



An Exploratory Study on Physicians' Diligence when Dealing with Patient Data

Journal:	<i>18th European Conference on Information Systems</i>
Manuscript ID:	ECIS2010-0204.R1
Submission Type:	Research Paper
Keyword:	Health informatics/health information systems/medical IS, Privacy/information privacy, Information security/privacy, E-health



AN EXPLORATORY STUDY ON PHYSICIANS' DILIGENCE WHEN DEALING WITH PATIENT DATA

Cornelia Kuckein, Zeppelin Baumaschinen GmbH, Graf-Zeppelin-Platz 1, 85748 Garching, Germany, cornelia.kuckein@gmx.de

Michael Schermann, Chair for Information Systems, Technische Universität München, Boltzmannstrasse 3, 85748 Garching, Germany, michael.schermann@in.tum.de

Ali Sunyaev, Chair for Information Systems, Technische Universität München, Boltzmannstrasse 3, 85748 Garching, Germany, sunyaev@in.tum.de

Helmut Krcmar, Chair for Information Systems, Technische Universität München, Boltzmannstrasse 3, 85748 Garching, krcmar@in.tum.de

Abstract

Recent history shows an increasing number of privacy breaches, usually attributed to a lack of diligence when handling personal data. Little awareness for privacy concerns is asserted as the pivotal negative effect on diligence. Challenging this conventional wisdom, this study shows that physicians are fully aware of the privacy issues. Their lack of diligence mainly results from a trade-off between the prospected consequences resulting from a privacy breach and the impediments diligent data handling has on the actual workflow of the physicians. Based on the grounded theory method, we chose hospitals as research field since patient data is commonly perceived as especially sensitive. We add to the body of knowledge by emphasizing the role of actors processing personal data in contrast to existing research that focuses on the behavior of affected actors, such as consumers. In sum, we provide a new perspective on the factors leading to privacy breaches.

Keywords: Privacy, Healthcare, Hospital, Patient Data, Workflow Impediments.

1 INTRODUCTION

The oldest and most widely cited definition of privacy is “the right to be let alone” (Warren and Brandeis, 1890). Westin (1967) broadens this definition to “the claim of individuals, groups, or institutions, to determine for themselves, when, how, and to what extent information about them is communicated to others”. This emphasizes two types of actors when defining privacy. Data subjects refer to actors identifiable by the data in question. Data handlers are individuals, groups, or institutions that process such data for a purpose. Data subjects and data handlers agree on a policy that defines boundaries of data processing, in particular the rights of the data handler to transfer data to other data handlers. Hence, privacy is the ability to control the acquisition and use of personal information (Hann et al., 2002; Regan, 1995; Rindfleisch, 1997).

Recent cases of privacy breaches have demonstrated risks associated with handling personal data. For example, in September 2004, ChoicePoint, a company offering identification and credential verification services had to report the theft of data records on more than 163,000 people (Shostack and Stewart, 2008). The thieves created accounts with ChoicePoint using stolen identities and collected data without alerting the internal control system of ChoicePoint. In May 2006, the U.S. Department of Veterans Affairs reported the theft of information allowing the identification of 26.5 million people. An employee had taken the data home when the media holding the information was stolen (United States Department of Veterans Affairs, 2006). Similar privacy breaches were reported worldwide. For instance, in 2008 personal data about customers of Deutsche Telekom in Germany were stolen and offered to data aggregation companies (Kuri, 2008).

As the examples show, lack of diligence by the employees entrusted with the processing of personal data seems to be the cause of the breaches. Usually, little awareness for privacy concerns is asserted as the pivotal diminutive effect on diligence. Hence, raising awareness for privacy concerns of employees entrusted with personal data, e.g. awareness trainings, is often suggested as the best approach to reduce the risk of privacy breaches (Siponen, 2001). However, the underlying factors, determining the level of diligence when handling personal data are largely unexplored (Siponen, 2001). Hence, our main research question is: *What are the factors that influence the diligence of data handlers when dealing with personal data?* In contrast to the existing research on privacy behavior, we particularly highlight the role of data handlers (see Figure 1).

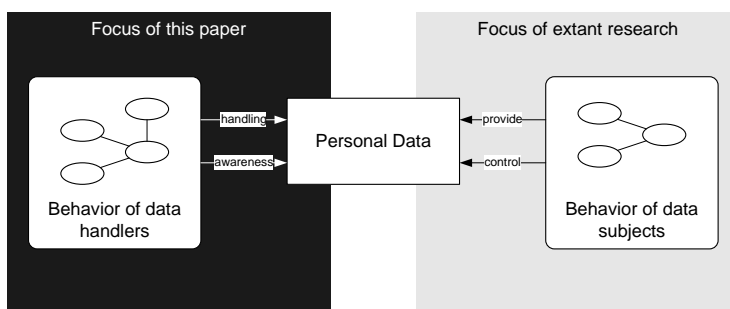


Figure 1. Focus of this paper.

