concern

It has been found that users perceive security features more important than security seals, privacy statements, and privacy seals when buying goods or services over the web.[55] Therefore, it appropriate to examine information security now. Information security "risks"[56] are often associated with terms like "data breach", "data theft", "Hackers attack", due to the fact that mainstream media often calls them like that.[57] Therefore, users may mainly see these potential risks when thinking of security. In this section possible threats to security are listed, because all of these threats may trigger user concerns and there is no defined framework for information security concern. It is chosen the domain of "Cloud Computing", centered on the "Software as a Service"-concept (SaaS), as an example because it is relevant for the domain of PHS in a posterior chapter of this thesis.

4.2.2.1 Information Security Framework

Information security consists of three main concepts: *Data Confidentiality, Integrity, and Availability*.[58] Thereby, *Confidentiality* means that only authorized parties or systems with access skills are allowed to access the protected data. *Integrity* refers to the point that changes of data, applications, and equipment should only be performed in an authorized manner and or by authorized parties. As a result they are protected through

---

[54] cf. for this and following sentence Li (2011, pp. 459–460)

[55] cf. for this and following sentence Belanger et al. (2002, p. 265)

[56] for further details see chapte 4.2.4.1

[57] cf. Ion, Sachdeva, Kumaraguru, and Čapkun (p. 12)

[58] cf. for this paragraph Georgescu and Suicimezov (2012, pp. 223–225)

the non-authorization of creation, change or deletion. Lastly, *Availability* implies that a system or data should be accessible and usable when requested of authorized entities.

4.2.2.2 Information Privacy Concern compared to Information Security Concern

A study of information privacy concerns yielded the dimensions of secondary use, improper access, collection, and errors. Since no framework for information security concern was found we will use the dimensions of confidentiality, integrity, and availability from the field of information security. The concepts of information security and information privacy concern overlap each other and it is unknown whether users see them as different concepts at all.[59] Confidentiality means that only authorized parties are allowed to access the protected data. For an individual this means that they control the data, since they initially are the only ones authorized to access their own personal data and may give that access to others. Privacy is defined as "the ability of individuals to personally control information about themselves"[60]. Therefore, it is argued that confidentiality highly overlaps with privacy. Integrity refers to the protection of data against non-authorized creation, change or deletion. In comparison, Errors refer to incorrect data. Accordingly, it is argued that errors highly overlap with integrity. Finally, the dimension of improper access of the CFIP-framework is also associated with security.

4.2.2.3 Information Security in Software as a Service

Cloud Computing is defined as "a style of computing where massively scalable IT-enabled capabilities are delivered 'as a service' to external customers using Internet technologies"[61]. Furthermore, SaaS is defined as "SaaS is a software deployment model where applications are remotely hosted by the application or service provider and made available to customers on demand, over the Internet"[62].

In this environment many security issues arise.[63] Firstly, *data security* is concerned with the additional security problems that arise when data is not stored inside the boundaries

---

[59] cf. Belanger et al. (2002, pp. 247–248)

[60] cf. Smith, H. Jeff et al. (1996, p. 168); Li (2011, p. 454)

[61] cf. Subashini and Kavitha (2011, p. 2)

[62] cf. Subashini and Kavitha (2011, p. 3)

[63] cf. for this and following two sentences Subashini and Kavitha (2011, p. 4)

of the organization, but at the SaaS vendor end. Unauthorized access could occur due to security vulnerabilities in the application or through malicious employees. Secondly, *network security* deals with the additional security issues caused by the information flow via the internet.[64] The threat persistent is that a user with bad intentions could abuse weaknesses in network security configuration in order to sniff network packages. *Data locality* refers to problems that may occur when data is stored in other countries, because each country has different data privacy laws. For example, in some countries certain types of data are not allowed to leave the country. *Data integrity* has already been mentioned earlier, though in the SaaS-environment its complexity multiplies. For example, in the SaaS-environment "multitenancy" is common, which describes the sharing of aspects of information security among memory, applications, network, and data.[65] The sharing of those aspects triggers confidentiality problems that would not exist without sharing. Multitenancy is also reason for *data segregation* issues, because multitenancy makes it possible that multiple users can store their data using the application. The downside of this is that due to the same location of users' stored data one user may invade another user's data. *Data access* refers to the problem, that multiple organizations may store data in a single cloud. Each of these organizations may want to give certain of their employees access rights to information and others not. The cloud must be able to support each of these different privacy policies of organizations.

Web application security deals with problems that occur because the application has to be used and managed over the web.[66] Thereby, all its features and data are accessible through the web and can potentially be altered. This means that this problem does not only affect one user, but can potentially affect all users that use this application. Furthermore, this problem is known for some time now, because it is true for all web application technology, and traditional network security measures such as network firewalls, still do not sufficiently address the problem. Another possible risk is *data breach*, which concerns intrusion into the cloud-environment.[67] In the cloud-

---

[64] cf. for this paragraph Subashini and Kavitha (2011, p. 5)

[65] cf. for this and following sentence Georgescu and Suicimezov (2012, p. 224)

[66] cf. for this and following three sentences (2011, p. 6)

[67] cf. for this and following eight sentences Subashini and Kavitha (2011, p. 7)

environment data from multiple users and business organizations is stored and therefore, in case of intrusion, in danger. This makes cloud a highly valuable target for attacks.[68]Also, employees of the SaaS providers do not have direct access to the databases, still they have access to other data in the system and therefore, it does not reduce the risk of breaches. *Vulnerability in virtualization* implies that virtualization, which means multiple instances on the same physical machine running isolated from each other, is not yet operating entirely as it is supposed to. Nowadays, Virtual Machine Monitors do not entirely offer isolation. "Some vulnerability has been found in all virtualization software which can be exploited by malicious, local users to bypass certain security restrictions or gain privileges"[69]. *Availability* has also already been mentioned earlier, but is as well concerned as integrity in terms of the fact that SaaS makes several things more complex.[70] For instance, in order to achieve availability, a "multi-tier architecture needs to be adopted, supported by a load-balanced farm of application instances, running on a variable number of servers"[71].Additionally, *backups* are necessary to prevent loss of data. If not encrypted and secured properly, information may leak from the backups instead from the original data, which in terms of security does not make any difference. Last, but not least, *identity management and sign-on process* refers to identification of individuals in a system. If weaknesses exist in this area, it can be used to take over user accounts and endanger sensitive data.

4.2.3 Antecedents of Information Privacy Concern

This section covers the antecedents of Information privacy concerns. First, the demographic factors are examined closer, and then we investigate the non-demographic factors and the typologies of privacy.

4.2.3.1 Demographic Factors

Gender: Several studies were realized that investigated whether gender had an influence on users' IPC or not. There are several studies that argue that the gender does not

---

[68] cf. Kaufman (2009, p. 63)

[69] cf. Subashini and Kavitha (2011, p. 7)

[70] cf. for this and following five sentences Subashini and Kavitha (2011, p. 8)

[71] cf. Subashini and Kavitha (2011, p. 7)

influence users' IPC.[72] But there are also studies that argue that the gender does influence users' IPC.[73] Hence, a clear statement regarding the influence of gender on IPC cannot be made.

