2011

Research Toward the Practical Application of a Risk Evaluation Framework: Security Analysis of the Clinical Area within the German Electronic Health Information System

Ali Sunyaev
University of Cologne, Germany, sunyaev@wiso.uni-koeln.de

Johannes Pflug
University of Vienna, Austria, johannes.pflug@univie.ac.at

24th Bled eConference
eFuture:
Creating Solutions for the Individual, Organisations and Society
June 12 - 15, 2011; Bled, Slovenia

Research Toward the Practical Application of a Risk Evaluation Framework: *Security Analysis of the Clinical Area within the German Electronic Health Information System*

Ali Sunyaev

University of Cologne, Germany

sunyaev@wiso.uni-koeln.de

Johannes Pflug

University of Vienna, Austria

johannes.pflug@univie.ac.at

Abstract

The following study provides a risk analysis of the forthcoming nationwide healthcare information system in Germany. Based on the information security audit methodology of the Federal Office for Information Security (BSI), we evaluated the introduction of the new system in hospitals with respect to security. Conceptually, the study focuses explicitly on an organizational level; specifically the use of healthcare telematics components such as electronic health card and health professional card. A dual approach of both security process and risk analysis thereby established an adequate level of information security. For this purpose, an appropriate framework specifically designed for the clinical area is first developed and explained in detail. Based on these perceptions it is possible to precisely check the workflows "patient admission" and "prescription of medicine" for inherent organizational threats. The aim of this paper is to propose appropriate steps to mitigate potential risks before German healthcare telematics comes into use.

Keywords: electronic health card, eHealth, organizational risk analysis, information security management

1 Introduction

As part of a larger health sector reform in 2006, the introduction of the electronic health card (EHC) in Germany was decided. For the first time, modern information technology is being introduced on a wider range in the health sector. A network of data crossing the boundaries of single medical institutions (medical practices, hospitals, pharmacies etc.) opens many new possibilities and prospects. The electronic health card should have come into use in 2006, but due to various problems the introduction of the cards has been delayed. Although the exact extent of applications to be offered by the EHC is subject of a controversial debate at the moment, there is no question that it will have a significant impact on workflows in medical institutions. While technical issues have been widely discussed (Sunyaev, Leimeister and Krcmar, 2008), less attention has been paid to organizational matters. The impact on hospitals and their business processes has, especially, been broadly ignored in the past.

This paper examines the changes in clinical workflows and reveals inherent organizational hazards. By doing so, this work demonstrates information systems research (ISR) in its truest sense: presentation of a real-world problem, its analysis, corresponding lessons learned and the provision of solutions for further development. The conducted analysis is based on the well-known framework by the German Federal Office for Information Security (BSI).

2 The BSI Risk Management Framework

The BSI offers a methodology that provides efficient management of information security which can be adapted to the specific circumstances of any institution. The framework, known as “IT baseline protection”, bundles different established approaches and represents a standard for establishing and maintaining adequate protection of all information in a predefined organization.

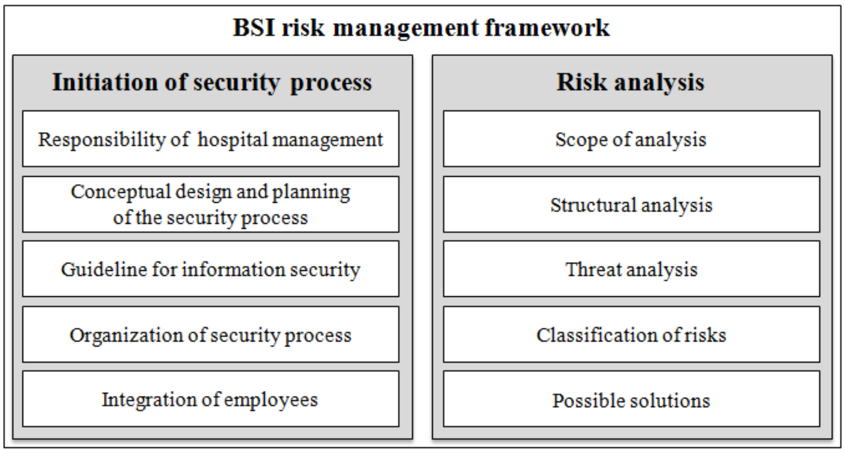
BSI risk management framework
Initiation of security process
Responsibility of hospital management
Conceptual design and planning of the security process
Guideline for information security
Organization of security process
Integration of employees
Risk analysis
Scope of analysis
Structural analysis
Threat analysis
Classification of risks
Possible solutions

