Access Control for Electronic Health Records

A Delphi study of current challenges and highlighting of potential improvements

Rune Hystad[a], Rune Fensli[b]

[a] *Department of Health and Nursing Science, University of Agder, Norway*
[b] *Center for eHealth and Health Care Technology, Department of ICT, University of Agder, Norway*

Abstract

Access control is an essential function in electronic health records (EHR) to maintain the duality between patient safety and patient privacy by ensuring that authorized personnel are allowed access to health records. In the Norwegian secondary care, access control in EHR must be given on the basis of decisions about health care, so called decision based access. There is however no empirical data on experiences with the use and setup of decision based access. A Delphi survey was therefore undertaken to identify what end users and system administrators consider to be important challenges, and ways to improve the access control. The survey shows that challenges identified in previous studies are still present. Access control is not sufficiently tailored to treatment processes, and there is extensive use of exception mechanisms, which creates long event records that are not followed up systematically and therefore may go at the expense of patient privacy. Possible improvements include more education, standardization of access control, easier use of exception mechanisms and a more process oriented access control.

Keywords: Access control, Electronic health records, security measures, patient safety, Delphi Technique

Introduction

Access control is an important feature of EHR, and deals with enforcing laws and policies to ensure that only authorized users gain access to confidential information. In health care, this means protecting patient privacy, while patient safety. This method requires that healthcare professionals have access to the information they need to make the most informed decisions about care and treatment of the patient [1]. Treatment Processes may be unpredictable, making it difficult to implement strict rules for access control, which adequately protects both privacy, by minimizing the possibility of misappropriation of confidential information (snooping), and patient safety.

There are many models for access control, but there is little published research regarding the health services requirements for access control. Literature shows that most models for access control in healthcare are studies or prototypes where health professionals have not participated in the development of either policies, models or mechanisms for access control [2].

Decision based access, which is a further development of traditional role-based access control is in use in much of the Norwegian secondary healths EHR systems. On the basis of legislation concretized through the EHR-standard [3], and standards for information security in the health care and social sector [4] are required to use this. Within a few years the decision controlled access is likely to be introduced in all regional health enterprises, each with a set of standardized principles for access control. There is, however, little empirical evidence about this model among those who daily work with it; end users and system managers.

This paper has sought to identify what the end users and system administrators consider important challenges and possible improvements of access control, through a Delphi study and data from an EMR database.

Materials and Methods

Delphi survey

The survey was conducted with end users from one health enterprise, and system administrators from several health enterprises and regional system administrators. This study used the Delphi method as described by Schmidt [5] to identify and rank important challenges and possible improvements with regard to access control. Data were collected via SurveyXact online survey program.

Expert panels

End users and system managers were allocated to each their panel, and the selection of experts was partially based on Okoli and Pawloski's [6] recommendations of the preparation of a knowledge resource nomination worksheet (KRNW). The end users were recruited from Sørlandet Hospital health enterprise (SSHF). Criteria for inclusion was that the end users as far as possible should use exception mechanisms, i.e. cases where regular access control does not cover the need for access. To identify relevant categories of end users, data on the use of actualization mechanisms were extracted from the EHR-database. In addition, nurses were invited as they are the largest user group, and feedback from them was therefore considered important. There was also a criterion that end users should have received additional training in, and having been involved in testing decision based access when this was introduced at SSHF. The latter criterion was set to increase the likelihood that end users in the study were aware of concepts like decision based access and related concepts and issues that would come up during the questionnaires in the survey. The

author got help from the IT dept. in SSHF to get an overview of which users met these criteria, and on this basis a KRNW was prepared.

The system administrators were recruited from different regional health enterprises. To ensure a variety in the group, experts with expertise in both direct management of EHR (local system managers at each health authorities, and regional system managers), and individuals with expertise in policy and legislation related to access control were nominated.

A total of 35 end users, and 20 system administrators were then invited to participate in the survey, to account for non-response and attrition, so that after the last round would be left with between 10 to 18 respondents, as this is a recommended number [6].