Age: In contrast the uncertainty regarding the influence of gender on users' IPC, it is certain that age has an influence on users' IPC, as multiple studies pointed out. [74] In general, it is argued that older users are more concerned regarding IPC than younger users.[75] But there are also other influences reported, for example that older users are either very concerned or unconcerned and younger users are most likely moderately concerned.[76]

Income: The Income also has an influence on users' IPC, but it is not entirely clear whether higher income decreases or increases the level of users' IPC, though usually the results indicate that higher income causes higher level of IPC.[77]

Education Level has a negative effect on users' level of IPC.[78] Therefore, users that are higher educated are less concerned about information privacy.[79]

Internet Experience has been found to influence the users' level of IPC negatively, meaning that more experience reduces the level of users' IPC.[80]

All together the overall influence of demographic factors on users' IPC remains unclear, since several studies constantly yielded different results in certain areas.[81]

4.2.3.2 Non-Demographic Factors

The country people live in has an influence on their IPC.[82] However, it does not influence users' level of IPC overall, but the level of concern regarding a dimension of

---

[72] cf. Phelps, Nowak, and Ferrell (2000, p. 36); Zukowski and Brown (p. 202)

[73] cf. Fogel and Nehmad (2009, p. 157); Janda and Fair (2004, p. 14)

[74] cf. Kim Bartel Sheehan (2002, p. 27); Zukowski and Brown (p. 202)

[75] cf. Zukowski and Brown (p. 202)

[76] cf. Kim Bartel Sheehan (2002, p. 27)

[77] cf. Zukowski and Brown (p. 202); Graeff and Harmon (2002, p. 311); Phelps et al. (2000, p. 36)

[78] cf. Zukowski and Brown (p. 202)

[79] cf. Phelps et al. (2000, p. 36)

[80] cf. Bellman, Johnson, Kobrin, and Lohse (2004, p. 322)

[81] cf. Hwang, Han, Kuo, and Liu (2012, p. 3786)

IPC. When examining closer what the factors for these differences are, it has been found that the privacy regulatory framework present in a country has the biggest influence.[83] Cultural values are a smaller factor, but they also influence the dimensions of IPC.[84] For instance, cultural values affect two dimensions of the CFIP-framework: Secondary use and errors, but they do not affect improper access and collection.

Awareness reflects whether people are informed about the usage or collection of data. [85] It has been suggested that as long as people are not aware of certain secondary uses of their data, they are not concerned. When they learn about the use without their permission though, privacy concerns are triggered.[86] For example, people who are not aware of name removal procedures seem to be less likely to be concerned about name removal than people who were informed about the procedures.[87] In contrast, if companies ask clients for permission about collection and use of data in the first place, they tend to be less concerned.[88]

Experience: When people already experienced privacy intrusion in earlier stages of their lives their IPC are on a higher level than for people that have not yet had negative experience with privacy intrusion.[89]

Personality: Each individual has his own personal boundary up to which it is acceptable that others collect their private information.[90] These boundaries further change depending on who wants to collect their information and how it is collected.

4.2.3.3 Typologies of Privacy

Westin divided consumers into three different privacy typologies.[91] The first category is named “Fundamentalist” and consumers in this group nearly always tend to choose their

---

[82] cf. for this and following sentence Chiung-wen Hsu (2006, p. 575); Bellman et al. (2004, p. 313)

[83] cf. Bellman et al. (2004, p. 323)

[84] cf. for this and following sentence Bellman et al. (2004, p. 321)

[85] cf. Malhotra et al. (2004, p. 348)

[86] cf. Cespedes and Smith, H. Jeff (1993, pp. 10, 16); Smith, H. Jeff et al. (2011, p. 998)

[87] cf. Culnan (1995, p. 14); Smith, H. Jeff et al. (2011, p. 998)

[88] cf. Nowak and Phelps (1995, p. 57)

[89] cf. Culnan (1993, p. 351)

[90] cf. for this and following sentence Cespedes and Smith, H. Jeff (1993, p. 13)

privacy protection over consumer benefits. The other extreme are the "Unconcerned", they tend to always choose consumer benefits over privacy protection. In between those two extremes, there are the "Pragmatists", who always assess perceived advantages through benefits and perceived disadvantages through privacy intrusion and then decide based upon whether they value of the advantages or the value of the disadvantages higher.

However, this separation was not dedicated to online consumers but to consumers in general. Hence, a study was conducted in order to determine whether the given categories also apply to online consumers or not.[92] The results were that in the online environment further criteria applies.[93] Therefore, online users were divided into unconcerned internet users, circumspect internet users, wary internet users and alarmed internet users, listed in ascending level of concern and likelihood to provide incomplete data upon registration on websites. Moreover, the percentage of registrations on encountered websites decreases from unconcerned internet user to alarmed internet user. In this study 16 % of the questioned users were unconcerned, 38% were circumspect, 43% were wary and 3% were alarmed internet users. It has been argued though, that alarmed internet users may not have participated in the study, because they were too concerned.[94] Thus, the category alarmed internet users may be bigger than in the results of this study.

4.2.4 Consequences of Information Privacy Concern

First we have a closer look on the concepts of risk and trust, because they are very often discussed in the context of information privacy concern.[95] Afterwards, we have a look on behavior and information privacy concern.

4.2.4.1 Risk

Risk is generally defined as "the possibility of loss or injury"[96]. However, in the context of IPC the risk involved is normally not known. Therefore, the users' perceived risk is

---

[91] cf. for this paragraph Kim Bartel Sheehan (2002, p. 23)

[92] cf. Kim Bartel Sheehan (2002, p. 21)

[93] cf. for this and following three sentences Kim Bartel Sheehan (2002, p. 30)

[94] cf. for this and following sentence Kim Bartel Sheehan (2002, p. 31)

[95] cf. Li (2011, pp. 454, 462)

normally used within the context of user concerns. Perceived risk is a calculation performed by the user, evaluating the likelihood of negative consequences and the severity of those consequences.[97] The negative consequences that individuals may get affected by are of material, emotional, or physical nature.[98] Known sources for negative consequences is, for example, opportunistic behavior of organizations that sell personal data to, or share personal data with, third parties like government agencies or financial institutions.[99] Besides, insider disclosure or unauthorized access to personal information and its' theft may occur. As for influences that risk has on other variables, conducted studies support that perceived risk increases the level of IPC.[100] Furthermore, studies support that perceived risk decreases the willingness to disclose private information and it also decreases users' trust.

4.2.4.2 Trust

In the context of Information privacy trust is defined as "the degree to which people believe a firm is dependable in protecting consumer's personal information"[101]. The relationship between IPC and trust seems to be complex.[102] Generally, most studies show that trust reduces privacy concern, although occasionally studies also find that there is no influence or even an increase of privacy concern.[103] Trust can be increased by firms by implementation of fair information practices, privacy policy, and/or display of privacy statements and/or seals of approval.[104] One study found that as a strategy, increasing trust may be more effective than reducing privacy concern when managing consumer information.[105]

---

[96] cf. Boehm (1991, p. 427)

[97] cf. Peter, J. Paul and Tarpey Sr, Lawrence X. (1975, p. 30)

[98] cf. Moon (2000, pp. 323–324)

[99] cf. for this and following sentence Smith, H. Jeff et al. (2011, p. 1001)

[100] cf. for this and following sentence Dinev and Hart (2006, p. 72)

[101] cf. Malhotra et al. (2004, p. 341); Li (2011, p. 464)

[102] cf. for this and following sentence Li (2011, p. 464)

[103] cf. Bansal, Zahedi, and Gefen (2010, p. 143)

[104] cf. Smith, H. Jeff et al. (2011, p. 1000)

[105] cf. Milne and Boza (1999, p. 18)

4.2.4.3 Behavioral Intention

The privacy calculus is a model that suggests that behavioral intentions to disclose information base on the assessment of the consequent risks versus the consequent benefits.[106] The behavioral intention to disclose information follows if benefits are higher than risk. If risk is higher than benefits, the intention is not to disclose information. In general, IPC negatively affect the willingness to disclose information. [107] Furthermore, users' perceived internet privacy risk increases internet privacy concern and also decreases the willingness to disclose information.