Figure 1: The BSI risk management framework

A fundamental requirement for achieving adequate protection is the execution of a risk analysis. Reasonable results can be expected only if a formal and unified approach is followed. The basic idea of the risk analysis by BSI is that risks can arise due to both flawed conditions and from within the institution itself through poorly protected business processes.

This situation is the reason why the reference model distinguishes between two sets of activities: The initiation of a security process and the “actual” risk analysis. Both parts together form a unit. During the phase of the security process all necessary parameters are set in order to guarantee data security against “external” threats. The risk analysis, however, is applied directly to the workflows in order to uncover vulnerabilities and find appropriate solutions.

3 Initiation of security process

3.1 Responsibility of hospital management

Along with the introduction of the electronic health card, information technology is becoming an increasingly important issue in hospitals. There can be no doubt that management has to prioritize the maintenance of security and adherence to guidelines. However, surveys reveal that even in big institutions this is not always the case (Dinnie, 1999). The situation in German hospitals is even worse as information from the data protection commissioners' manifest reveals. As a matter of principle, information security is considered to be a "problem of other people". The responsibility is usually delegated and redelegated until, ultimately, no one considers himself responsible for it (BSI, 2008).

This situation prevents medical institutions from reaching adequate levels of information security. The situation won't change significantly until the management of the hospital is given sole responsibility for security. Furthermore, the responsibility of the management is the fundamental prerequisite for the next steps of initiating the security process.

3.2 Conceptual design and planning of the security process

Using an approach of three steps, the major issues related to the basic conditions of medical institutions are resolved, followed by the definition of security objectives, from which ultimately an adequate level of security can be derived.

To ensure a certain methodology, the most important business and technical tasks and their need for information security have to be determined. The cohesion between workflows on the one hand and the information processed respectively the required IT on the other hand is the basis for the decision about which security level is appropriate to protect the institution. The processed information for the most striking workflows is shown in table 1.

Table 1: Processed information for the most important activities in hospitals

Category	Activity	Processed information
Administrative	Patient admission	First and last name, sex, birth date, address, name of health insurance (Gematik, 2008c)
	Electronic referral	i.a. writer, addressee (doctor or hospital), optionally assignment
Hybrid	Electronic prescription	i.a. name of medicine, packaging size, id (Gematik, 2008b)
Medical	Ambulant or in-patient treatment	i.a. diagnoses, radiographs, findings, correspondence
	First-aid treatment	i.a. intolerance to medicine, allergies, chronic ailments, additional important facts for cases of emergencies (Gematik, 2008a)

Based on table 1, it is possible to evaluate the processed information with regard to its need for confidentiality, integrity and availability. Data are especially at risk when they have a high value to certain groups. Considered which conclusion employers or insurance companies could draw out of these data this also applies for the electronic health record (Huber, Sunyaev and Krcmar, 2008). Therefore the security level for the health record and the limited swift of data for emergencies has to be "very high". In contrast, administrative data have a far lower value and consequently the need for protection is comparatively "low".

A similar picture emerges from patient information that is processed during referrals, as the name of the receiving doctor alone is no source for useful knowledge. A slightly higher sensitivity results only if the referral is associated with an optional assignment. In this case the security level can be determined as "medium". The prescription of medicine, moreover, can be classified to the same category because the processed information gives a clue about the health in general or even specific diseases of the patient. Yet, a holistic picture, such as from the electronic health record, cannot be derived. The collected evidence is presented in table 2.