The study was conducted as a four-round study. SurveyXact was used to distribute questions and collect data. An e-mail was sent to the experts with a link to the questionnaire. Response time was set to three working days, with a reminder the fourth working day. Analysis was conducted in 1-3 working days, and then returned to the experts. It took five weeks between the distribution of the first round, and the last was analyzed. The language used in the study was Norwegian, and answers were translated to English by the main author, and validated by the coauthor. Table 1shows the participation in the rounds.

Table 1- Participation

	End users	**System administrators**	**Total**
Round one (%)	18 (100)	17 (100)	35 (100)
Round two (%)	18 (100)	17 (100)	35 (100)
Round three (%)	16 (89)	16 (94)	32 (91)
Round four (%)	13 (72)	15 (88)	28 (80)

Analysis

A qualitative content analysis of the first round of questionnaires was done, where it was chosen to use Directed Content Analysis, described by Hsieh and Shannon [7], which assumes that one has a theoretical framework as a basis for coding statements. The Extended InfoSec model [8] for information security in healthcare was used as the theoretical foundation. The model is developed with the purpose to describe in a simple manner what information security presents, and can express the problems and needs in information security. In this paper the model is used to highlight areas in which respondents' factors of challenges and improvements in access control can be placed. The model is shown in figure 1.

Respondents' statements were therefore shortened and categorized according to the predefined categories in the InfoSec model. In the fourth round, the statements average rating was calculated, and the degree of consensus was analyzed in SPSS by calculating Kendall's W.

Round 1

In the first round, the experts answered the following questions:

Question 1: *What challenges do you experience related to decision based access (the access control in DIPS)? You should mention point wise (in brief) at least five challenges you can think of*

Question 2: *How can access control in DIPS in your opinion be improved? You should mention point wise (in brief) at least five factors you can think of.*

The qualitative data were then consolidated so that the answers with equal meaning were merged, and answers were sorted under the overarching theme, and a number of replies were reformulated to clarify the challenge or improvement suggestion.

Based on question 1, a total of 56 unique challenges were identified after the consolidation of similar answers.

Based on question 2, a total of 44 unique ideas for improvement were identified after the consolidation of similar answers.

Round 2

After answering the first round, the experts automatically received an e-mail with the answers they had given, and in the second round they were asked the following requests related to the questions from the first round:

Question 1: I asked: What challenges do you experience related to decision based access (the access control in DIPS)? You should mention point wise (in brief) at least five challenges you can think of. The answers that came in are summarized below (but not necessarily verbatim). Look through the list and if you cannot find your answer, write it down in the field below, in brief.

Question 2: I asked: How can access control in DIPS in your opinion be improved? You should mention point wise (in brief) at least five challenges you can think of. The answers that came in are summarized below (but not necessarily verbatim). Look through the list and if you cannot find your answer, write it down in the field below, in brief.

Three of the respondents came with feedback in this round, and as a result, three new factors in Question 1 were included in round three, and it was made an addition to one of the factors in Question 2.

Round 3

In the third round, the experts were treated as two independent panels, and asked to select at least ten of the most important statements/factors associated with each of the two initial questions. The statements/factors were arranged in random order to avoid bias, due to context effects.

Question 1: Select at least 10 statements/factors that you think are important challenges to decision based access. Your answers should be based on the expertise you have in your position. The challenges do not have to relate to your own experiences.

Question 2: Select at least 10 statements/factors that you think are important factors for improving the access control. Your answers should be based on the expertise you have in

your position. Improvement proposals do not have to relate to your own experiences.

For the panel with end users, the statements/factors which were selected by over 30 % of the experts were retained, while it for the system manager panel was set a cut- off point of 35% for question one and 40 % for question two. This was done to reduce the list to a manageable size of about 10 factors, while ensuring that important factors were not rejected in this round.

Round 4

In the fourth round, the experts were asked to rate statements/factors from the reduced list after the previous round, related to each question. The statements/factors were arranged in random order to avoid bias due to context effects. In addition, the experts could post comments to explain or justify their rankings.