4.2.4.3.1 Privacy Paradox

The privacy paradox was developed to explain the fact that users state they have high concerns to disclose information, but then share their information freely more frequently than one would expect, for example on Facebook.[108] It argues that the earlier perceived benefits are likely to appear and the more perceived risk is diffused, the more probable it is that users disclose information.[109] This is interesting in the context of IPC, because the benefits may be immediate (convenience of buying goods or services online) and the risks may be invisible or diffused over time (identity theft).[110]

4.2.4.3.2 Elaboration Likelihood Method

The Elaboration Likelihood Method suggests that individuals' judgment method differs in state of high concern versus state of low concern. When in high concern, users are motivated to assess carefully whether to disclose information or not and therefore, they are more persuaded by argument quality. However, in low concern state, they are not motivated to assess their decision carefully, for example, by reading a privacy policy. Hence, they decide on basis of peripheral cues. This is also interesting in the context of IPC, because by domain usually you can find different levels of IPC.[111]

---

[106] cf. for this and following sentence Culnan and Armstrong (1999, p. 106); Derlega, Metts, Petronio, and Margulis (1993)

[107] cf. for this and following sentence Dinev and Hart (2006, p. 72)

[108] cf. Wilson and Valacich (p. 2)

[109] cf. Wilson and Valacich (p. 7)

[110] cf. Smith, H. Jeff et al. (2011, p. 1000)

[111] cf. Chiung-wen Hsu (2006, pp. 577–578)

4.2.4.3.3 Privacy Protection Behavior

When users want to benefit from online services, but their privacy concerns regarding that service are high, they normally have to choose between two options.[112] Either usage of the service and disclosure of private information, or protection of their private information or no usage of the service. However, they have developed strategies that help them to get what they want:[113] To protect their private information and to obtain the benefits of the service. These strategies can be further divided into dimensions.[114] For example they can be divided into "Fabricate", "Protect", and "Withhold". "Fabricate" refers to users making up information in order to hide their true identity, "protect" refers to users measures to prevent others from obtaining their private data. Withhold" refers to rejection to disclose requested information. "Fabricate" and "Protect" are unique to the online environment, whereas "Withhold" is present in the physical world as well as in the online environment. Though, if they withhold information, they might not be able to use the service.

4.2.5 Information Type and Information Context

The type of information disclosed influences the overall level of users' IPC. Different information types are demographic information, contact information, online contact information, health information, and other family members' information.[115] Within those, health information and other family members' information are perceived most sensitive and disclosed the least. Contact information is also considered quite sensitive in contrast to online contact information, which is considered the least sensitive. It is followed by demographic information, which is second least sensitive. Other very sensitive information types are financial information and personal identifier information.[116] It is known that a higher level of concern is related to a lower

---

[112] cf. for this and following sentence Culnan and Armstrong (1999, p. 106); Derlega et al. (1993)

[113] cf. for this and following sentence Chen and Rea, Alan I, Jr (2004, p. 85)

[114] cf. for this paragraph Wirtz, Lwin, and Williams (2007, p. 332)

[115] cf. for this and following three sentences Chiung-wen Hsu (2006, p. 578)

[116] cf. Phelps et al. (2000, p. 33)

willingness to disclose information.[117] Taking this into consideration, it is assumable that it is the same case vice versa.

However, in the right context even in general highly sensitive information may not be perceived that sensitive anymore.[118] This may be the case if the disclosure of information is logically comprehensible to the user. For example, if a medical service or web site requests medical information from the user and his family members. This is reasonable, because family disease background and the users' own health history may help to receive better medical treatment.

The whole construct of information privacy concern and its causes and consequences is shown in the following figure. The figure also distinguishes between IPC in general (General CFIP) and IPC when influenced by information type and context, which is then called specific CFIP. Since information security concern overlaps with IPC in several aspects, probably this framework is also partly applicable for information security concern. However, this has not been investigated until now, so this remains speculation.

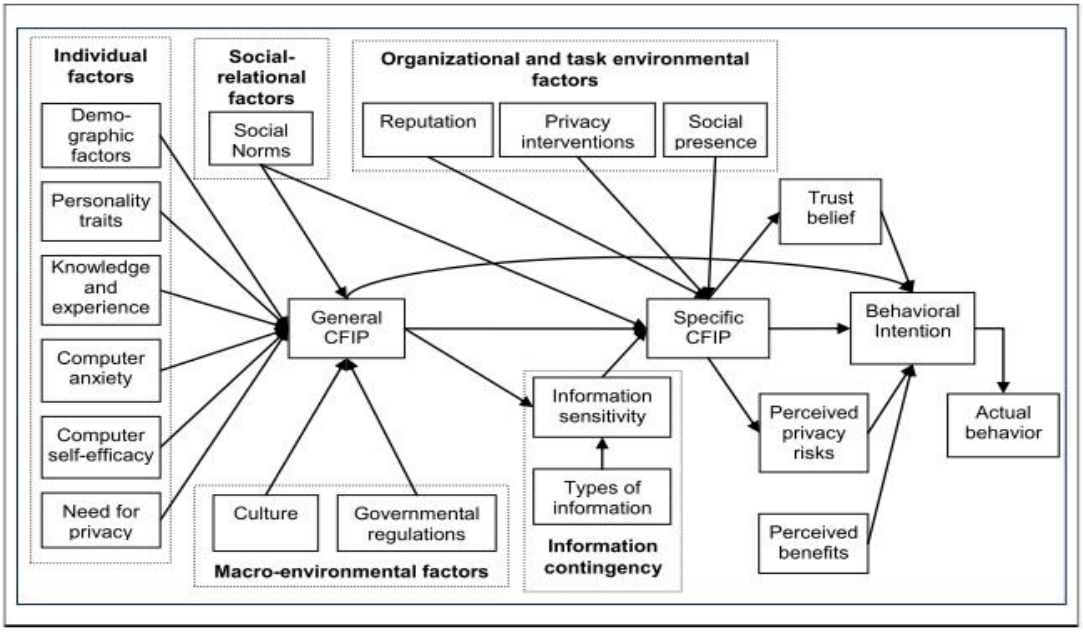

Fig. 4-1: Integrative Framework for the study on CFIP[119]

[117] cf. Dinev and Hart (2006, p. 72)

[118] cf. for this paragraph Chiung-wen Hsu (2006, pp. 571, 583)

[119] cf. Li (2011, p. 466)

4.2.6 Empirical Data about Information Privacy Concern

First, we investigate empirical data about the level of information privacy and security concern, and then we will examine empirical data about information privacy and security concern in context.

4.2.6.1 Level of Information Privacy and Security Concern

The data of Rose (2006) about information privacy concern, using the CFIP model, shows an average level of concern of 4.20 on a five-point likert scale with a standard deviation of 0.56.[120] This shows that users are generally concerned with information privacy. The ranking of CFIP-dimensions, in descending order, is as follows: improper access (mean 4.49), secondary use (mean 4.40), errors (mean 4.13), and collection (mean 3.79).