Table 2: Required security level for processed information

Required security level	Kind of information
low	Administrative data
	Referral (without assignment)
medium	Electronic prescriptions
	Referral (including assignment)
high	Electronic health records
	Data for emergencies

The results obtained will be used to develop security goals for hospitals. Only a complete and appropriate definition of security objectives will avoid the risk of developing strategies and approaches that fail to meet the actual requirements. This may mean that unwanted risks are being taken but also that too many resources are being invested into improper security precautions (BSI, 2008). The main goals related to data security in hospitals are described subsequently:

- Information about the health of patients must be of high quality, since it constitutes the basis for further treatments.
- The security precautions of the EHC must not disturb smooth workflows.
- Legal requirements must be met.
- Users of the hospital information system must only be allowed to access files corresponding to their authorization; unauthorized access must be prevented (Gematik, 2008e).
- Maximum transparency has to be ensured. The rights of the patient must not be restricted.

This set of objectives forms a basis for all further actions. However, it is important to understand that defining the security level should not imply that individual business processes all share the same demands for security. In fact, certain activities require, due to their characteristics, special and individualized analysis.

Based on their extraordinary importance, it is necessary to carry out an investigation of two workflows that are directly affected by the introduction of the electronic health card: patient admissions and electronic prescription of medicine. These two activities will also be investigated for inherent hazards by the risk analysis, which is the second part of the BSI framework. The definition of the individual, appropriate security level is based on ISO 27001 (2005), where the three aspects "confidentiality", "integrity" and "availability" are distinguished. A deep analysis for the patient admission results in a desired level of security which is "**normal**". Obviously, the process of prescribing medicine requires an entirely different protection since the data processed are more critical. Taking all aspects into account the prescription of medicine requires a "**high**" protection level.

By now, all necessary information has been gathered and therefore, the conceptual designing and planning of the security process is complete. The deployment can be prepared in a further step.

3.3 Guideline for information security

Actual improvement of comprehensive security is only possible if the security objectives and security strategy are communicated to all employees of the institution. For this reason, a guideline is required, i.e. a document which expresses the main principles of the security strategy in a clear and understandable way.

It is the central strategy document for the entire institution, so the guideline needs to be designed in a way that all recipients can identify with it. Therefore briefness and conciseness are basic requirements for the document. In practice, a document more than 20 pages in length will probably be a failure (BSI, 2008). Only the field of application, the security objectives (as shown in 3.2), the security strategy (as discussed within the security process) and the organization of the security process (as shown below) should be included.

3.4 Organization of the security process

Even a well-designed security process only contributes to a better protection if it is executed in a suitable way. The organizational structure and security management of the institution should be designed in a way that makes them compatible with one another.

In order to define an appropriate organizational structure, the activities occurring in the area of information security have to be recorded and named. A detailed analysis of hospital procedures shows that it is possible to divide occurring tasks - independent of the specific institution - into four categories: (a) Information security in the narrowest sense; (b) Executive functions; (c) Data protection and (d) Pure IT work.

In order to define an appropriate organizational structure, it is necessary to link individual activities from the categories above to a role. Unlike the term "job", which describes the scope of a single employee, a "role" delivers no information about its associated effort. In hospitals, there is the role of the management, which is responsible for the administrative functions. Furthermore, according to German law (BDSG, 2009) it is necessary to commission a data protection officer, as "personal data is processed automatically". IT work can therefore be assigned to the IT department. Consequently, only the activities from the category "information security in the narrowest sense" are left over. The BSI risk management framework suggests the establishment of the role of security administrator for these tasks (BSI, 2008). From this, a reference model for an organizational structure of hospitals concerning security is proposed (figure 2).

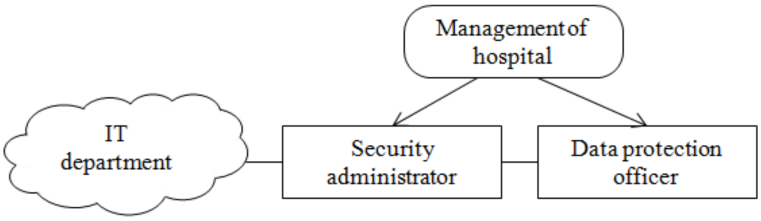

Figure 2: Reference model for the organizational structure

The implementation of these concepts is already an important step towards greater information security. The security process is fully designed and ready to be introduced in the hospital. All necessary parameters are set in order to guarantee data security against “external” threats. But risks also arise from the business processes themselves. For this reason, it is necessary to carry out a special risk analysis for three workflows that are directly affected by the introduction of the electronic health card.