The remainder of the paper is structured as follows. In the next section, we review the literature on the behavior of actors when handling and processing personal data. We show that little research is available on the role and behavior of data handlers. Next, we apply the grounded theory method to explore potential factors that are influencing the level of diligence of data handlers. We chose hospitals as research field, because patient-related data is commonly perceived as especially sensitive. An unintended disclosure of personal medical data can have severe negative consequences for a patient, ranging from social discrimination to economic consequences. The resulting theoretical model identifies four factors that influence the diligence of data handlers. Then, we discuss the implications of the theoretical model. Our study shows that the effort for maintaining a higher level of diligence

conflicts with the structure and constraints of the workflows. Following an analysis of limitations to our study, the final chapter summarizes the results and suggests future research topics.

In sum, our research contributes to the general debate concerning due diligence when working with patient data by emphasizing on the importance of the factors structuring the behavior of data handlers. Furthermore, we show that data handlers may have a high awareness of privacy concerns but fail to resolve the conflict of maintaining a high level of diligence within the structure and constraints of existing workflows.

2 LITERATURE REVIEW

To identify relevant research, journals in the field of privacy, security and healthcare issues of information systems were examined by a full-text electronic search on selected keywords like “privacy”, “diligence”, and “healthcare”. We used the following databases: Business Source Premier, Science direct, JSTOR archive, INSPEC. This search identified 477 articles. The titles and abstracts of each article were examined as to relevance for this research (i.e. the article appeared to be concerned with or relevant to the topics privacy and diligence). This process generated 241 articles for in-depth review. In an effort to broaden the search beyond the original set of journals, following a snowball sampling technique (Goodman, 1961), cited works of potential interest in those articles were analyzed which yielded an additional set of articles. In sum, 121 articles were considered as relevant.

Our review indicates that IS research on privacy focuses on three areas: technologies and controls that help to ensure privacy and data security, typologies based on the behavior of actors in privacy scenarios, and paradoxical behavior of actors in privacy scenarios. Here, we are interested in explaining the behavior of data handlers. Therefore, we omit discussing the literature on privacy-enhancing technology. We review the other two research streams in the following subsections.

2.1 Typologies of actors in privacy scenarios

There have been multiple attempts at defining the dimensions of actors’ privacy concerns. For instance, Smith et al. (1996) suggest four dimensions: collection, unauthorized (internal/external) secondary use, errors, and improper access. Their dimensions were empirically confirmed by Stewart and Segars (2002). Malhotra et al. (2004) refined it to consider new technologies, in particular the use of the internet. Their so-called Internet Users Information Privacy Concerns (IUIPC) scale has three dimensions: collection, control, and awareness of privacy practices. Other authors investigated antecedents of concerns or searched for factors that reduce actors’ concerns like empowerment (Dyke v. et al., 2007).

Actors can be grouped into clusters depending on their privacy-related attitudes and concerns. There are different approaches to grouping actors (see Table 1). Based on multiple surveys, Westin (1996) distinguished between privacy fundamentalists, privacy pragmatists, and privacy unconcerned, whereas Ackermann et al. (1999) named their groups privacy fundamentalists, pragmatic majority, and marginally concerned. Sheehan (2002) found unconcerned Internet users, circumspect Internet users, wary Internet users, and alarmed Internet users, whereas Hann et al. (2007) distinguished privacy guardians, information sellers, and convenience seekers.

Author	Clusters	Focus
(Westin, 1996)	privacy fundamentalists, privacy pragmatists, privacy unconcerned	Data subjects
(Ackerman et al., 1999)	privacy fundamentalists, pragmatic majority, marginally concerned	Data subjects
(Sheehan, 2002)	unconcerned users, circumspect users, wary users, alarmed users	Data subjects
(Hann et al., 2007)	privacy guardians, information sellers, convenience seekers	Data subjects

Table 1. Actor groups based on privacy-related attitudes and concerns.

As shown in Table 1, presented clusters provide the empirical foundation of privacy-related behavior of data subjects mostly with a focus on commercial transactions. However, Table 1 reveals as well that no similar work could be found for data handlers.