	Collection	Secondary use	Errors	Access
U.S.A. [26]	4	1	3	2
New Zealand [26]	3	1	4	2
New Zealand (this study 2002)	4	2	3	1

Fig. 4-2: Rank order of privacy concern dimensions[121]

In table 4-1 rankings of other surveys are found. In these three surveys secondary use and improper access raise more concern than errors and collection. In table 4-1 user concerns concerning internet are shown. Concerns about privacy score 5.0544 on a seven-point likert scale. Hacking and financial security score 5.2005 and 5.1311 , which is only slightly more than privacy. It can be argued that hacking and financial security both represent the concept of information security, because hacking is known to be one of the primary threats that users think about when thinking about information security, due to mass media.[122] As a result of this and the fact that those 2 items and the privacy item only differ slightly, one can argue that it encourages the theory that in terms of user concerns, security and privacy are highly overlapping concepts.[123]

---

[120] cf. for this and following three sentences Rose (2006, pp. 328–329)

[121] cf. Rose (2006, p. 329)

[122] cf. Ion et al. (p. 12)

[123] cf. Belanger et al. (2002, p. 248)

Measure	Mean	Std. Deviation	Variance
Protecting Children	5.2407	1.4141	2.000
Hacking	5.2005	1.3511	1.826
Financial Security	5.1311	1.3736	1.887
Spamming	5.1127	1.4138	1.999
Fraud	5.0951	1.3874	1.925
Privacy	5.0544	1.1379	1.295
Information Credibility	4.7488	1.2607	1.589
Personal Relationships	4.1368	1.5769	2.487
Product Experience	4.0346	1.5015	2.254
Compulsive Internet Use	3.8558	1.5242	2.323
Intellectual Property	3.7476	1.5417	2.377

Fig. 4-3: Internet Users' Concerns[124]

4.2.6.2 Information Privacy Concern and Context

When asking users to share their electronic medical records the dimensions of the CFIP scale score as follows: secondary use (mean 4.60), improper access (mean 4.39), errors (mean 4.09), and collection (mean 3.54). Therefore, users are more concerned with secondary use, improper access, and errors than with collection. Yet, they are still concerned with collection. The average scores for every dimension except collection exceeded four. Therefore, it can be argued that users are very concerned with respect to these aspects. Furthermore, users expressed that they are very concerned if business they did not do business with previously, purchased a list with medical information. Also, the majority of users were concerned when their protected health information was transferred between health professionals electronically.[125]

Credit card number and social security number are perceived very sensitive type information by users.[126] Therefore, they cause high concern among users. Other information types that cause much concern are financial information, medical information, and to a slightly lesser extent contact data.[127] Also users were quite

[124] cf. Janda and Fair (2004, p. 13)

[125] cf. Agaku et al. (2014, p. 375)

[126] cf. Tsai, Cranor, Acquisti, and Fong (2008, p. 15)

[127] cf. Cespedes and Smith, H. Jeff (1993, p. 13); Tsai et al. (2008, pp. 14–15); Chiung-wen Hsu (2006, p. 578)

concerned when information could indicate that they were terrorists or criminals and when information referred to bad physical state or deeper emotions such as depression or adult diapers.[128] Demographic information causes very little concern.[129]
When differing the recipient of information, the majority of individuals is concerned that employers or insurance companies use the personal information they acquire in marketing efforts about individuals.[130] For grocery stores and drug stores only the minority is concerned that they do it. This is also true within the social environment, people share the same information with some persons and with others not.[131]

4.3 Characteristics of Patient-Centered Health IT Services

In this chapter special characteristics of PHS are examined, in comparison to other applications, websites and further software.

4.3.1 Sensitive Information

The sensitivity of health information in medical records ranges from quite low sensitivity (age, weight, height, broken bones) to high sensitivity, for example, emotional problems, sexual behaviors, and genetic information.[132] However, apart from medical information a medical record often contains a medical history, which also contains background information about the client such as alcohol consumption, smoker or non-smoker, sedentary lifestyle, and family medical and mental history. [133]
Therefore, health information is, in general, deemed very sensitive and patients are highly concerned when their medical information is disclosed to others, probably regardless of other factors that normally influence privacy concern level.[134] If concern is high and the trust in the physician/the organization combined with the benefits of the

---

[128] cf. Tsai et al. (2008, pp. 16–17)

[129] cf. Chiung-wen Hsu (2006, p. 578)

[130] cf. for this and following sentence Rohm and Milne (2004, p. 1007)

[131] cf. Prasad, Sorber, Stablein, Anthony, and Kotz (p. 123)

[132] cf. Rindfleisch (1997, p. 94)

[133] cf. Laric et al. (2009, p. 100)

[134] cf. Rohm and Milne (2004, p. 1008); Chiung-wen Hsu (2006, p. 577); Bansal et al. (2010, p. 145); Li (2011, p. 469)

treatment are not assessed high enough to compensate too high levels of concern, according to the privacy calculus patients probably would not disclose information.[135] The privacy protection strategies that users normally could use at this point are not applicable in the health environment. Protection of the information is not possible, because the physician needs the information to treat the patient. Fabricate will not help either, because if they try to disclose made up or false information, if it works at all, they would not receive the correct treatment. Finally, withholding information is a solution that some patients chose, but this may negatively affect their own health or even health of others.[136] Moreover, it may also decrease the quality of healthcare surveillance systems. Especially when considering that individuals with poorer health status have higher perceived health information sensitivity, which increases privacy concern and therefore, also decreases willingness to disclose information.[137]

4.3.2 Information Flow

In contrast to other domains, in the healthcare domain the amount of parties involved in interactions is at least three, if the patient is insured.[138] These three parties are the patient, a physician and the insurance. If a hospital or medication is needed, the number of parties increases further. Nevertheless, with each party involved, the number of information pathways gets further multiplied and matters become more complex.[139] **Figure 2** shows possible information flows and their complexity within the health care sector. In addition to the five already mentioned parties, information may be needed or wanted from various other parties, for example, researchers, employers, or health information organizations.

---

[135] cf. Rindfleisch (1997, p. 94); Bansal et al. (2010, p. 144)

[136] cf. for this and following sentence Agaku et al. (2014, pp. 2, 4)

[137] cf. Bansal et al. (2010, pp. 144–145)

[138] cf. for this and following two sentences Laric et al. (2009, pp. 96–97)

[139] cf. Laric et al. (2009, p. 98)

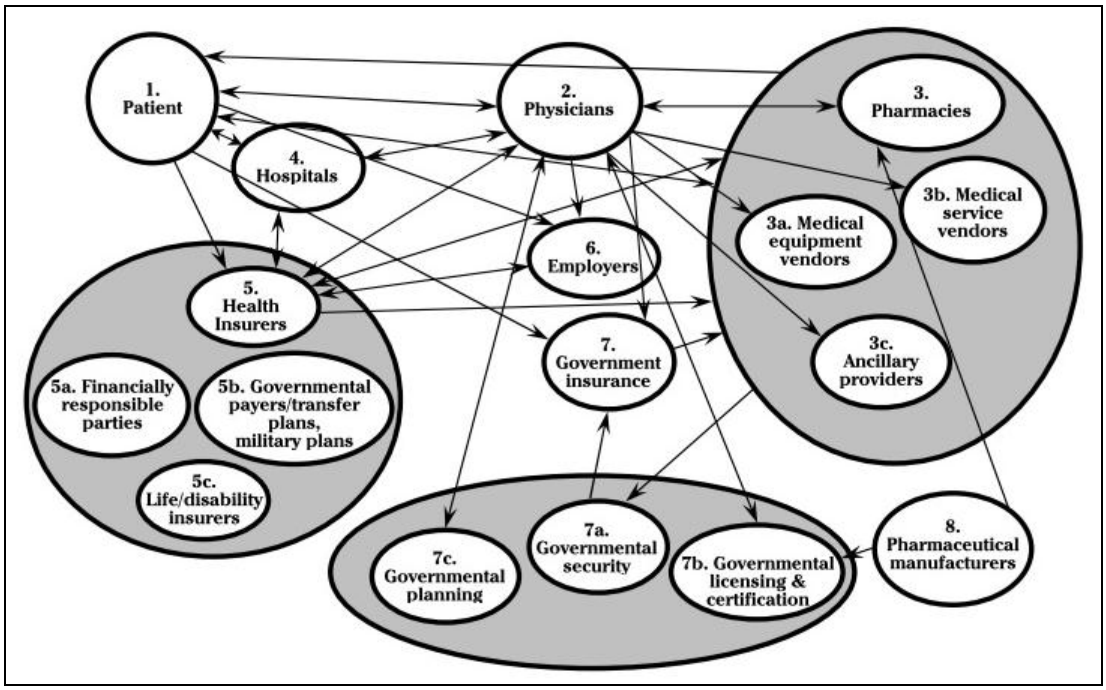

Fig 4-4: Information flow in healthcare[140]

