Pre-print of Åhlfeldt, R.-M. & Huvila, I. Patient Safety and Patient Privacy When Patient Reading Their Medical Records. In Saranto, K.; Castrén, M.; Kuusela, T.; Hyrynsalmi, S. & Ojala, S. *(Eds.) Safe and Secure Cities : 5th International Conference on Well-Being in the Information Society, WIS 2014. Turku, Finland, August 18-20, 2014, Proceedings, Springer,* 2014, 230-239.

Patient Safety and Patient Privacy when patient reading their medical records

Rose-Mharie Åhlfeldt

School of Informatics, University of Skövde
Box 208, SE 541 08 SKÖVDE
+46500-44 86 28
rose-mharie.ahlfeldt@his.se

Isto Huvila

Department of ALM, Uppsala University
Box 625, SE 571 26 UPPSALA
+46 18-471 22 17
isto.huvila@alm.uu.se

Abstract. When patients get access to their personal health information new security demands arise. This paper presents results from a study aiming to improve the understanding of how the patients' different perceptions of their own personal health and health information preferences can be linked to anticipated positive and negative security concerns. The analysis and discussion focuses on investigating how the security issues and patients' perception on the benefits and threats of accessing their medical records relate to each other. The results show that a more holistic systemic perspective to information security is needed to support the effective use of medical records in the healthcare in information and data driven society in order to improve both patient safety and patient privacy.

Keywords: information society, information security, patient safety, patient privacy, well-being.

1 Introduction

In healthcare, patient information is a critical factor. The right information at the right time is necessary for providing the best and safest possible care for patients. Patient information must also be protected from unauthorized access in order to protect patient privacy. The healthcare sector faces a great challenge concerning how

patient information security can be managed in healthcare in order to achieve both patient safety and patient privacy for the citizens [1,2,3,4]. In the contemporary information society, patients are also interested in taking part of their patient information and are involved in their care. Residents, patients and relatives can participate actively in the care on their own terms and achieve public and personal health information, treatment and care [5]. Better access to own patient information and becoming more involved in care, raises also questions of the impact of these developments on patient safety and patient privacy [4].

Even if information security research has clearly demonstrated that security, safety and privacy are complex intertwined phenomena, the earlier literature has had a tendency to discuss privacy as a separate issue and not as a part of the concept of information security [6]. "Information security and privacy" is an often-mentioned term in the research literature. One particular reason for this is that information security is often conceptualised solely from the perspective of organizational goals while the notion of privacy tends to place more emphasis on individuals and, from an organizational point of view, on "customers" instead of the organization [7]. Information security controls are primarily based on the aims and objectives of the organization. However, even if the notion of security is closer to the organisational agenda, in most of the legal contexts, privacy is a statutory obligation organizations need to address as well. There is a risk that privacy is regarded more as a complementary than an inclusive part of the security arrangements and policies. Furthermore, a specific aspect of this problem in healthcare is that it is not unusual that patient privacy issues may be weighed against patient safety. In these cases it can be difficult to find a balance between the two [2], [4]. To bridge the gap between organizational objectives and privacy concerns and to obtain a high level of information security, it is necessary to incorporate the overlying goal of healthcare – good quality of care – and privacy aspects as integral parts of a holistic information security work in the organization [4].

Another gap in the earlier research is that safety and privacy related studies on information security are mainly dealing with the technical aspects of the issues[6]. Other aspects of information security work related to, for instance, management and the administration, have been largely omitted in the earlier work. In the context of healthcare, when patients get access to their patient information digitally, for example, by accessing their own medical records, health records or other types of public e-health services, the need for a holistic perspective of the information security work (including safety and privacy as well as technical and administrative aspects) increases [4].