2.2 Paradoxical behavior of actors in privacy scenarios

Actors' stated privacy attitudes and actual behavior are often contradictory (Spiekermann et al., 2001; Weiland, 2006). For instance, there are consumers who claim to be concerned about their privacy, yet use loyalty cards when purchasing goods, thereby revealing a lot of personal information. Therefore, another field of research is concerned with explaining this "privacy paradox" (Norberg et al., 2007). There is no consensus on the reasons for actors' paradoxical behavior (see Table 2). Acquisti and Grossklags (2005) argue that actors' incomplete information and bounded rationality being the reason for paradox behavior, whereas O'Donoghue and Rabin (2000) attribute actors with a preference for immediate gratification, for instance, price reductions when using loyalty cards. This is corroborated by Weiland (2006) who assesses that actors tend to act in ways, which reduce their privacy because they are unable to anticipate the long-term consequences of disclosing personal information. Based on Laufer and Wolfe's (1977) concept of "privacy calculus", researcher argue that consumers tend to be willing to disclose personal information in case of a positive net outcome of a cost-benefit-estimation (Chellappa and Sin, 2005; Culnan and Bies, 2003; Dinev and Hart, 2006).

Author	Factors of paradoxical behavior	Focus
(O'Donoghue and Rabin, 2000)	preference for immediate gratification	Data subjects
(Acquisti and Grossklags, 2005)	incomplete information, bounded rationality	Data subjects
(Weiland, 2006)	unable to correctly estimate costs, benefits and long-term consequences	Data subjects
(Chellappa and Sin, 2005; Culnan and Bies, 2003; Dinev and Hart, 2006)	willing to disclose personal information in case of a positive net outcome of a cost-benefit-estimation: "privacy calculus" (Laufer and Wolfe, 1977)	Data subjects

Table 2. Arguments explaining paradoxical behavior of actors in privacy scenarios.

As Table 2 shows, again, no work could be found on the behavior of data handlers. However, the presented research reveals that the privacy-related behavior of actors is controlled by a trade-off between privacy and perceived benefits.

2.3 Research Gap

As we have argued above, few research results are available on the behavior of data handlers as the counterpart to data subjects. The little existing research focuses on topics such as how online retailers should formulate their privacy notices to positively influence consumer's trust (Tsai et al., 2007). In the health care domain, research focuses, e.g., on the adoption rate of Electronic Patient Records (EPR) in hospitals and subsequent changes in workflows (e.g. Ash and Bates, 2005; Hier et al., 2005). The work of Patel et al. (2000) was the only study found during our literature review that investigates how medical staff can be motivated to treat patient data confidentially. However, they focus on how to structure awareness trainings with medical personnel.

3 A GROUNDED THEORY STUDY ON PHYSICIANS' DILIGENCE

Based on the identified research gap, we conducted an exploratory study using the method of grounded theory as proposed by Corbin and Strauss (1990). We split our main research question into the following three study-specific questions: Which factors influence a physicians' diligence when dealing with sensitive patient data? What kind of influence does each factor have on the diligence? What relationship is there between the factors? In the following, we report on the methodological framework of our study.

3.1 Setting

To answer the research questions, an empirical qualitative study was conducted. The study was set up in the healthcare sector. As medical data is a very sensitive kind of personal data, it was found to be of special interest to analyze the handling of patient data by physicians (Win et al., 2006). There are various professions in the healthcare sector such as hospital physicians, general practitioners, nurses, pharmacists, etc. with each profession having its specific processes (Mouratidis et al., 2009). Therefore, the study focuses on hospital physicians to receive comparable data and consistent results. However, privacy-related positions in hospitals were investigated as well.

3.2 Participants

Ten people were interviewed for the study: six assistant physicians, all belonging to an age group of 30-40 years, two senior physicians, in an age group of 50-65 years, one Chief Information Security Officer and one director of a hospital data processing center, both in an age group of 50-65 years. The interviewees were chosen based on their willingness to participate in the study. Furthermore, they worked for different hospitals in Germany and belonged to different areas of expertise, including anesthesia, cardiology, gynecology, pediatrics, surgery, and urology.

3.3 Data Collection

The interviews were semi-structured and ranged from 53 minutes to 81 minutes. Three interviews were conducted in groups of two or three participants, while the other three were single interviews. An interview guideline was used in order to ensure that the same topics were covered in all interviews. However, the guideline was not followed in a strict order to allow for emerging topics. In addition, open-ended questions were asked to get the interviewees to phrase their answers freely. The interview guideline addressed the following topics: (1) use of EPR, (2) specific processes and workflows in hospital, (3) handling of passwords, personal computers, and patient records, (4) nature of physician-patient relationship, (5) physician confidentiality, and (6) consequences of privacy breaches. As privacy, confidentiality, and handling of passwords and patient data are rather sensitive topics, the participants were guaranteed anonymity in order to facilitate honest answers. Each interview started with a short introduction into the study topic. However, there was no detailed information about the specific aspects of the study so as not to influence participants' answers. With consent of the participants, all interviews were recorded. After each interview, the recorded data was transcribed and analyzed. The results were integrated into the next interview as it is required by the grounded theory method (Corbin and Strauss, 1990). Thus, relevant topics could be identified and incorporated into following interviews.