Each of the parties is a potential danger for the privacy of the patient, when keeping in mind that for each party involved, not only one person gains access to the information, but several employees of that party.[141] At each place where the information is present, outsiders or insiders who are not authorized to have access to the information have the chance to force their access to the information or to accidentally disclose information. The possible scenarios can be summarized as:

"Accidental disclosure: Healthcare personnel unintentionally disclose patient information to others […].

Insider Curiosity: An insider with data-access privilege pries upon a patient's records out of curiosity or for their own purpose […].

Data breach by insider: Insiders access patient information and transmit it to outsiders for profit or revenge.

Data breach by outsider with physical intrusion: An outsider enters the physical facility either by coercion or forced entry and gains access to the system.

Unauthorized intrusion of network system: An outsider, including former employees,

---

[140] cf. Laric et al. (2009, p. 98)

[141] cf. for this and following sentence Laric et al. (2009, pp. 97–98); Anderson, British Medical Association, and others (1996, p. 4)

patients, or hackers, intrudes into an organisation's [*sic*] network from the outside to gain
access to patient information or render the system inoperable."[142]
In the case of insiders, for example, they could gain access simply by abusing their access rights to the system. Accidental disclosure could, for instance, be triggered by information on a prescription label on a bottle. With that being said, patients strongly believe that their information should only be disclosed to people who are involved in their care.[143] In contrast to this, healthcare organizations often give more access privileges than necessary to their employees, because of the complexity of data access management in the healthcare domain.

4.3.3 Special interest in Health Information

The medical information of a patient may be particularly interesting for others because of several reasons.[144] For employers, for example, health information about a potential employee is valuable, because they might be able to roughly estimate time of disruption because of sickness. For a current employee it could mean denial of promotion. They could use this data to assess applicants and if some of their applicants have high chances of be on sick leave for longer times than average, or weakened for a longer period of time in terms of concentration capability they will probably hire or promote another applicant. The same applies to insurance companies.[145] They might deny insurance coverage if they think insuring that patient is too risky in terms of economical perspective. Often medical treatment such as ambulatory care, prescribed pharmaceuticals, or services rendered by physicians and others requires information sharing.[146] As a consequence, the nature of the sickness may be disclosed to third parties. In fact, several organizations collect medical information, which makes it

---

[142] cf. for this and following two sentences Appari and Johnson, M. Eric (2010, pp. 284–285)

[143] cf. for this and following sentence Appari and Johnson, M. Eric (2010, pp. 285, 288)

[144] cf. for this and following two sentences Laric et al. (2009, p. 100); Appari and Johnson, M. Eric (2010, pp. 284–285)

[145] cf. for this and following sentence Appari and Johnson, M. Eric (2010, p. 285)

[146] cf. for this and following sentence Laric et al. (2009, p. 100)

possible for them to make medical inferences.[147] Another example is pharmaceutical companies working jointly with advertising agencies; they could use demographic information (age, income, and ethnicity) in order to try to improve marketing strategy and, therefore, sell more of their pharmaceutical.[148] But not only organizations might have a special interest in patient's medical information, also the social environment of a patient might have an interest in his/her medical information. For example, a partner in a romantic relationship might want to check if his/her partner has a sexually transmitted disease or an infectious disease, or a family member might want to know if he/she is at risk hereditarily.[149] Additionally, healthcare providers are obliged to report highly communicable diseases to medical authorities, in this case an individual's privacy is considered less important than safety rights of the larger community.[150]

4.3.4 Health Research and Likability od Data

In healthcare, information sometimes has to be shared to other stakeholders such as insurance agencies or research organizations to support their larger interest.[151] The information disclosed is masked for identifying and sensitive information, but it has to maintain analytic properties to assure statistical inferences. As a result, the data could still contain personally identifying information and sensitive information and thus cause corresponding bad consequences for patients. Some scholars argue that it is impossible to achieve complete independence of identity and medical data via delinking the both subjects from each other.[152] This problem only applies when the patient agrees that research uses his data.[153]

---

[147] cf. Rohm and Milne (2004, p. 1008)

[148] cf. Laric et al. (2009, p. 101)

[149] cf. Appari and Johnson, M. Eric (2010, pp. 284–285)

[150] cf. Laric et al. (2009, pp. 95–96)

[151] cf. for this and following three sentences Appari and Johnson, M. Eric (2010, pp. 290–291)

[152] cf. Behlen and Johnson (1999, p. 438)

[153] cf. Dehling and Sunyaev (2014, p. 2)

4.3.5 The Role of Technology

Generally, it has been found that the level of information security and privacy concerns of users concerning medical information increases with the level of technology used.[154] Additionally, it has also been found in other context that users think that data is safer when stored locally than when in the cloud.[155] Therefore, they prefer to store sensitive data locally.[156] However, the findings about cloud storage show big differences between countries (Switzerland and India). Moreover, the findings about increased level of concern when level of technology increases also found that individuals that were highly knowledgeable in terms of the given electronic health system, and individuals highly educated felt more comfortable with more advanced technology. This is especially relevant for PHS, since it is a web-application, which is a quite new technology.
[definition insider, …]

4.4 Information Privacy and Security Concerns of Users related to Patient-Centered Health IT Services

The objective of this thesis is to determine categories for information privacy and security concerns. A study of information privacy and security concerns yielded the dimensions of secondary use, improper access, collection, and errors. Since no framework for information security concern was found we will instead use the dimensions of confidentiality, integrity, and availability from the field of information security. In chapter 3.2.2.2 we found that security and privacy concerns overlap each other, especially the dimensions confidentiality and privacy, and integrity and Errors. Therefore, it is argued that confidentiality is a part of the concept of privacy or at least highly similar to a part of it and that the dimension of errors is a part of the concept of integrity, or at least highly similar to a part of it. Therefore they are both removed from the list. This leaves the dimensions of collection, secondary use, improper access, integrity, and availability.

The study of healthcare literature showed that security and privacy threats can be divided into five levels of organizational threats: accidental disclosure, insider curiosity, data breach by insider, data breach by outsider with physical intrusion, and

---

[154] cf. Angst, Agrawal, and Downing (2006, p. 14)

[155] cf. for this and following sentence Ion et al. (p. 8)

[156] cf. Subashini and Kavitha (2011, pp. 6–7)

unauthorized intrusion of network system.[157]Additionally, systemic threads have also been taken into consideration, but are for now left out.[158] The five levels of threats are altered, in order to fit the context of information privacy and security concerns more conveniently. Firstly, for the user it does not matter, whether the intruder uses physical intrusion or network intrusion, because for privacy concern it only matters whether someone gets access to information or not. How someone gains access is irrelevant in the context of privacy. Therefore, these two levels are summarized by data breach by outsider.