4 Risk analysis

4.1 Research approach

First, the scope of the analysis must be defined. This step ensures maximum transparency and thoroughness, so that all potential threats are detected in the risk analysis. The subsequent structural analysis is about the preliminary investigation of information that is useful for the later detection of potential threats. The workflow examined is described in great detail. The goal is to create a substantial and formal foundation on which the risk analysis can be constructed. The actual process of detecting hazards is about the analysis of every aspect in respect to vulnerabilities and risks.

To get a better overview of the threat level, the hazards identified in the risk analysis are classified. In the final and most important part of the risk analysis, possible solutions are developed to explain how the threats can be dealt with appropriately. Each threat is analyzed individually to determine whether complete prevention is possible or whether the limitation of risk is reasonable.

4.2 Admission of patients

The scope of analysis includes all sub-processes of the patient admission that are affected by the introduction of the electronic health card. Aspects such as the internal scheduling of the hospital or the procedure in the event of EHC systems going offline haven’t changed compared to the old system. The structural analysis assumes that the patient is conscious. This applies to any ambulant and in-patient admission but it might not be the case with emergency treatments. In such cases, admission will then be done retroactively at a later date, so this scenario can be ignored.

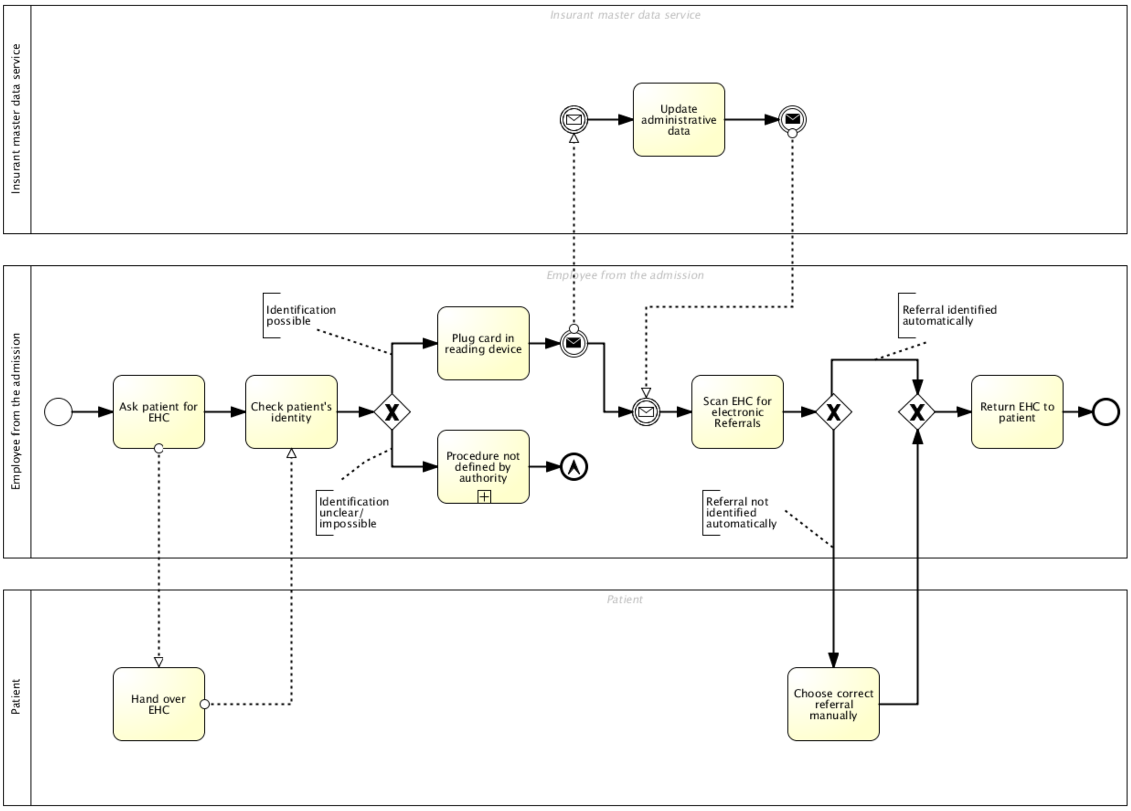
Insurant master data service
Update administrative data
Employee from the admission
Identification possible
Plug card in reading device
Ask patient for EHC
Check patient's identity
Procedure not defined by authority
Identification unclear/ impossible
Scan EHC for electronic Referrals
Referral identified automatically
Referral not identified automatically
Return EHC to patient
Patient
Hand over EHC
Choose correct referral manually

Figure 3: Model for the process “patient admission”

The threat analysis serves as a basis for the detection of threats. Based on the structural analysis, a systematic search and identification of threats along the workflow is possible (table 3).