The aim of this study is to improve the understanding of how the patients' different perceptions of their own personal health and health information preferences can be linked to anticipated positive and negative security concerns. The study is based on a survey of patients (N=254) who had ordered a paper copy of their medical record from a Swedish county council according to the legislation that allows all citizens to access information on themselves held by public bodies. The analysis and discussion focuses on investigating how the security issues and patients' perception on the benefits and threats of accessing their medical records relate to each other. The analytical framework is derived from the model of information security characteristics [1]: confidentiality, integrity, availability (CIA) and accountability. The findings are discussed in relation to the concepts patient safety and patient privacy.

2 Background

2.1 Information security in healthcare: safety and privacy

According to the European Health Strategy [1], the aim of healthcare is to provide citizens with good health while respecting the dignity and equal worth of every individual. Hence, the care providers should provide patients with opportunities for the best care and

[1], European Commission (2007). *Together for Health: A strategic Approach for the EU 2008 - 2013*. Brussels: Retrieved from http://ec.europa.eu/health-eu/doc/whitepaper_en.pdf.

ensure that care decisions are based on the right information at the right time. They should make every effort to obtain as high level of *patient safety* as possible. Lack of information should not lead to incorrect treatments or unnecessary interventions, such as unneeded visits to the doctor only because patient information from a one healthcare provider is unavailable with another organisation. On the other hand, sensitive patient information must be protected from being distributed to unauthorized persons, that is, one should strive to maintain *patient privacy*. [5].

In order to empower the patient, it is necessary to give patient access to their personal health information. Patients are no longer passive receivers of healthcare services. Instead they will become active players in the management of their own health [8].

2.2 Patient Safety

The Swedish Patient Safety Act[2] defines patient safety as a safeguard against medical injury. Medical injury is defined as affliction, malaise, physical or mental injury, illness or death caused by healthcare and not an inevitable consequence of the patient's condition. The definition is similar to that of WHO Europe [9]: prevention of errors and adverse effects to patients associated with healthcare. It is obvious that patient safety is closely related to patient information. In order to be able to suggest solutions for improving patient safety and increasing the quality of care, it is necessary to secure the management of patient information. In the Swedish context, under the principle that all citizens should be provided access to the information on themselves held by public bodies, a part of this process is to provide patients with a means to get an oversight of their personal medical information. Besides the democracy-related benefits of this oversight, when patients get access to their own information, they get an opportunity to become more knowledgeable of their health and more involved in their own care. The increased informedness has a capability to lead to improved health outcomes and, in long term, also improve patient safety[8].

[2] SFS 2010:659 *The Patient Safety Act*. Available from http://www.notisum.se/rnp/sls/fakta/a0100659.htm

2.3 Patient Privacy

In contrast to patient safety, there is no similar consensus of the definition of patient privacy. The notion of privacy is highly complex and tends to involve different perspectives and dimensions. As a consequence, there is no single universal definition of *privacy* [10]. In general, privacy has been defined as the right to be free from secret surveillance and to determine whether, when, how, and to whom, one's personal or organizational information is to be revealed [11]. The Swedish Patient Data Act[3] states, "the healthcare record must be designed with respect to the patient's integrity". According to the regulation SOSFS 2008:14[4], this is self-evident. Patient information is sensitive and must be protected from unauthorized access for the respect of patients and to achieve trustworthiness in healthcare. When patients get access to their personal health information, new privacy issues may arise. Patient information is not only transferred and communicated inside the healthcare systems. New risks, including both technical and administrational security threats, arise when patient information is transferred outside health organisations [12].

2.4 The Information Security Model

The conclusion of the discussion so far is that patient safety and patient privacy are closely related to patient information and consequently, also to information security. Using the information security model of Åhlfeldt [2], [13], the different information security related requirements of patient information can be mapped to four major aspects (characteristics) of information security (Fig. 1). In order to achieve patient safety, the right patient information (in-

[3] SFS 2010:659 *The Patient Data Act*. Available from http://www.riksdagen.se/sv/Dokument-Lagar/Lagar/Svenskforfattningssamling/Patientdatalag-2008355_sfs-2008-355/?bet=2008:355

[4] SOSFS 2008:14 Socialstyrelsens föreskrifter om informationshantering och journalföring i hälso- och sjukvården. Available from http://www.socialstyrelsen.se/sosfs/2008-14. (In Swedish)

tegrity) at the right time (availability) is needed. Similarly, in order to achieve patient privacy, only the right person (confidentiality and accountability) should have access to patient information. The premises of the model and the relation of patient safety and patient privacy, and information security are discussed in more detail in [2] (c.f. Fig 1).