3.4 Data Analysis

The process of grounded theory analysis is iterative and consists of three specific phases: Open Coding, Axial Coding, and Selective Coding (Corbin and Strauss, 1990). Through increasing levels of abstract classification, a theoretical model is hereby developed from empirical data. During Open Coding, the interview is analyzed line by line by searching for discrete topics and events in the verbatim descriptions. Similar descriptions are grouped under a conceptual label. Related concepts are then merged into categories, which are more abstract. This reduces the number of units to work with and helps to structure the data and construct a model (Strauss and Corbin, 1996). The emerging categories are defined regarding their properties and dimensions. During Axial Coding, the relationships between the categories are explored. In Selective Coding, a theoretical model is constructed by relating the categories to the core category and to one another. In this study, the core category "physicians' diligence when dealing with patient data" was defined in advance by the research gap.

Open Coding

First, 13 concepts were identified (see Table 3). Following the coding by the first author, a person initially not involved with the here presented research likewise coded the transcripts. The comparison of the two codings revealed that 10 concepts of the 13 concepts were applied identically. With regard to the other three concepts, both coders and the others authors analyzed the codings and resolved the mismatches, which were always based on obvious reasons (e.g. the second coder had simply forgotten to code a statement).

No.	Concept	Category
(1)	Discreet and confidential data handling	Awareness regarding interactive confidentiality
(2)	Internalized physician confidentiality	
(3)	Mutual trust	
(4)	Responsibility	
(5)	Disturbance of workflow	Impediment of workflow
(6)	Handling of passwords	
(7)	Practicability	
(8)	Time	
(9)	Handling of patient records	
(10)	Problems with handling computers	
(11)	Insufficient knowledge of consequences	Awareness regarding consequences
(12)	Deterrence	Perceived probability of data abuse
(13)	Personal estimation	

Table 3. *Concepts and Corresponding Categories*

Second, the concepts were then merged into four abstract categories. The concepts “discreet and confidential data handling”, “internalized physician confidentiality”, “mutual trust”, and “responsibility” were merged into the category “awareness regarding interactive confidentiality”. The incidents described in this category indicate that physicians are aware of their obligation to handle patient data confidentially and that they have internalized this duty during their medical training. Therefore, they do not need to think about it actively in their daily work. For instance, this shows in their practice of not talking about patients in front of unauthorized persons. The patient-physician relationship is described to be very important and valuable. The patients trust in the physicians’ discretion when telling them about their medical condition. This imposes responsibility on the physician to handle this sensitive information appropriately.

The second category, “impediment of workflow”, consists of the concepts “disturbance of workflow”, “handling of passwords”, “practicability”, “time”, “handling of patient records”, and “problems with handling computers”. The events described in this category indicate that privacy and security measures such as individual accounts with different access rights and logins with passwords hamper physicians’ work are seen as very time-consuming. Therefore, the majority of physicians share their password with their colleagues by telling them or by pinning it on the workstation’s monitor. Reported incidents show that trade-offs are made in favor of time saving or convenience. For instance, some physicians do not log out of the system at all, thereby allowing colleagues to work under their account name. Generally, time is an important issue in hospital workflows. Physicians have to do several tasks at once and look after a high number of patients in little time. In addition, technological equipment plays an important role: physicians reported about old hardware that is slow and unreliable, which hampers their work. Due to high time pressure, interviewees reported about taking patient records home to continue work outside of the hospital. Although such behavior is officially prohibited, it is tolerated – and sometimes even expected – by chief physicians. The last concept, which adds to an impediment of workflow, consists of older physicians having problems with the handling of computers and programs. For instance, typing takes a lot of time, which hinders their work.

The third category named “awareness regarding consequences” was obtained by merging the concepts of “insufficient knowledge of consequences” and “deterrence”. The incidents described in this

category indicate that physicians are unaware of the consequences of privacy breaches, both consequences for themselves, for instance, fines or lawsuit, and consequences for the patient. They can imagine that there is a public interest in patient information of well-known public figures such as celebrities and politicians. However, they do not know that there are companies who have an economic interest in acquiring medical data from “normal” persons, as well. If those consequences would be known, physicians claim to be more motivated to handle the data more carefully.