Table 3: Threats arising from the patient admission

No.	Inherent threats
#1.1	Patient has an electronic health card, but delivers the old insurance card. Consequently, services that should prevent malpractice can be bypassed. The danger arises because the old insurance card does not need to be returned. It is valid at least until the nationwide launch of the EHC, which may happen around four years from now.
#1.2	There is no legal compulsion to submit a photo for the EHC. The insurance protection remains nonetheless (Juerjens and Rumm, 2008). This legal loophole enables misuse.
#1.3	The photograph is not being checked by the insurance company. Legally, this is not obligatory. It is already apparent that companies won't validate the picture due to short-term financial benefits. Consequently, it is possible for the insured to deliver intentionally unclear photographs or even photographs of another person.
#1.4	The employee does not compare the photograph with the patient's identity. This hazard arises mainly due to the increasing workload of hospital staff in hospitals, which motivates employees to search for ways to speed up the workflows. Such a scenario would be intentional ignorance of the photo validation requirement.
#1.5	At the moment there is no defined procedure if the photograph and the patient's identity don't match.
#1.6	There is also no defined procedure in case of unclear correspondence between the patient and photograph.
#1.7	The process of updating the administrative data is aborted manually. Therefore, there is a risk that employees could use the manual abort function (Häber et al., 2009) to save time. This makes fraud possible.
#1.8	At the moment, there is no defined procedure for the event that the EHC is not valid.
#1.9	Personal information about the health of the patient can be derived from the electronic referrals. This problem arises particularly when the patient has to choose the appropriate referral on the display. Data protection is not guaranteed in this situation.
#1.10	The employee selects the proper referral on the display right by himself. In practice, such an approach leads to a faster process but it can also create conflicts related to the patient's right to self-determination.
#1.11	The process of choosing the proper referral on a display is too complicated for some patients. Reasons may include sanitary restrictions or language problems.
#1.12	Technical issues complicate the use of an appropriate referral. In this case, no procedure is defined at the moment.
#1.13	A patient forgets their electronic health card inside the reading device. This is far more problematic than the loss of the former insurance card as the patient will find it difficult to access medicine without their EHC.

Regarding the consequences of the risks, the damage can be classified into three categories: Financial loss for the health insurance providers, violation of data protection law, and discomfort for patients. The three categories now serve as the starting point for the development of solutions for the threats. The goal is to prevent as many risks as possible by eliminating their cause. If there is no complete solution then, at least, the probability of their occurring should be limited. Fortunately, the results of a comprehensive analysis show that most threats can be entirely avoided by relatively simple measures. There are, for example, two solutions for the scenario of criminals using old insurance cards instead of the EHC. First, the patient may be asked to return his old insurance card upon receipt of the new electronic health card. If he fails to do so and continues to use the existing card, he should become a self-paying patient. Another quite simple approach would be the reduction of the transition period in which both systems can be used. But there is also a good method to ensure that patients deliver a correct photograph for the EHC: As the insured person has to submit a photo by mail or digital communications anyway, it would be easy to add a copy of an official identity document, e.g. identity card, passport or driver's license. The check for compliance does not involve unreasonable costs for the health insurance companies but would avoid a major risk.

Threats arising from undefined procedures can also be eliminated completely by developing instructions for these specific scenarios. Consider at first the cases of unclear match between the photo on the EHC and the patient's identity. The easiest way is to ask the insurant for another identity document. If there is no compliance, a suspicion of abuse is existent and therefore, the health insurance company needs to be notified (Sunyaev et al, 2009a). Furthermore, the employee is entitled to confiscate the doubtful card. However, far more complicated is the question whether a patient has a right to receive medical treatments despite abuse. In principle, the German policy of compulsory treatment implies that a doctor cannot refuse a patient from a public health insurance provider. Indeed, a decision from the German administration court says that it is not evident, "from which legal obligation a compulsory treatment arises", if the patient cannot submit his health card (Weichert, 2006). Only in "urgent cases" is immediate treatment mandatory. Therefore, the procedure is defined and the staff can be briefed appropriately.