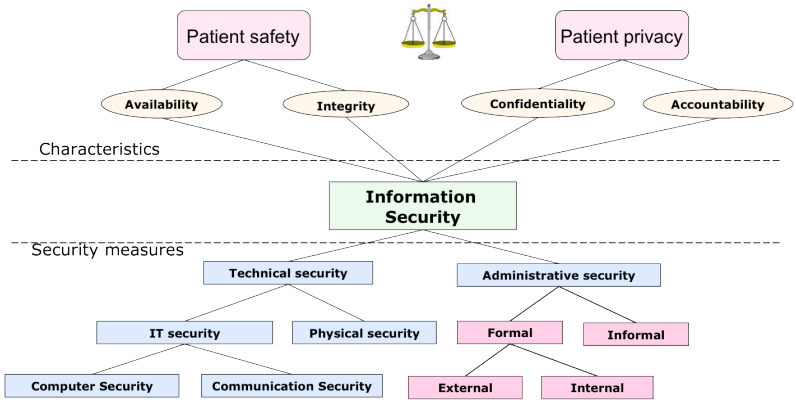

Fig. 1. Information Security Model related to patient safety and patient privacy [2].

However, even if the premise of information security is to achieve high levels of availability, integrity, confidentiality and accountability, it should be noted that these connections are not absolute. There are cases when confidentiality and accountability need to be emphasised in order to achieve patient safety, and vice versa. What is necessary is to find a balance between patient safety and patient privacy. A sufficient level of information security is a sum of all of its main characteristics.

In addition to explicating the relation of information security and patient safety and privacy, the information security model emphasizes the importance of both technical and administrative security measures in achieving a comprehensive level of information security. The lower part of the model presents information security measures organized in a hierarchical order [2]. Since the notion of "information security" is an amalgam of several types of security

measures, the model is useful as a basis for achieving a conceptual understanding of its constituent elements.

3 Material and methods

In order to investigate the safety and privacy aspects of accessing medical records and using e-health services, patient attitudes were investigated using a combined postal and web survey sent to 1000 patients living in a Swedish county that had ordered a paper copy of their medical record in June-August 2012. The aim of the survey was to investigate patient attitudes to reading their medical records to form a baseline before the implementation of a new online access system as a complement of an earlier paper-based model. Response rate was 35,4% (N=354). An invitation to participate in the study and a survey form was mailed to the respondents in the same envelope as a copy of their record. Respondents were also offered the possibility to fill in the survey online. The county council administered the mailing of the survey forms and the online survey. All responses were completely anonymous. No identifying personal data was collected.

The survey instrument consisted of 39 questions. Eight of them (consisted of 53 statements on 5-point Likert-like scale) were analysed using exploratory factor analysis (EFA) in SPSS 21.0. The questions explored 1) the reasons of ordering a copy of the medical record, 2) self-perceived understanding of the content of the medical record, 3) what type of help the patients preferred if they did not understand something in the record, 4) meaning/significance of reading medical records, 5) views of a potential online access service to medical records, 6) interest in future e-health services, 7) health condition and 8) health information behaviour. The survey questionnaire was constructed on the basis of earlier questionnaires [14,15] and complemented with additional questions developed by the researchers on the basis of their expertise and the specific research questions of this study.

4 Results

Seven factors emerged in the exploratory factor analysis (Table 1). The factors were interpreted as attitudes related to health services and medical records. The ranking order of the factors provides additional information about their relative strength (one being the strongest). A detailed description of the whole analysis and results are published in [16]. The means for the directly security related questions "I am generally worried of the security of the service"(mean 3.06, sd 1.451) and "I am worried that the medical records are not managed securely enough in the healthcare information systems if they can be read online" (mean 3.18, sd 1.422) were not especially high.