Question 1: To what extent do you consider the following statements/factors as challenges in access control?

Below is a list of the most important factors you have chosen, and now I want you to rank them by typing a number from 1 to 10 in the small pane by the factor. You must use all the numbers from 1 to 10, where 1 = most important.

If you want to explain the rankings, you can type this into the text field to the right.

Question 2: To what extent do you think the following statements/factors can improve the access control?

Below is a list of the most important factors you have chosen, and now I want you to rank them by typing a number from 1 to 9 in the small pane by the factor. You must use all the numbers from 1-9, where 1 = most important.

If you want to explain the rankings, you can type this into the text field to the right.

Degree of consensus among the experts were then analyzed using Kendall's W in IBM SPSS Statistics 19.

In addition, the scale was inverted for readability upon presentation of the results, and the average rating for each factor was calculated.

Kendall's W was <0.3 for all the questions, indicating weak agreement [5]. The survey was still ended for practical reasons, and not to waste the panel members' time, when it was believed that more rounds would not lead to strong agreement among the experts. Dissensus, or lack of agreement can also be a valid findings of a Delphi study [9]. The panels agreed on the key factors, lack of strong consensus was on the ranking of these factors.

Results

In round one and two, the aim was for the experts to identify and validate statements concerning challenges and possible improvements of access control. A total of 56 challenges, and 44 suggestions for improvement were identified. The results of the fourth and final round are here presented. The respondents were asked to rank the most important factors from the previous round. In the tables, the scale is inverted for easier viewing, with the highest ranking factors on top.

Table 2 - Ranking question 1, end users

Factor		Average ranking (inverted)
1.	Insufficient number of/covering implicit decision templates	7
2.	Missing/too few appropriate explicit decision templates in relation to real reason for opening the journal	6,92
3.	User may choose a wrong decision template	6,31
4.	Lack of clarity regarding use of the free text field when deciding access	6
5.	One must too often decide for access, for example when checking test results, printing to general practitioner, ended contact etc.	5,69
6.	Insufficient education in access control	5,62
7.	Users lack understanding of decision based access	5,46
8.	It requires too many keystrokes to decide access	4,46
9.	Having to decide access gives a feeling of doing something illegal, and to be mistrusted and monitored	3,92
10.	When deciding access, you automatically only have access for one day	3,62

Kendall's W = 0,150

Table 3 - Ranking question 2 end users

Factor		Average ranking (inverted)
1.	Upon referral from psychiatric to somatic department, one should have access to the referral	6,31
2.	The screen for deciding access should appear at once you try to open a patient journal you do not have access too	5,92
3.	The possibility to create custom decision templates	5,85
4.	Ability to choose what you get access to when deciding access	5,85
5.	Ability to choose what you get access to when deciding access	5,31
6.	Ability to select a default decision template that applies to all medical records	4,77
7.	Provide examples for grounds in the text field for deciding access	3,77
8.	Reduce the number of clicks needed to decide access	3,62
9.	The decision for access should automatically last more than one day	3,62

Kendall's W = 0,158

Table 4 - Ranking question 1 system administrators

Factor		Average ranking (inverted)
1.	The interface of the administrator section of DIPS is too little intuitive and transparent	6,47
2.	The access control is not integrated with the personnel system	5,67
3.	Defining the correct access profiles	5,2
4.	Little standardization of access control across health enterprises	5
5.	It is impossible/difficult to quickly get an overview of what access rights a particular user has	5
6.	There is insufficient support for log analysis	4,87
7.	Procedures for ordering and/or termination of access are not complied	4,87
8.	Insufficient functionality for blocking access to journals	4,4
9.	Adaptations to special permissions are challenging for system administrators	3,53