The fourth category identified was “perceived probability of data abuse”. It was built from the concept “personal estimation”. Physicians report to rely on personal estimation if people are credible. For instance, if a person claims on the phone to be a patient’s relative they rely on their intuition whether giving information about the patient’s condition or not. Furthermore, they reported to willingly take the risk of letting other physicians work under their account and of leaving patient records accessible. For instance, they assess a low risk when letting the trolley with patient records standing unattended on the corridor, thinking that others have no interest in reading them because they would not understand the medical notes.

Axial Coding and Selective Coding

Next, we developed a model by exploring the relationships between the categories and their influence on the predefined core category. With regard to our research interest, the core category is “diligence while dealing with patient data”. Based on the open coding, four categories or factors were identified that influence the core category. These are: (1) awareness regarding interactive confidentiality, (2) awareness regarding consequences of a privacy violation, (3) estimated probability of data abuse, and (4) impediment of workflow caused by privacy measures. The first three factors have an enhancing effect on the core category. This means that, *ceteris paribus*, the higher the factor, the higher the level of diligence:

- the higher the awareness regarding interactive confidentiality, the higher the diligence when dealing with patient data,
- the higher the awareness regarding consequences, the higher the diligence when dealing with patient data,
- the higher the perceived probability of data misuse, the higher the diligence when dealing with patient data.

The fourth factor, impediment of workflow, has a diminishing effect on the core category, which means that:

- the higher the impediment of workflow, the lower the diligence when dealing with patient data.

In addition, two of the categories are related to one another. The “perceived probability of data misuse” depends on the “awareness regarding consequences”. Thus, changes in the awareness regarding the consequences of a privacy violation cause a different estimation of probability of data misuse. For instance, if physicians would have better knowledge about the economic interest of some pharmaceutical organizations in patient data, it would influence their estimated probability of a person trying to get access to patient records. Hence, they would take better care and would not leave the trolley with patient records unattended.

3.5 Theoretical Model

The resulting model of our study is shown in Figure 2. The factors have different weightings in their influence on the core category. Thus, a factor with a higher weighting can outweigh the influence of another factor with a lower weighting. The resulting level of diligence is a function of all weighted factors. In the following discussion, we will apply the model to explain privacy-related situations in the daily routine of hospital physicians as reported in the interviews.

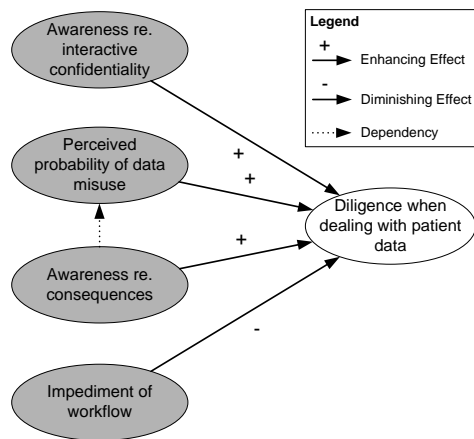


Figure 2. Theoretical model.

4 DISCUSSION

In the following, we analyze the implications of the theoretical model. However, we first discuss the major limitations of our study to establish the context for interpreting the results. However, we show in the discussion of the theoretical model that this awareness is applicable to patient-physician interactions only.

4.1 Limitations

As the study was conducted in the healthcare domain, the results cannot be generalized and there are some limitations to the use of the results. Firstly, the study focuses on physicians working in a hospital. It needs to be researched whether some factors have different effects on the diligence when applying the model to general practitioners and other professions in the healthcare sector. For instance, given the long-term nature of patient-physician relationships in a practice it could be tested if the concepts of relationship and trust play a bigger role than in a hospital setting. If this were the case, it could result in a higher influence of the factor “awareness regarding confidentiality” on physicians’ diligence with patient data. In addition, the majority of physicians that were interviewed were assistant physicians between the ages of 30 and 40. Therefore, this study does not give insight into the influence of age and work experience on physicians’ diligence with handling patient data. Further research is necessary to substantiate our exploratory results.

4.2 Characteristics of the Categories in Practice and Resulting Level of Diligence

As described above, the four factors have an enhancing and respectively diminishing effect on the core category. The resulting diligence can range from low to high. In the interviews, a medium reported level of diligence could be observed. This results from the characteristics of the four factors as they occur in the daily work of the interviewees. The following quotes were translated from German to English by the authors.

The physicians reported to have a high level of awareness regarding interactive confidentiality. They know that they are obliged to treat patient data confidentially. However, in their daily work, they show two differing behaviors. In direct patient contact, on the telephone, or when conferring with colleagues, they pay heed to the fact that unauthorized persons may not overhear the conversation. Yet at the same time, they leave patient records unattended and pin their passwords onto workstations:

“You just do not use patient names when discussing their condition and therapy for instance with colleagues. “

„Actually, the trolley with the patient records must not be left unsupervised during ward round. However, for practical reasons the trolley is usually left unattended in the hallway. “

This leads to the conclusion that the physician-patient relationship becomes more abstract when there is a medium in between, such as an electronic or a paper-based record. Physicians tend to think that technical security of patient data is not their responsibility but that of the IT department. In sum, this leads to a medium level of awareness regarding confidentiality.