Undoubtedly those risks that directly relate to the behaviour of employees can at least be minimized. Reality has shown that a clear and understandable explanation of the purpose and value of security measures has significant positive effects on employee behaviour. With regard to the threat of a possible loss of the EHC in the reading device, the following solution has proven to be of value: based on a similar scenario at cash dispensers, the problem could be minimized by a procedure that completes the entire procedure only after the card has been removed from the reader. This technique should be adapted to the health sector.

4.3 Prescription of medicine

The prescription of medicine describes the process of issuing the required schedules that allow a patient to purchase a specific drug. In Germany there are three kinds of prescriptions: prescriptions from the compulsory health insurance providers, private prescriptions, and prescriptions for narcotic substances. The migration from a manual procedure to an electronic process refers primarily to the first kind. However, private prescriptions differ only in the aspect of patient co-payment - the organizational processes remain the same, so the analysis results can be adopted. In contrast, prescriptions for narcotic substances need to fulfil very high security requirements. Since an adequate electronic implementation is currently impossible, these prescriptions are not processed by the telematics infrastructure (Gematik, 2008d) and are therefore not part of the analysis.

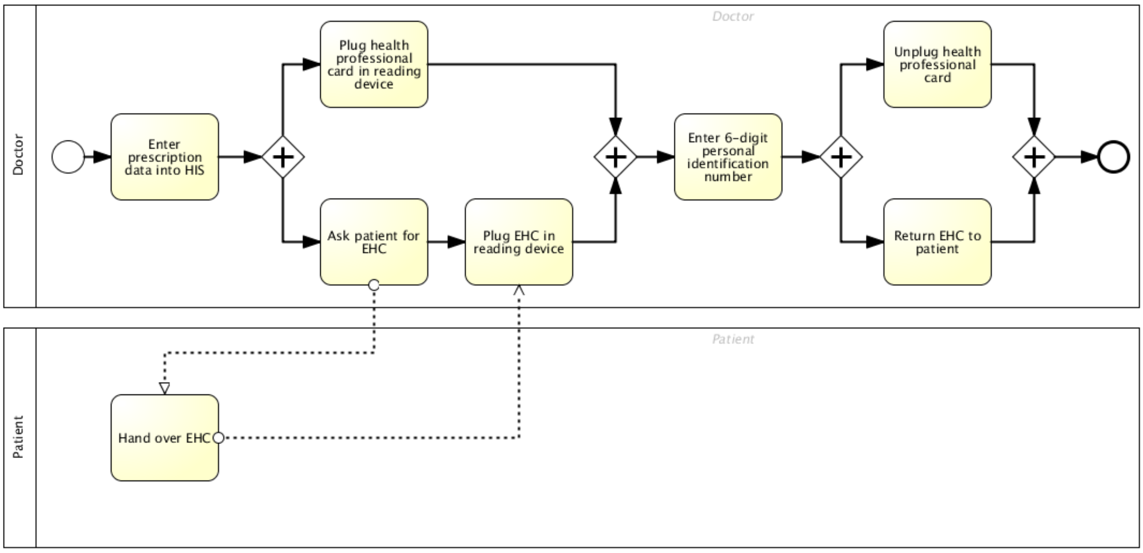
Doctor
Enter prescription data into HIS
Plug health professional card in reading device
Ask patient for EHC
Plug EHC in reading device
Enter 6-digit personal identification number
Unplug health professional card
Return EHC to patient
Patient
Hand over EHC

Figure 4: Model for the process of prescribing medicine

A sequential analysis of the workflow described in regards to any possible problems results in the threats shown in table 4.