Kendall's W = 0,086

Table 5 - Ranking question 2 system administrators

Factor		Average ranking (inverted)
1.	Simplify the process of creating and terminating access in the administrative section of DIPS	5,13
2.	Clearer guidelines from national authorities on how access control is to be organized	5,07
3.	The access control should be integrated with personnel system so that access is automatically generated	5,07
4.	Common guidelines for access control at regional or national level	4,93
5.	Logic for access control should be done nationally and linked to patient care/referral periods	4,4
6.	Better overview of everything a user has access to	4,4
7.	The screen to decide access should come up instantly when you try to enter a journal you do not have access to	3,73
8.	Active use of the access log for quality assurance	3,27

Kendall's W = 0,080

Summary of challenges and suggestions for improvement

Figure 1 shows the InfoSec model with the assembled factors for challenges and improvements of access control. Letter and number codes in the figure are listed according to the expert panel, questions and factor, where A = end user, B = system administrator (eg. code A2-4 refers to the panel with end users, question 2, factor 4).

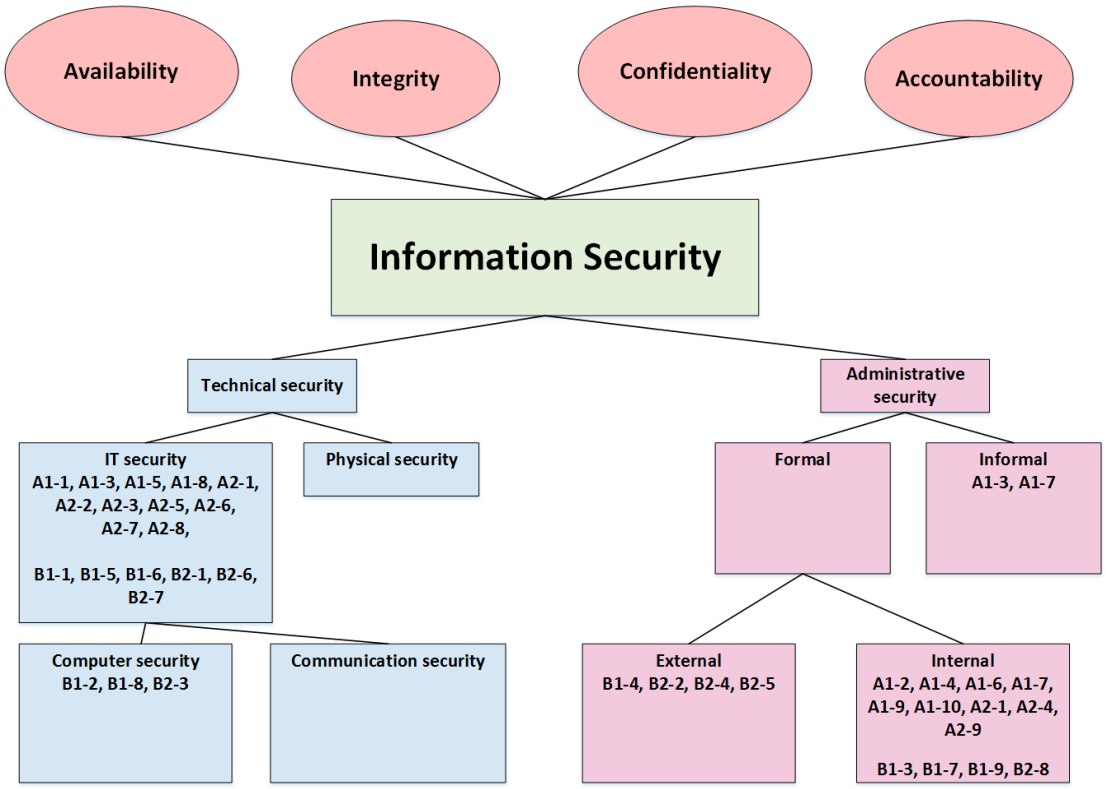

Figure 1 – The Extended InfoSec model with assembled factors

Table 6 - Average number of actualizations per position for the period 01.08.13-30.09.13