In the interviews, physicians reported that the impediment of workflow caused by privacy measures is perceived to be high. With a high pressure of time in their daily work, they are motivated to save time wherever possible. Hence, they bypass time-consuming security measures such as personal passwords and role-based access rights:

“Keeping passwords secret is impractical. You simply need various types of access during the day. Anything else would make work really difficult.”

“Passwords are nonsense.”

“The problem is that at least 80 percent of my colleagues do not have any computer skills. They are just happy, when they somehow could enter their data.”

In addition, many older physicians have problems with handling computer programs. This is partly the result of a lack in training, but also of a low level of acceptance of IT systems from people belonging to that age group. The level of impediment of workflow is therefore high.

In the interviews, it became apparent that the awareness regarding consequences of medical data disclosure is very low. Physicians have little knowledge about financial or legal consequences for their actions. Although they are well aware that consequences exist, they do not have an interest in learning more about the consequences. In fact, they push it aside and convince themselves that it is very unlikely that they will be facing such a situation themselves:

“Of course, you know there are consequences – theoretically. But, I do not know of any actual incidents.”

As for the consequences of data disclosure for patients, they have little knowledge of the monetary value of patient data. Apart from data of well-known public figures, they do not think anyone would be interested in acquiring medical data of their patients. This may be because the study was conducted in Germany, where there have not yet been any scandals of companies buying personal medical data as has been the case in the US (Lo and Alpers, 2000).

Due to its relation to the category “awareness of consequences”, the probability of data misuse is also estimated to be very low unless the patient is a well-known public figure. Frequently, physicians are aware that they are putting the confidentiality of patients’ records at risk, for instance, when leaving the records unattended or when pinning the password onto the workstation. However, as they assume that nobody is interested in the records, they are deliberately taking that risk:

“When someone steals a single patient record ... I do not think that the employer is interested in the data. How should the employer become aware of this? I think it gets critical, when a lot of records get stolen.”

In addition, they presume that no outsider would be able to understand the medical data and abbreviations contained in the records.

Overall, the level of diligence that results from a medium awareness regarding confidentiality, a high level of impediment of workflow, a low level of awareness regarding consequences and a low estimated probability of data misuse is medium. However, it became evident that the diligence of physicians in hospitals has two aspects: there is a high level of diligence in direct communication, with physicians ensuring that unauthorized people cannot overhear conversations with or about a patient.

However, as soon as there is a medium in between, such as an electronic patient record or a paper-based record, the relation becomes more abstract and the diligence is lower:

“It is not a patient anymore, just a stack of paper or a file in the computer”

In sum, our study shows that physicians are fully aware of their actions in face-to-face interactions. The lack of diligence is the result of a trade-off between potential privacy issues, prospected consequences resulting from a privacy breach, and the impediments diligent data handling has on the actual workflow of the employees. We show that the use of technology abstract from patient-physician relationships. Subsequently, handling patients' data and ensuring their privacy is seen as part of the administrative workflows.

4.3 Implications for Theory

This study provides initial insights on the role of data handlers in privacy-related situations. The model can be applied as an exploratory attempt to explain incidents of careless data handling or unintended data disclosure that arise in practice. For instance, interviewees reported leaving the trolley with patient records unattended in the corridor. This can be explained using the model: as there is no direct patient contact and only the paper-based patient record, the awareness regarding interactive confidentiality is lower. In addition, the awareness regarding consequences and the perceived probability of misuse are low because the physicians do not think anyone would be interested in the records. At the same time, the perceived impediment of workflow is very high as it is inconvenient and time-consuming to maneuver the trolley into the rooms while doing rounds in the ward. All of this results in a low level of diligence, leading to the trolley being left unattended in the corridor. Here, our results need to be augmented with a psychological perspective as well as with an ergonomic perspective. Furthermore, our study shows the importance of information technology in physicians' diligence in privacy-related situations. Data handling and data processing is decoupled from the patient-physician-relationship resulting in a low level of diligence. We argue that design-oriented research on hospital information systems in particular should suggest means to transfer the patient-physician relationship into interactions with information systems.