Next, the dimensions *availability, integrity, secondary use, improper access,* and *collection* are merged with the remaining *accidental disclosure, insider curiosity, data breach by insider,* and *data breach by outsider*. The only difference between data breach by insider and data breach by outsider is that an insider already has access to the data and an outsider needs to gain (improper) access to access it. Therefore, secondary use correlates with data breach by insider and as a result they are merged. When looking at the dimensions of CFIP, secondary use and improper access were the two highest rated dimensions in the healthcare environment, with secondary use being rated slightly higher. In fact, the dimensions of the CFIP scale were found to be correlated, improper access and secondary use had an estimated correlation factor of 0.81.[159] As a result data breach by outsider is merged with improper access and also with secondary use. This makes the categories indistinct, but it will be fixed later on by other criteria. Furthermore, improper access and insider curiosity are merged because an insider, who should not have access to data but has access to data, has improper access to the system. Accidental disclosure also leads to improper access of data and is therefore also merged with improper access and insider curiosity. Availability and integrity are also merged, because they both refer to data and security. As a result the categories “collection”, “accidental disclosure, insider curiosity, improper access”, “data breach by outsider, secondary use, improper access”, “data breach by insider, secondary use” and “availability and integrity” remain.

---

[157] cf. for this and following sentence Appari and Johnson, M. Eric (2010, pp. 284–285)

[158] cf. Etzioni (2008); Appari and Johnson, M. Eric (2010, p. 285)

[159] cf. Malhotra et al. (2004, p. 345)

Until now, the systemic threats were not considered. Systematic threats are organizations that have access to the information anyway, and use it for other purposes.[160] In the case of user concerns, this belongs to the category of secondary use and is therefore added to this category. Since the systemic threads clearly arise from insiders, they are merged with the category data breach by insider. Originally, the category of unauthorized intrusion of network system also consisted of the aspect that someone may want to render the system inoperable. This aspect is added to the category availability and integrity. Finally, the categories are now listed, renamed and defined.

4.4.1 Collection

This category is equal to the category collection of the CFIP scale.

4.4.2 Improper Access by a Person

This category indicates concerns that are caused by an employee of the medical environment having improper access to patient information, because he has more access privileges than necessary. Another cause of concern is that an employee accidentally discloses a small amount of personal information, which results in improper access. For example, an e-mail sent to the wrong recipient or a prescription bottle label with personal information is read by non-authorized individuals. The characteristics of this category are that one person or a small amount of people gain unauthorized access to a small amount of personal data. In the majority of the cases they will not use the information for other purposes, because they cannot, or do not want to make use of it. However, there might be underlying circumstances that cause people to use information for their own personal benefit. When financial benefits are obtained, for example by blackmailing, this incident is part of another category. An example for this would be a nurse or physician checking a fellow employee's medical records in order to check the possibility that the employee has sexually transmitted diseases or an e-mail accidentally sent to a wife instead of the husband because they have the same last name and they are both patients of the physician, which results in them being listed in the system consecutively. The e-mail could reveal that her husband had recently been tested for HIV (because he was unfaithful) or that he has a very severe sickness that he has not told his wife (yet). Therefore, the consequences for patients in this category are of emotional nature.

---

[160] cf. Etzioni (2008); Appari and Johnson, M. Eric (2010, p. 285)

4.4.3 Secondary Use by an Insider for Own Purpose

The main aspect in this category is secondary use of information by insiders, in the healthcare environment it is often named data breach. The insider is an organization that either already has access to the relevant information or to parts of it. In the case that they only have access to parts of it, they might use observations of patients to deduct (correctly or incorrectly) their medical state, which refers somewhat to improper access, and use it for their advantage in decision making.[161] Examples for this kind of concerns are employers denying employment or promotion, or insurance firms denying insurance coverage. Yet, the organization does not sell the information to others, they use it only for own purposes. For the most part consequences for patients in this category are of financial nature.

4.4.4 Numerous Sale or Disclosure of Information by a Person

The main aspect in this category is secondary use of information as well as in the previous category, but in this case the data breach is caused by an outsider or insider who usually wants to sell the information. This intrusion is performed by persons, but organizations are involved as well, because they might buy the information. The concerns refer to persons that use information for their own advantage at the expense of patients. If they initially do not have access to the information they find a way to access it. Consequences for patients are mainly of material nature but in rarer cases could be of emotional nature as well. The perceived severity of the consequences is quite high, because the information is possibly available for a lot of people and organizations, which may result in high financial losses or social rejection. **[ZITAT]** For example, a hacker may hack into the system or into the cloud and acquire a lot of data to sell to others. This does not only affect one user but many and additionally it is also dangerous for the application provider, because this may cause bad reputation. Another example is when the HIV infection of a patient becomes public because of an intruder, this might result in social rejection in the social environment of the patient.

4.4.5 Information Integrity and Availability

This category mainly refers to integrity of medical records and the concerns about errors in medical records. Within the scope of this thesis, concerns about non-availability

---

[161] cf. Laric et al. (2009, p. 100)

because of loss of information or temporarily down time of medical records systems were not found. Yet, in some rare cases like an emergency, the unavailability of medical records might cause severe physical consequences for patients.[162]
Errors in medical records also refer to the concerns about physical consequences as consequence of wrong medical treatment. Therefore, both factors are summarized in this category.

When prioritizing regarding the relevance of concerns for PHS it is suggested in descending order: C,D, E and B ,A. This order results from the following fact: it has been found that insiders are a major threat to the healthcare-environment. Additionally, the concept of SaaS, which is the concept that PHS is built on, has found to be complicated and not entirely secure (yet). Moreover, users' level of concern is higher the newer the technologies in healthcare are.[163] Lastly, collection concerned the users the least and has not yet created any problems for PHS, thus it is placed last. The remaining two categories cannot be prioritized by reference to the existing data.
When trying to prioritize regarding the relevance for the users, it is speculated that the descending order would be D, C, B, E, A. This order is speculated as a result of the results of Hwang et al. (2012), but a single study is not enough to support the speculation.

5. Discussion

The results suggest that information privacy and security concerns can be divided in the categories:

- Collection
- Improper Access by a Person
- Secondary Use by an Insider for Own Purpose
- Numerous Sale or Disclosure of Information by a Person
- Information Integrity and Availability

Furthermore, the characteristics of PHS are:

---

[162] cf. Rindfleisch (1997); Dehling and Sunyaev (2014, p. 4)

[163] cf. Angst et al. (2006, p. 14)

- PHS uses the advanced SaaS technology, but users level of concern increases with the level of technology used
- Information stored on PHS is nearly always perceived very sensitive
- Many parties have an special interest in the information stored on the PHS,
- Information has to be disclosed to certain parties, in order to guarantee medical treatment and payment
- Medical research needs to maintain a certain level of cross-linking

The information privacy and security concerns of users regarding PHS can be interpreted form many dimensions. Those dimensions are the source of the concern, for example, the attackers like insurance companies, employers, partners, employees of the medical environment, or hackers. Other dimensions are the dimensions of CFIP, the type of attacker (person, insider, outsider, organization), intention of attacker, type of consequence (material, emotional physical), and the amount of people the information is disclosed to. And it is suggested that they are also influenced by the antecedents and consequences of IPC. With this knowledge, researchers can easier develop features improving PHS for its users, because they know what problems they are addressing. Furthermore users of PHS are helped by making them aware of the aspects that user concerns cover, and with the new knowledge they are in a better position to decide whether they want to use PHS or not.