Position	Number
Skilled worker (n=19)	47,1
Consultant (n=115)	43
Audiologist (n=16)	27,4
Medical student with license (n=5)	21
Secretary (n=588)	19,9
Other position (n=1)	17
Adviser (n=23)	13
Unit manager (n=131)	11,4
Senior physician (n=452)	7,6
Physician (n=278)	7
Engineer/technical position (n=4)	6,3
Head of Department (n=32)	5,7

Table 7 - Number of record lookup per decision template

Decision template	Count
Internal control / quality assurance	10031
Request from the patient's physician	6733
Supplementary work	4844
Order of documents from government and legal agencies and insurance companies	4375
Request from patient	3091
Reported patient	1410
External test results/notes for review	1315
Supervision in other departments	591
Request from the patient's relatives	512
Research	362
Emergency access	180
Patient access to information	91
IT system work	42
Total	33577

Discussion

Challenges

End users

Among the main challenges end users arrived at, the first half were placed in the general category of IT security, and the second half in administrative security, of which the majority was Internal, under Formal administrative security.

The two highest ranked challenges concerned the lack of appropriate implicit and explicit decision templates. Missing implicit templates are placed in the category Technical safety, as they are set by the vendor as default for all customers, while the challenge of too few explicit templates are placed in the category Internal, as new explicit templates can be ordered by the customer (health enterprise). These two challenges are logically connected, as lack of relevant implicit decision templates means that you do not automatically get access to the records you need, and thus must use exception mechanisms. When you try to get access via the exception mechanism named “greenlight access”, you get a list of decision templates, but based on respondents' answers, there should have been more decision templates, as the real reason for opening the records are not always found in the list they have access to. These challenges have thus consequences both for end users, who must spend time using exception mechanisms to bypass normal access control, and system managers, who review the logs for the use of the exception mechanisms. End users also think that it is an important challenge that you have to decide access too often. This suggests that the access control is not sufficiently tailored to adhere to treatment processes, which is seen in previous studies [1]. Exception mechanisms were used 33 577 times over a period of two months in the end users health enterprise, as shown in table 7. This number indicates that it must be difficult to follow up event logs, which corresponds to an interview survey [10] where it appears that the use of exception mechanisms is too large to be systematically followed up. If you also cannot rely on the decision template that is used to correctly indicate reason for opening the record, it seems at best unclear what value a log of this has. These challenges are previously described by Røstad [1] who analyzed an event log from Siemens DocuLive EHR, from eight hospitals in central Norway. Røstad also revealed a lack of predefined reasons for deciding access, and came with a recommendation for six new templates:

- Physician referrals.
- Hand over patient information to other hospital/health personnel on request.
- Request for information from a patient or next of kin.
- Release information to other external entity: insurance, legal, complaints.
- Out-patient clinic patient encounters.
- Patient not registered correctly in admin system (results in access denied, even though patient is physically present at ward).

In DIPS, decision templates with similar reason to the top four of these are included as standard for all health enterprises with decision based access, but there is still a need for more, according to the end users. If the Health enterprise defines a need, more templates can be ordered. The challenge, and a possible solution with regard to explicit decision templates, is therefore placed in the internal formal level.

When exception mechanisms are used extensively, the process of using them to gain access should therefore be simple and fast. Based on the factor A1-8 "It requires too many keystrokes to decide access" it may seem that this is not the case. It should be further investigated how many keystrokes is needed, and if this is something the vendor can reduce. End users' perception that exception mechanisms for access control occupy too much time and can be "annoying" is also described in previous studies [11].

The last factor directly linked to decision templates is factor A1-3; "User may choose wrong decision template". This is included in the category Informal. Wrong template may be used by mistake, lack of knowledge about which template is correct, or it can be a culture to select a random template, even if the user knows that the template does not match the cause for opening of the journal. The factor is also included in the category Computer security, as it ideally should be impossible for users to open a record, and choose a reason that is not correct, as this result in poor data quality in relation to monitoring of the event register.