Table 1. Results of the factor analysis (EFA).

Factor	Description
P1	Hypothetically positive to e-health services generally
P2	Positive to reading medical records due to implications
P3	Positive to all Internet use including medical records online
P4	Distrustful and wants to be in control of health treatment
P5	Worried about health
P6	Wants communication with healthcare professionals
P7	Does not understand their medical record

The first factor is noted, P1, "Hypothetically positive to e-health services generally", since the variables associated with P1 all relate to supportive e-health services. The second principal factor, P2, is associated with variables, which are associated to being "Positive to reading medical records due to implications". This is due to the variables indicating a desire to access medical record as a means to improve communication with healthcare, receive better care, better understand their health situation and to be better at taking care of oneself.

The principal factor P3 is interpreted as representing "Positive to all Internet use including medical records online". The variables associated with P3 indicate proneness to use social media to get help if there are problems in understanding something in the medical record, a positive attitude to reading their medical record online

and then not worry about security issues, and a positive attitude to communicating with medical staff via email, searching for health information on internet including using social forums.

The label for factor P4 is “Distrustful and wants to be in control of health treatment”. The variables associated with P4 indicate likelihood of having ordered the medical record to get an overview of their health condition, check details in their medical record and the received treatment, and to follow up what was said during a healthcare visit. It is also related to distrust of the healthcare providers and willingness to be able to check who has accessed the medical records.

The variables associated with the factor P5 indicate persons who are not in good health and have worries about their condition. P5 is thus labelled “Worried about health”. The factor P6 is associated with variables representing a preference to ask healthcare professionals either online, via phone, or at their next visit if they do not understand something in their medical record. The label chosen for P6 is “Wants communication with healthcare professionals”. The last factor, P7, ”Does not understand their medical record” is associated with variables that indicate difficulties in understanding both the medical record in general and the part they are specifically interested in.

Besides the apparent repercussions in healthcare, information management and systems design contexts, we argue that all the seven identified attitudes have specific implications from the security and privacy perspective. In Table 2, the factors have been mapped into the four information security characteristics (Fig. 1) using a plus (+1) to mark a significant factor from the point of view represented by the factor or minus (-) if the aspect is explicitly trivialised by the standpoint represented by the factor.

Table 2. Factors P1-7 mapped to the four information security characteristics (+ significant aspect for factor; - (empathetically) unsignificant aspect).

	Availability	**Integrity**	**Confidentiality**	**Accountability**
P1	+			

P2	+	+		
P3	+	-	-	-
P4	+	+	+	+
P5	+			
P6				
P7				

Availability is the characteristic that can be related to the largest number of factors. An analysis of the vantage points represented by the factors indicate that access to information has a significant (+) relation to very different types of health related needs and wants. The attitude represented by P1 and P3 are in support of the general availability of eHealth services and online information exchange. P2 can expected to be benefitting of availability of information due its capability to facilitate communication with and participation in healthcare with an aim of receiving more adequate care. Availability of information can help patients to better understand their health and ultimately take better care of their health. Patients' desire for improved communication with healthcare is also consistent with their desire to use various eHealth services for this purpose. In P4, it is possible to see frustration among patients that they did not feel that have received enough information and therefore does not have control over their healthcare. A similar experience of the lack of availability is also indicated by the standpoint represented by the factor P5, patients that are worried about their health. As a whole, it seems that the availability of information may be considered as a crucial element for the experience of a good quality of care that is relevant even if the patients' would have very different attitudes to eHealth services the their current care providers.