Table 4: Threats arising from the prescription of medicine

No.	Inherent threats
#2.1	The paper prescription is still exhibited excessively. The threat arises because the old, paper-based system will be preserved as a back-up alternative due to security issues. This carries the risk that the electronic referrals aren't applied to their full extent, which would mean massive financial loss for the compulsory health insurance.
#2.2	The health professional card remains with the employees at the reception. The plugging and unplugging of the card could be considered inconvenient. Concerns have been raised that doctors will sooner or later deposit their cards permanently near the reading device.
#2.3	Waiting times expand because of the location of the reading devices. This means inconvenience to the patients and slower workflows.
#2.4	The prescribed medicine is not reviewed during the signing process by the doctor. Due to the high number of prescriptions, the danger arises that the doctor enters his PIN "blindly" and as a result the wrong medication is prescribed.
#2.5	The correction of false prescriptions might lead to significant delays. If the doctor recognizes such a mistake on the display, the specific prescription needs to be deleted or corrected within the hospital information system. This might take a while and cause serious delays.
#2.6	PIN of the health professional card is compromised. The high number of necessary prescriptions forces the doctors to enter their PIN very often. This implies a considerable risk that the secret code can be stolen and misused (BSI, 2007).
#2.7	Doctor gives his PIN to the staff at the reception. A completely new dimension in bypassing security mechanisms occurs if the employees at the front desk are allowed to prescribe medicine themselves. This scenario is not impossible as many doctor's practice today make a habit of storing prescription forms with blank signatures at the reception.
#2.8	The choice between local and central storage of electronic referrals confuses the patients.
#2.9	A patient forgets their electronic health card inside the reading device. This is far more problematic than the loss of the former insurance card, as the patient cannot access any medicine without their EHC.
#2.10	The doctor forgets his health professional card inside the reading device. This incident is problematic as the doctor is virtually paralyzed in the telematics environment without his card.

In the context of the process workflow “prescription of medicine”, three categories of damage could be identified: In addition to financial loss for insurance companies and discomfort for patients, which are familiar from the analysis of first process, a new category called “bypassing security measures” is added.

Fortunately, five of the ten recognized threats can be completely avoided by eliminating their causes. The theft of PIN numbers from health professional cards could be prevented by using a biometric identification system, e.g. a fingerprint scan. This would both prevent abuse and speed up the workflow. The danger of the doctor leaving his personal identification number at the reception desk would be solved as well. Given these significant advantages, it is incomprehensible that the provider of the EHC has developed such concepts but has not yet scheduled their implementation (Sunyaev et al, 2009b). Regarding patient inconvenience resulting from a faulty prescription, the following procedure is a possible solution: employees at the reception desk should be allowed to access and correct prescription data in the hospital information system. As some hospitals will probably take the line of the least resistance and simply keep their paper-based prescription systems, automated controls should be introduced. Finally, the currently proposed freedom of choice between central and local storage of prescriptions is unnecessary. Although both alternatives certainly have assets and drawbacks, the consequence may be confusion among patients. The provider of the EHC should make a clear decision.

The occurrence of at least three more threats can also be limited. A major problem is the risk that doctors might deposit their health professional card at the reception desk. This threat should be solved in two ways: Both doctors and the administration personnel should be educated about the importance of strict compliance with all regulations. Furthermore, the medical association should provide a basis for sanctioning misconduct. The threat of forgetting the health card or the health professional card has already been examined during the analysis of patient admission. In principle, the same solution can be applied, i.e. the prescription process should only terminate after both cards have been removed from the reading device. Adding an acoustic signal would help to reduce the risk even more.

5 Conclusion

Perfect security in information technology is neither technically or organizationally possible, nor economically viable. Security is always subjective and depends on the threats facing each individual institution. The variety of factors affecting security makes the protection of information technology a very complex task. Implementation, maintenance, development and evaluation should therefore be based on a reliable reference model that covers all aspects of information security.