The five remaining factors are placed in the category Internal, and are considered challenges that the health enterprise itself may influence, as they relate to education, or lack of such of end users. The relevant factors in ranked order are:

- Lack of clarity regarding the use of free text field when deciding access
- Insufficient education in access control
- Users lack understanding of decision based access
- Having to decide access gives a feeling of doing something illegal, and to be mistrusted and monitored
- When deciding access, you automatically only have access for one day

When one decides access, you must firstly choose a decision template you have access to, and then you may insert a justification in free text. This can be useful as an elaboration of the reason why you opened the record. It does not appear that it has been communicated to the end user how and in which cases this field should be used. The next three factors indicate that end users perceive that they have too little knowledge of access control, and therefore lack understanding of the use of decision based access, and the legislation that requires this to ensure patient privacy, which is a challenge identified in an earlier study [8]. The last of the formal internal factors "”When deciding access, you automatically only have access for one day" can also be attributed to lack of training and/or knowledge, when how many days one has access can be adjusted by the end user himself.

The seemingly lack of education in access control, coincides with an earlier study of information security in the health service in Norway, Finland and England, which points out that the most neglected area around information security, is user education [8].

Four factors; A1-1, A1-5 A1-8, and A1-10, indicates that increased time spent because of access control mechanisms are considered an important challenge for end users, and is consistent with previous studies [1,8,11].

System Managers

Among the key challenges system managers came up with, five are related to technical security, and four to administrative security, and most concerned challenges to the administration of user access.

Of the challenges related to technical security, we find the highest rated factor: "The interface of the administrator section of DIPS is too little intuitive and transparent" That the user interface is not perceived as sufficiently intuitive and straightforward, together with factor B1-5; "It is impossible/difficult to quickly get an overview of what access rights a particular user has" may affect both patient privacy and confidentiality if wrong permissions are granted, and you do not have an overview of what access a user is actually assigned.

It also seems as though system managers consider the granting of access rights involves many manual procedures, as the second highest ranked challenge is that access control is not integrated with the personnel system. Such an integration could be thought to reduce, if not eliminate, manual administration of user access, thus reducing human error related to granting and maintaining access.

System managers believe that there is insufficient support for log analysis. The event registers may contain a high volume of entries. It is therefore generally only taken random samples, or access logs for profiled personalities such as celebrities are reviewed, or access logs are printed at the request of the patient [10,12]. Without a systematic approach for log analysis you cannot effectively achieve adequate privacy when widespread use of exception mechanisms exists [8]. Software for pattern recognition may be used as a tool to analyze event logs to identify possible violations of patient privacy, and the use of this will clearly be an improvement from the current situation where there apparently is no automaticity in this.

The last factor under technical security is "Insufficient functionality for blocking access to journals”. Patients have a legal right to blocking of their medical record. If a patient objects to extradition of information, this must result in a denial of the relevant information in the EHR so that access control can take into account the patient's wishes. In what way functionality is insufficient is not evident in this study and should be investigated further, as a denial of access to records can result in a risk of errors in patient care if the end user does not have access to the necessary information, or violation of patient privacy, if the information is not in sufficiently inhibited [8].

Of the challenges that can be categorized under administrative security, system managers came up with three factors among the nine regarded most important:

- Defining the correct access profiles
- Little standardization of access control across health enterprises
- Adaptations to special permissions are challenging for system administrators

Defining the correct access profiles is mainly to set up the default permissions users may be given. As stated by the InfoSec model, one must deal with internal and external constraints, in the form of laws, rules and regulations, and internal policies for access control. The challenge here is to deal with all these guidelines, and simultaneously create default permissions that protect end user needs for access to information to ensure patient safety, while patients' privacy is protected. Norwegian laws and regulations and the EHR standard applies to all hospitals in Norway, but these provide only general guidelines for access control. Each health enterprise is responsible for its own access control. For system managers who manage access control across several health enterprises, it is therefore clear that there can be a challenge to deal with each health enterprises distinctive layout and guidelines for access control.