Integrity indicates the significance of right and correct information. In case of the attitude P2, it is important to be able to assess that a particular piece of information is correct and the patient has an opportunity to access information using various communication channels and to follow up what was said during a healthcare visit. Moreover, there is frustration among the patients on not getting an overview of their health condition not being able to check details in

their medical record and accessing information about their treatment. Hence, the integrity aspect is of crucial importance regarding the patient's confidence in healthcare especially with the factor P4. On the other hand, for P3 that represents a largely carefree attitude of the eventual risks, the patients' uncritically positive attitude to be able to get access to various eHealth services may lead to unwarranted trust on unreliable information. Information can be retrieved from a variety of sources with different levels of quality without any guarantees that the accuracy of information could be ensured. This type of an attitude is a challenge for eHealth service providers and puts pressure on, for instance, the coordination and standardization of patient information.

Confidentiality aspects is not the primary concern of the patients. The generally very positive attitude (represented by P3) to all types of Internet-mediated use of healthcare services may be seen as an indication of a belief that healthcare provides secure eHealth services. Otherwise these services would not exist. However, when more information is disseminated about the patients via the Internet, the likelihood of unauthorized access to patient information increases. In contrast, patients' frustration of not being in control of their treatment (P4) can lead to a naive attitude of overemphasising confidentiality and simultaneously disparaging the benefits of letting relevant professionals access, for instance, the contents of the medical record. In general, however, looking at the results of the factor analysis, the availability and integrity of information seem to be more important for the patients than the risk of having their information revealed by others.

Accountability seems to be similarly to the confidentiality, a relatively minor concern for the patients. Accountability of information tends also to be more a technical question. This aspect becomes crucial for the patient first when an incident has taken place and the question of accountability gets practical relevance. For a person with a generally positive attitude towards online services (P3), accountability is plausibly similarly to confidentiality, a non-question that is taken for granted. On the other hand, when

the patient wants to have a better control over their healthcare (P4), traceability and accountability is an apparent issue with an immediate relevance.

5 Discussion and conclusions

When the results of the factor analysis are mapped to the dimensions of information security, it becomes apparent that there is a clear bias in the patients' privacy and safety concerns and priorities. In general, the patients' attitudes may be characterised as relatively naive. There are three factors that are largely unrelated to privacy and safety, and even in the factors that incorporate information security related reasoning, in contrast to access, safety is not a central aspect in how people conceptualise medical records and how they are accessed. It seems plausible to suggest that security is more or less taken as granted even if it is apparent that the picture may be more complex that it seems. The present analysis of the collected quantitative data does not provide us means to elaborate the relation of the attitudinal constellations revealed by the factor analysis and, for instance, how the different individuals in practice act in their daily life and cope with their eventual concerns on information security. Similarly, the present factor analysis based approach does not give us possibilities to measure actual levels of concerns and awareness in the population. It merely provides a glimpse into the different types of priorities patients have concerning their health information.

A closer analysis of the intersection of the security characteristics and the factors presented in the paper does provide, however, some clues how the security thinking might be broadened in the future in the different clusters of attitudes represented by the factors P1-P7. Partly, it would be important to counter the occurrence of highly naive attitudes, but also to take into account the diversity of concerns, wants and needs of different aspects of information security. Even if a trustful and distrustful patient benefits of the general improvement of information security, it may be necessary to be more explicit about the precise mechanisms of confidentiality and accountability for distrustful persons and provide them guid-

ance how to manage their personal settings than for a trusting person who would probably be satisfied with more general settings. Similarly, an online-oriented person (P3) could be assumed to expect a more general availability of information, whereas an implications oriented individual might be assumed to be content with a more limited availability. Restricting the availability of information according to the practical needs and demands of individual patients helps to prevent unnecessary transferring of confidential information on the net (cf. [12]).

Our conclusion is that a more holistic systemic perspective to information security [17,18] is needed to support the effective use of medical records in the healthcare in information and data driven society. Availability and integrity, and confidentiality and accountability are all necessary elements of an eHealth service as demonstrated before [2], [13] and their significance is related both to the general quality of the services, but also to the specific needs and wants of particular groups of their users. Safety and privacy are neither mechanistic aspects of technical systems, but issues that pertain to the entire healthcare process [6], [4]. A more systematic approach does not only improve the safety and privacy of patients, but would also enhance the general understanding and possibilities to unleash the real potential of patient access to medical records in improving the care and well-being of patients.