The analysis of organizational aspects of the electronic health card in hospitals is therefore based on the risk management framework from the German BSI. The basic idea of the risk analysis is that threats arise due both to flawed conditions and from the institutions themselves through poorly protected workflows. Consequently, this study distinguished two sets of measures: the initiation of a security process and a risk analysis. Both parts together form a unit and have been applied to the introduction of the electronic health card in hospitals. The result is a comprehensive examination of potential organizational risks. Regarding the organizational framework, ambiguous responsibilities are a major threat. The study explains in detail why an active role for hospital management is an indispensable component of a viable organization. A major achievement is the developed reference model that provides an appropriate structure and allocation of roles for hospitals regardless of their size. With both the guideline on information security and the proposed catalogue to a meaningful involvement of all stakeholders in the security process, two instruments have been introduced that will effectively contribute to the protection of the sensitive health data. An important intermediate result is the evaluation of the required protection level for selected workflows, which forms the basis for the risk analysis. An approach consisting of five sequential steps made it possible to identify threats within the business processes “patient admission” and “prescription of medicine”. A total of 22 unique hazards could be categorized into four different classes of damage. The developed measures provide solutions for most of the threats: 11 problems can be avoided completely by eliminating their cause and another 8 risks are limited in terms of the likelihood of their occurrence.

The study shows that an appropriate level of security can be achieved in hospitals. For this purpose, the proposed measures must be implemented fully and consistently. In the long term, new risks will probably arise. It will be the task of the provider gematik to react both quickly and appropriately to any upcoming dangers and thus maintain the effectiveness of the security mechanisms on a sustained basis. The conducted analysis contributes to a topic that will affect any person in Germany for the upcoming decades and that directly concerns a domain oriented risk analysis (with rising importance to ISR).

References

BDSG – Bundesdatenschutzgesetz (2009) Datenschutzrecht. DTV-Beck, München.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2007). Technische Richtlinie - Komfortsignatur mit dem Heilberufsausweis. Version 2.0. BSI, Bonn.

BSI - Bundesamt für Sicherheit in der Informationstechnik (2008) BSI-Standard 100-2 IT-Grundschutz Methodology. Version 2.0. BSI, Bonn.

Dinnie, G. (1999) The Second Annual Global Information Security Survey. In Information Management & Computer Security, Vol. 7 Iss: 3, pp.112 – 120.

Gematik (2008a) Facharchitektur Daten für die Notfallversorgung (NFDM). Version 1.7.0.

Gematik (2008b) Facharchitektur Verordnungsdatenmanagement (VODM). Version 1.5.1.

Gematik (2008c) Fachkonzept Versichertenstammdatenmanagement (VSDM). Version 2.8.1.

Gematik (2008d) Fachkonzept Verordnungsdatenmanagement (VODM). Version 2.6.0.

Gematik (2008e) Übergreifendes Sicherheitskonzept der Telematikinfrastruktur. Version 2.4.0.

Häber, A. et al. (2009) Leitfaden für die Einführung der elektronischen Gesundheitskarte im Krankenhaus. Westsächsische Hochschule, Zwickau.

Huber, M., Sunyaev, A. and Krcmar, H. (2008) Security analysis of the health care telematics infrastructure in Germany. In: ICEIS 2008 - Proceedings of the Tenth

International Conference on Enterprise Information Systems, Vol. ISAS-2, pp. 144-153. Barcelona, Spain.

ISO/IEC (2005) 27001 - Information technology - Security techniques - Information security management systems - Requirements.

Jürjens, J. and Rumm, R. (2008) Model-based Security Analysis of the German Health Card Architecture, Methods Inf Med, vol. 47, pp. 409-416.

Kuckein, C., Schermann, M., Sunyaev, A., and Krcmar, H. (2010) An Exploratory Study on Physicians' Diligence when Dealing with Patient Data. In: Proceedings of the 18th European Conference on Information Systems.

Statistisches Bundesamt (2008) Krankenhauslandschaft im Umbruch. Pressekonferenz am 10. Dezember 2008. Wiesbaden.

Sunyaev, A., Göttlinger, S., Mauro, C., Leimeister, J. M. and Krcmar, H. (2009a) Analysis of the Applications of the Electronic Health Card in Germany, Proceedings of Wirtschaftsinformatik 2009, pp. 749-758.

Sunyaev, A., Kaletsch, A., Mauro, C. and Krcmar, H. (2009b) Security Analysis of the German electronic Health Card’s Peripheral Parts, Proceedings of the 11th International Conference on Enterprise Information Systems (ICEIS 2009), pp. 19-26.

Sunyaev, A.; Leimeister, J.M.; Krcmar, H. (2010): Open Security Issues in German Healthcare Telematics. In: Proceedings of the Third International Conference on Health Informatics (HealthInf 2010), January 20-23, 2010, Valencia, Spain, pp. 187-194.