However, it can be argued that the category “Secondary Use by an Insider for Own Purpose“ could be divided and partly be fit into the categories “Improper Access by a Person” and “Numerous Sale or Disclosure of Information by a Person”. Yet, I believe that the users of PHS see these categories as distinct, because they have different attributes. Furthermore it could be argued that the category “Information Integrity and Availability” should be divided more in detail, but to users it doesn’t really matter how the information was stolen or lost, it counts only that it is disclosed and used against them. Loss of information also does not seem to be a big concern, as no concerns were found referring to loss of information. A possible explanation could be that users know about the important aspects of their health anyway, therefore they may not feel affected by loss of data. Additionally, the results are probably not considering all factors of information privacy and security concerns because it is a complex area, therefore there might be aspects of information privacy and security concerns that have to be added.

However, the goal of this thesis was to develop suiting categories to better distinguish different information privacy and security concerns and this has been achieved.
The limitations of the study were that there was no empirical data collected to support the results. Additionally, the used data was often student centric.[164] Also, the security and privacy regulations are different among the countries. The regulation in the country has been found to have an impact on information privacy concern therefore it is probable that it also has an effect on information privacy and security concern and this thesis uses results from many different nations. [165] Nevertheless, this thesis gives a good insight about the scope of the field and all the different factors that have an influence on it.

6. Conclusion and Outlook

The field of information privacy and security concerns of users is broad and very complex. The influences on privacy and security concerns have been studied quite a lot, yet many relationships remain inconclusive because of contradictory findings of studies. In this thesis it was first examined what information privacy and security concerns of users are, then special characteristics of PHS were identified, in order to help patients and developers of PHS. The categories were introduced to distinguish different aspects of these concerns and were created by applying the characteristics to the framework that was found for information privacy and security concerns of users.
Interesting topics for future research could be which type of information is perceived particularly sensitive in PHS or the electronic medical record. Another interesting topic for information privacy and security concerns could be the emergence of health banks and the implied privacy and security threats. Moreover, it might be interesting to examine whether the numerous antecedents and consequences of IPC also have an influence on information privacy and security concerns.

---

[164] cf. Bansal et al. (2010, p. 145); Belanger et al. (2002, p. 256); Hwang et al. (2012, p. 3787)

[165] cf. Bellman et al. (2004, p. 323)

7. References

Ackerman, M. S. (2004). Privacy in pervasive environments: next generation labeling protocols. *Personal & Ubiquitous Computing*, *8*(6), 430–439. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=15310999&site=ehost-live

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy Magazine*, *3*(1), 26–33. doi:10.1109/MSP.2005.22

Agaku, I. T., Adisa, A. O., Ayo-Yusuf, O. A., & Connolly, G. N. (2014). Concern about security and privacy, and perceived control over collection and use of health information are related to withholding of health information from healthcare providers. *Journal Of The American Medical Informatics Association: JAMIA*, *21*(2), 374–378. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=cmedm&AN=23975624&site=ehost-live

Ambrose, P., & Basu, C. (2012). Interpreting the Impact of Perceived Privacy and Security Concerns in Patients' Use of Online Health Information Systems. *Journal of Information Privacy & Security*, *8*(1), 38–50. Retrieved from http://search.proquest.com/docview/1037693069?accountid=10218

Anderson, R. J., British Medical Association, & others. (1996). *Security in clinical information systems*: British Medical Association London.

Angst, C. M., Agrawal, R., & Downing, J. (2006). *An Empirical Examination of the Importance of An Empirical Examination of the Importance of Defining the PHR for Research and for Practice*. University of Maryland. Retrieved from http://maint.ssrn.com/?abstract_id=904611

Appari, A., & Johnson, M. Eric. (2010). Information security and privacy in healthcare: current state of research. *International Journal of Internet & Enterprise Management*, *6*(4), 1.

Bansal, G., Zahedi, F. "., & Gefen, D. (2010). The impact of personal dispositions on information sensitivity, privacy concern and trust in disclosing health information online. *Decision Support Systems*, *49*(2), 138. Retrieved from http://search.proquest.com/docview/89303762?accountid=10218

Behlen, F. M., & Johnson, S. B. (1999). Multicenter patient records research: security policies and tools. *Journal Of The American Medical Informatics Association: JAMIA*, *6*(6), 435–443. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=cmedm&AN=10579601&site=ehost-live

Belanger, F., Hiller, J. S., & Smith, W. J. (2002). Trustworthiness in electronic commerce: the role of privacy, security, and site attributes. *The Journal of Strategic Information Systems*, *11*(3-4), 245–270. doi:10.1016/S0963-8687(02)00018-5

Bélanger, F., & Crossler, R. E. (2011). Privacy in the digital age: a review of information privacy research in information systems. *MIS Quarterly*, *35*(4), 1017–A36. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=67123613&site=ehost-live

Bellman, S., Johnson, E., Kobrin, S., & Lohse, G. (2004). International Differences in Information Privacy Concerns: A Global Survey of Consumers. *Information Society*, *20*(5), 313–324. Retrieved from http://search.proquest.com/docview/204835233?accountid=10218

Boehm, B. W. (1991). Software risk management: principles and practices. *IEEE Software*, *8*(1), 32–41. doi:10.1109/52.62930

Cespedes, F. V., & Smith, H. Jeff. (1993). Database Marketing: New Rules for Policy and Practice. *Sloan Management Review*, *34*(4), 7. Retrieved from http://search.proquest.com/docview/224960792?accountid=10218

Chen, K., & Rea, Alan I, Jr. (2004). Protecting personal information online: a survey of user privacy concerns and control techniques. *The Journal of Computer Information Systems*, *44*(4), 85–92. Retrieved from http://search.proquest.com/docview/232578985?accountid=10218

Chiung-wen Hsu. (2006). Privacy concerns, privacy practices and web site categories: Toward a situational paradigm. *Online Information Review*, *30*(5), 569–586. Retrieved from http://search.proquest.com/docview/194545060?accountid=10218

Culnan, M. J. (1993). "How Did They Get My Name?": An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use. *MIS Quarterly*, *17*(3), 341–363. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9404050726&site=ehost-live

Culnan, M. J. (1995). Consumer awareness of name removal procedures: Implications for direct marketing. *Journal of Direct Marketing*, *9*(2), 10–19. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9504061647&site=ehost-live

Culnan, M. J., & Armstrong, P. K. (1999). Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation. *Organization Science*, *10*(1), 104–115. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=2251838&site=ehost-live

Dehling, T., & Sunyaev, A. (2014). Secure provision of patient-centered health information technology services in public networks—leveraging security and privacy features provided by the German nationwide health information technology infrastructure. *Electronic Markets*, *Online First*. Retrieved from http://dx.doi.org/10.1007/s12525-013-0150-6

Derlega, V. J., Metts, S., Petronio, S., & Margulis, S. T. (1993). *Self-Disclosure*: Thousand Oaks, CA, US: Sage Publications, Inc.

Dinev, T., Bellotto, M., Hart, P., Russo, V., & et al. (2006). Internet Users' Privacy Concerns and Beliefs About Government Surveillance: An Exploratory Study of Differences Between Italy and the United States. *Journal of Global Information Management*, *14*(4), 57–93. Retrieved from http://search.proquest.com/docview/195151831?accountid=10218

Dinev, T., & Hart, P. (2006). An Extended Privacy Calculus Model for E-Commerce Transactions. *Information Systems Research*, *17*(1), 61–80. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=20410277&site=ehost-live

Etzioni, A. (2008). *The limits of privacy*: Basic Books.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior*, *25*(1), 153–160. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=34980171&site=ehost-live

Georgescu, M., & Suicimezov, N. (2012). Issues regarding security principles in Cloud Computing. *USV Annals of Economics & Public Administration*, *12*(2), 221–226. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=87522765&site=ehost-live

Graeff, T. R., & Harmon, S. (2002). Collecting and using personal data: consumers' awareness and concerns. *Journal of Consumer Marketing*, *19*(4), 302–318. doi:10.1108/07363760210433627

Heng Xu, Sumeet Gupta, Mary Beth Rosson, & John M. Carroll. Measuring mobile users' concerns for information privacy. In *Thirty Third International Conference on Information Systems* (pp. Xu, H., Gupta, S., Rosson, M.B., and Carroll, J.M. (2012). Measuring Mobile Users' Concerns For Information Privacy, Proceedings of 33rd Annual International Conference on Information Systems (ICIS), Orlando, Florida).