4.4 Implications for Practice

The impediment of workflows plays a pivotal role in the hospital setting. The impediment can be a result of organizational or technical factors. In many cases, these cannot be influenced by the physicians themselves but are predetermined by workflow-design or budget allotment. There are structural as well as financial boundaries that are hard to overcome. However, knowing about the causes is the first step to improving the situation. It could already help to integrate physicians into the design of hospital information systems and workflows. This would facilitate systems adapted to meet the specific requirements that exist in a hospital setting. Technical solutions such as account-based logins that are apt for clerks and other office professions may not be convenient for hospital workflows. Instead, contact-free identification with RFID (Radio Frequency Identification) or other technologies could be more suitable.

In order to close physicians' knowledge gap about possible consequences of data disclosure, the data protection officer could inform them about current incidents and legal consequences. Another simple, but effective way would be reminders in form of memos or screensaver notices. To raise the level of awareness regarding confidentiality of patient records, physicians should be informed about the commercial usability of patient records and about similar incidents in other countries or industries. Physicians should be aware that they are also responsible for the security of stored patient data, because technical solutions can only be efficient if they are used correctly by all users.

Due to the interdependency of the two categories, a raised level of awareness regarding consequences would lead to a more realistic estimation of the probability of data misuse. If physicians are aware of the interest of certain organizations in patient records, they will be more careful with those records.

5 CONCLUSION AND FURTHER RESEARCH

Our research provides a first theoretical lens on the role of data handlers in privacy-related situations. Since patient data is commonly perceived as especially sensitive since an unintended disclosure of personal medical data can have severe negative consequences for a patient, we chose workflows in hospitals as our research field. Based on the ground research method we developed a theoretical model containing factors that structure the level of diligence in privacy-related situations. In particular, we show that the impediments of diligent data handling on the actual workflow of the employees have a pivotal influence on the level of diligence. This raises important questions for both behavioral and design-oriented research in Information Systems. For instance, the physicians' trade-off between patient privacy and workflow impediments needs to be taken into account when designing new healthcare information systems. Furthermore, the importance of information technology in physicians' diligence in privacy-related situations raises issues for both organizational design and information systems design.

There are various limitations to take into account. In particular, we interviewed hospital physicians only. Although the use of technology in private practices is likely to have a similar abstracting effect, we will replicate the study with physicians in private practices as well as nursing staff. Furthermore, we will employ a quantitative approach to triangulate the model. In addition, further research on the model in other areas is necessary to show that it is applicable in other domains than the healthcare sector. Given the recent cases of privacy breaches in the business sector, it would be interesting to test the model's applicability to domains such as the telecommunications industry.

References

- Ackerman, M. S., Cranor, L. F. and Reagle, J. (1999) *Privacy in E-Commerce: Examining User Scenarios and Privacy Preferences*, 1st ACM conference on Electronic commerce, Denver, CO, USA.
- Acquisti, A. and Grossklags, J. (2005) *Privacy and rationality in decision making*, IEEE Security and Privacy, 3 (1), pp. 24-30.
- Ash, J. S. and Bates, D. W. (2005) *Factors and Forces Affecting EHR System Adoption*, Journal of the American Medical Association, 12 8-12.
- Chellappa, R. K. and Sin, R. G. (2005) *Personalization versus Privacy: An Empirical Examination of the Online Consumer's Dilemma*, Information Technology and Management, 6 (3), pp. 181-202.
- Corbin, J. and Strauss, A. L. (1990) *Grounded Theory Research: Procedures, Canons, and Evaluation Criteria*, Qualitative Sociology, 13 (1), pp. 3-21.
- Culnan, M. J. and Bies, R. J. (2003) *Consumer Privacy: Balancing Economic and Justice Considerations*, Journal of Social Issues, 59 (2), pp. 323-342.
- Dinev, T. and Hart, P. (2006) *An Extended Privacy Calculus Model for E-Commerce Transactions*, Information Systems Research, 17 (1), pp. 61-80.
- Dyke v., T. P., Midha, V. and Nemati, H. (2007) *The Effect of Consumer Privacy Empowerment on Trust and Privacy Concerns in E-Commerce*, Electronic Markets, 17 (1), pp. 68-81.
- Goodman, L. A. (1961) *Snowball Sampling*, Annals of Mathematical Statistics, 32 (1), pp. 148-170.
- Hann, I., Hui, K., Tom Lee, S. and Png, I. P. L. (2002) *Online Information Privacy: Measuring the cost-benefit trade-off*, Twenty-Third International Conference on Information Systems.
- Hann, I., Hui, K., Tom Lee, S. and Png, I. P. L. (2007) *Overcoming Online Information Privacy Concerns: An Information-Processing Theory Approach*, Journal of Management Information Systems, 24 (2), pp. 13-42.
- Hier, D. B., Rothschild, A., LeMaistre, A. and Keeler, J. (2005) *Differing faculty and housestaff acceptance of an electronic health record*, International Journal of Medical Informatics, 74 (7), pp. 657-662.