References

1. Kaelber, David C, & Bates, David W. (2007). Health information exchange and patient safety. Journal of biomedical informatics, 40(6), S40-S45.

2. Åhlfeldt, R-M. and Söderström, E., (2010). Patient Safety and Patient Privacy in Information Security from the Patient's View: A case study. *Journal of Information System Security (JISSec)*, Vol 6. No. 4, pp. 71-85 ISSN:1551-0123

3. Haas, S., Wohlgemuth, S., Echizen, I., Sonehara, N. & Muller, G. 2011. Aspects of privacy for electronic health records. *Int J Med Inform,* 80**,** e26-31.

4. Baker, D. B. Privacy and security in public health: Maintaining the delicate balance between personal privacy and population safety. Computer Security Applications Conference, 2006. ACSAC'06. 22nd Annual, 2006. IEEE, 3-22.

5. Ministry of Health and Social Affairs (2011). National eHealth – the strategy for accessible and secure information in health and social care: Ministry of Health and Social Affairs.

6. Appari, A. & Johnson, M. E. 2010. Information security and privacy in healthcare: current state of research. *International journal of Internet and enterprise management,* 6**,** 279-314.

7. Acquisti, Alessandro. (2004). Privacy and security of personal information *Economics of Information Security* (pp. 179-186): Springer

8. Ünver Ö., Atzori W. (2013). Questionnaire for Patient Empowerment Measurement Version 1.0 (pp. 1-74).

9. WHO Europe (2014) Patient Safety. Available on Internet: http://www.euro.who.int/en/health-topics/Health-systems/patient-safety [Accessed Mars 2014]

10. Leino-Kilpi, Helena, Välimäki, Maritta, Dassen, Theo, Gasull, Maria, Lemonidou, Chryssoula, Scott, Anne, & Arndt, Marianne. (2001). Privacy: a review of the literature. International journal of nursing studies, 38(6), 663-671.

11. Business Dictionary, (2014) Definition Privacy [on-line]. Available from: http//:www.businessdectionary.com/definition/privacy.html [Accessed Mars, 2014]

12. Baker, D. B, & Masys, D. R. (1999). PCASSO: a design for secure communication of personal health information via the internet. *Int J Med Inform, 54*(2), 97-104.

13. Åhlfeldt, R-M., Spagnoletti, P. and Sindre, G. 2007. Improving the Information Security Model by using TFI. In *Proceedings of the 22tn IFIP TC-11 International Information Security Conference (SEC 2007).* Sandton, South Africa, May 14-16, 2007. pp 73-84. ISBN: 13:978-0-387-72366-2, eISBN: 13:9780-387-72367-9, ISSN: 1571-5736

14. Ekendahl, M. (2011). En modell för att hantera journaluppgifter på internet för patienter. Tech. rep., INERA, Stockholm.

15. Fowles, J. B., Kind, A. C., Craft, C., Kind, E. A., Mandel, J. L., & Adlis, S. (2004). Patients' interest in reading their medical record: relation with clinical and sociodemographic characteristics and patients' approach to health care. *Arch Intern Med*, *164*(7), 793–800.

16. Huvila, I., Cajander, Å., Daniels, M. & Åhlfeldt, R-M (2014) Reading Medical Records Serve Different Needs for Patients: Patients' Perceptions of their Medical Records from Different Subject Positions. Journal of the Association for Information Science and Technology, In print.

17. Leveson, N. (2011) Engineering a safer world : systems thinking applied to safety. MIT Press, 2012.

18. Young, W. & Leveson, N. G. (2014) An Integrated Approach to Safety and Security Based on Systems Theory. Commun. ACM, 2014, 57 (2), 31-35.