Hong, W., & Thong, James Y L. (2013). Internet Privacy Concerns: An Integrated Conceptualization and Four Empirical Studies. *MIS Quarterly*, *37*(1), 275. Retrieved from http://search.proquest.com/docview/1505012949?accountid=10218

Hwang, H.-G., Han, H.-E., Kuo, K.-M., & Liu, C.-F. (2012). The Differing Privacy Concerns Regarding Exchanging Electronic Medical Records of Internet Users in Taiwan. *Journal of Medical Systems*, *36*(6), 3783–3793. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=80729905&site=ehost-live

Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. Home is safer than the cloud!: privacy concerns for consumer cloud storage. In L. F. Cranor (Ed.), *the Seventh Symposium* (p. 1).

Janda, S., & Fair, L. L. (2004). Exploring Consumer Concerns Related to the Internet. *Journal of Internet Commerce*, *3*(1), 1. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=27651358&site=ehost-live

Kaufman, L. M. (2009). Data Security in the World of Cloud Computing. *IEEE Security & Privacy Magazine*, *7*(4), 61–64. doi:10.1109/MSP.2009.87

Kim Bartel Sheehan. (2002). Toward a typology of Internet users and online privacy concerns. *Information Society*, *18*(1), 21–32. Retrieved from http://search.proquest.com/docview/204831865?accountid=10218

Laric, M. V., Pitta, D. A., & Katsanis, L. P. (2009). Consumer concerns for healthcare information privacy: A comparison of US and canadian perspectives. *Research in Healthcare Financial Management*, *12*(1), 93–111.

Li, Y. (2011). Empirical Studies on Online Information Privacy Concerns: Literature Review and an Integrative Framework. *Communications of the Association for Information Systems*, *28*, 1. Retrieved from http://search.proquest.com/docview/885090323?accountid=10218

Malhotra, N. K., Sung S. Kim, & Agarwal, J. (2004). Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model. *Information Systems Research*, *15*(4), 336–355. Retrieved from

http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=15648475&site=ehost-live

Milne, G. R., & Boza, M.-E. (1999). Trust and concern in consumers' perceptions of marketing information management practices. *Journal of Interactive Marketing*, *13*(1), 5–24. Retrieved from http://search.proquest.com/docview/1010584378?accountid=10218

Moon, Y. (2000). Intimate Exchanges: Using Computers to Elicit Self-Disclosure from Consumers. *Journal of Consumer Research*, *26*(4), 323–339. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=3087029&site=ehost-live

Nowak, G. J., & Phelps, J. (1995). Direct Marketing and the Use of Individual-Level Consumer Information: Determining How and When "Privacy" Matters. *Journal of Direct Marketing*, *9*(3), 46–60. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9508104250&site=ehost-live

Peter, J. Paul, & Tarpey Sr, Lawrence X. (1975). A Comparative Analysis of Three Consumer Decisions Strategies. *Journal of Consumer Research*, *2*(1), 29–37. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=4656816&site=ehost-live

Phelps, J., Nowak, G., & Ferrell, E. (2000). Privacy concerns and consumer willingness to provide personal information. *Journal of Public Policy & Marketing*, *19*(1), 27–41. Retrieved from http://search.proquest.com/docview/211109288?accountid=10218

Prasad, A., Sorber, J., Stablein, T., Anthony, D., & Kotz, D. Understanding sharing preferences and behavior for mHealth devices. In T. Yu & N. Borisov (Eds.), *the 2012 ACM workshop* (p. 117).

Rindfleisch, T. C. (1997). Privacy, information technology, and health care. *Communications of the ACM*, *40*(8), 92–100. doi:10.1145/257874.257896

Rohm, A. J., & Milne, G. R. (2004). Just what the doctor ordered: The role of information sensitivity and trust in reducing medical information privacy concern. *Journal of Business Research*, *57*(9), 1000–1011. Retrieved from http://search.proquest.com/docview/196325699?accountid=10218

Rose, E. A. (2006). An examination of the concern for information privacy in the New Zealand regulatory context. *Information & Management*, *43*(3), 322–335. Retrieved from http://search.proquest.com/docview/237021592?accountid=10218

Smith, H. Jeff, Dinev, T., & Xu, H. (2011). Information Privacy Research: An Interdisciplinary review. *MIS Quarterly*, *35*(4), 980–A27. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=a9h&AN=67129829&site=ehost-live

Smith, H. Jeff, Milberg, S. J., & Burke, S. J. (1996). Information Privacy: Measuring Individuals' Concerns About Organizational Practices. *MIS Quarterly*, *20*(2), 167–196. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=9610124512&site=ehost-live

Subashini, S., & Kavitha, V. (2011). A survey on security issues in service delivery models of cloud computing. *Journal of Network & Computer Applications*, *34*(1), 1–11. Retrieved from

http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=55208487&site=ehost-live

Tolchinsky, P. D., McCuddy, M. K., Ganster, D. C., Adams, J., Woodman, R. W., & Fromkin, H. L. (1981). Employee Perceptions of Invasion of Privacy: A Field Simulation Experiment. *Journal of Applied Psychology*, *66*(3), 308–313. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=5101520&site=ehost-live

Tsai, J., Cranor, L. F., Acquisti, A., & Fong, C. M. (2008). What's It To You? A Survey of Online Privacy Concerns and Risks. *SSRN Working Paper Series*. Retrieved from http://search.proquest.com/docview/1322064681?accountid=10218

van Deursen, N., Buchanan, W. J., & Duff, A. (2013). Monitoring information security risks within health care. *Computers & Security*, *37*, 31–45. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=89432934&site=ehost-live

Warren, S. D., & Brandeis, L. D. (1890). The Right to Privacy. *Harvard Law Review*, *4*(5), 193. doi:10.2307/1321160

Wilson, D., & Valacich, J. S. Unpacking the Privacy Paradox: Irrational Decision-Making within the Privacy Calculus. Retrieved from http://dblp.uni-trier.de/db/conf/icis/icis2012.html#WilsonV12

Wirtz, J., Lwin, M. O., & Williams, J. D. (2007). Causes and consequences of consumer online privacy concern. *International Journal of Service Industry Management*, *18*(4), 326–348. Retrieved from http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=26533887&site=ehost-live

Xu, H., Dinev, T., Smith, H. J., & Hart, P. Examining the Formation of Individual's Information Privacy Concerns: Toward an Integrative View. In *Proceedings of 29th Annual International Conference on Information Systems (ICIS), Paris, France, 2008* (pp. 1–16). Retrieved from http://faculty.ist.psu.edu/xu/papers/conference/icis08a.pdf

Zukowski, T., & Brown, I. Examining the influence of demographic factors on internet users' information privacy concerns. In L. Barnard & R. A. Botha (Eds.), *the 2007 annual research conference of the South African institute of computer scientists and information technologists* (pp. 197–204).