- Kuri, J. (2008) *Skandal um illegalen Datenhandel: Auch Telekom-Kunden betroffen*, <http://www.heise.de/newsticker/Skandal-um-illegalen-Datenhandel-Auch-Telekom-Kunden-betroffen--/meldung/114444>, Accessed at November 25, 2008.
- Laufer, R. S. and Wolfe, M. (1977) *Privacy as a Concept and a Social Issue: A Multidimensional Developmental Theory*, *Journal of Social Issues*, 33 (3), pp. 22-41.
- Lo, B. and Alpers, A. (2000) *Uses and abuses of prescription drug information in pharmacy benefits management programs*, *Journal of the American Medical Association*, 238 (6), pp. 801-806.
- Malhotra, N. K., Kim, S. S. and Agarwal, J. (2004) *Internet Users' Information Privacy Concerns (IUIPC): The Construct, the Scale, and a Causal Model*, *Information Systems Research*, 15 (4), pp. 336-355.
- Mouratidis, H., Sunyaev, A. and Jürjens, J. (2009) *Secure Information Systems Engineering: Experiences and Lessons Learned from Two Health Care Projects* In *Advanced Information Systems Engineering*(Eds, van Eck, P., Gordijn, J. and Wieringa, R.) Springer, Berlin, pp. 231-245.
- Norberg, P. A., Horne, D. R. and Horne, D. A. (2007) *The Privacy Paradox: Personal Information Disclosure Intentions Versus Behaviors*, *The Journal of Consumer Affairs*, 41 (1), pp. 100-126.
- O'Donoghue, T. and Rabin, M. (2000) *The Economics of Immediate Gratification*, *Journal of Behavioral Decision Making*, 13 233-250.
- Patel, V. L., Arocha, J. F. and Shortliffe, E. H. (2000) *Cognitive models in training health professionals to protect patients' confidential information*, *International Journal of Medical Informatics*, 60 143-150.
- Regan, P. M. (1995) *Legislating privacy*, University of North Carolina Press, Chapel Hill and London, England.
- Rindfleisch, T. C. (1997) *Privacy, Information Technology, and Health Care*, *Communications of the ACM*, 40 (8), pp. 92-100.
- Sheehan, K. B. (2002) *Toward a Typology of Internet Users and Online Privacy Concerns*, *The Information Society*, 18 21-32.
- Shostack, A. and Stewart, A. (2008) *The New School of Information Security*, Addison-Wesley, Upper Saddle River, NJ, USA.
- Siponen, M. T. (2001) *Five dimensions of information security awareness*, *ACM SIGCAS Computers and Society*, 31 (2), pp. 24-29.
- Smith, H. J., Milberg, S. J. and Burke, S. J. (1996) *Information Privacy: Measuring Individuals' Concerns About Organizational Practices*, *MIS Quarterly*, 20 (2), pp. 167-196.
- Spiekermann, S., Grossklags, J. and Berendt, B. (2001) *E-privacy in 2nd Generation E-Commerce: Privacy Preferences versus Actual Behavior*, *Proceedings of the 3rd ACM conference on Electronic Commerce*.
- Stewart, K. A. and Segars, A. H. (2002) *An empirical examination of the concern for information privacy instrument*, *Research*, 13 (1), pp. 36-49.
- Strauss, A. L. and Corbin, J. (1996) *Grounded Theory: Grundlagen Qualitativer Sozialforschung*, Psychologie Verlags Union, Weinheim, Germany.
- Tsai, J., Egelman, S., Cranor, L. and Acquisti, A. (2007) *The Effect of Online Privacy Information on Purchasing Behavior: An Experimental Study*, *The 6th Workshop on the Economics of Information Security (WEIS)*, Pittsburgh, PA, USA, pp. 1-33.
- United States Department of Veterans Affairs (2006) *Untitled announcement published in May 2006 warning of the theft of electronic data*.
- Warren, S. D. and Brandeis, L. D. (1890) *The Right to Privacy*, *Harvard Law Review*, 4 (5), pp.
- Weiland, M. (2006) *Economics and Privacy: A Survey of Research on "Economics and Privacy" and "Incentives and Privacy"*, Dresden University of Technology, Dresden, Germany.
- Westin, A. F. (1967) *Privacy and Freedom*, Atheneum, New York, NY, USA.
- Westin, A. F. (1996) *The 1996 Harris-Equifax Consumer Privacy Survey*, Equifax Inc., Atlanta, USA.
- Win, K. T., Susilo, W. and Mu, Y. (2006) *Personal Health Record Systems and Their Security Protection*, *Journal of Medical Systems*, 30 309-315.