It is also clear that not everything can be standardized, either nationally, regionally or locally, and the goal of access control is not doing the job easy for system administrators to manage this, but to protect patients' privacy. There may be cases where local adaptations need to be made, and special permissions must be granted to individual employees who have a need for this in their work. The last factor, "Adaptations to special permissions are challenging for system administrators” puts the spotlight on this. This is a factor that may be useful to investigate in further studies, to clarify what factors make it difficult to adapt to special permissions, be it administrative and/or technical challenges.

Potential improvements

End Users

Of the possible improvements end users deem most important, the majority were categorized under technical security. The highest ranked factor is: "Upon referral from psychiatric to

somatic department, one should have access to the referral" The underlying problem is that record documents in DIPS are associated with electronic referrals, and employees of somatic departments do not have access to psychiatric documents. Therefore, end user can open the electronic referral, but not an associated document. The routine today is that documents are manually sent electronically to the recipient, so that an implicit decision template is activated and the recipient can access the document, even if the end user initially do not have access to this type of document. Giving access to psychiatric documents in general will solve the problem, but may not be a solution that protects patient privacy. This factor shows that the definition of rules and policies may be more complex than the design of technical solutions [8]. It is the author's opinion that the vendor and customer together should arrive at a solution so that both privacy and safety are protected.

The remaining factors under technical security are mainly related to ease of use, and can be characterized as a response to the previously mentioned challenges. This applies to, for example, reduction of clicks needed to decide access, and include examples of the use of free text fields when manually deciding access. One factor it may be interesting to note is A2-5; "Ability to choose what you get access to when deciding access". It would appear that end users demand an even more granulated access control. This could conceivably be relevant if for example an end user receive a request from the patients' general practitioner about what medicines he or she currently is using, and the end user can then decide access to only the patient's medication. Such functionality will safeguard patient privacy at a deeper level than the current access control enables.

System Managers

Of potential improvements system managers deem most important, one half were categorized under technical security, and the other under administrative security. Under technical security, two factors (B2-1 and B2-6) are related to a desire to increase usability regarding the administration of access control. This may influence both patient privacy and safety if the user interface can be made easier and more transparent to possibly reduce human errors when administrating access control. Factor B2-3; "The access control should be integrated with personnel system so that access is automatically generated " may even further reduce human error when creating user access, when all default permissions can be granted automatically when the end users managers registers the employee in the personnel system. Such a solution is scheduled to be operational in OUS, autumn 2014 [15]. Hopefully this can simplify user administration, and thus conceivably have a positive effect on both patient safety and privacy.

Of the four improvement proposals categorized under administrative security, three of the four factors (B2-2, B2-4 and B2-5) are in the category formal external, and these factors show that system managers clearly want a more general regional and national management of how the access control should be set up. These factors can be seen as a response to factor B1-4 "Little standardization of access control across health enterprises". Several of the regional health authorities aim to consolidate EHR databases, so that there is one database per regional health authority [16], [17].

The last factor, B2-8; "Active use of the access log for quality assurance" show that system managers are concerned about patient privacy, while also seeing that it is appropriate to improve the use of logs to ensure that end users do not abuse the trust they are given by unlawfully acquire confidential information. .

Comparison of the panels and general discussion

The two panels have an almost equal distribution of factors under administrative and technical security, but the further distribution of the subcategories show obvious differences. Only end users have informal factors, and only system managers have external factor. Furthermore, only system managers have factors that according to the InfoSec model can be categorized as data security. This shows that both end users and system administrators are primarily concerned with factors that affect them on a daily basis. End users are experts in the use of access control, while the system managers are experts in the administration of it. For access control to work there should be good communication between these two groups on a local, regional and national level [8]. This is especially important to keep in mind when entering a period of increased focus on standardization of EHR, including access control at a regional and possibly national level.

End users regarded the lack of decision templates as an important factor, but system managers did not. It appears that the lack of templates have not been communicated to system managers. This seems unfortunate as it results in users in certain situations have to register false reasons for opening records, when it in DIPS does not exist a decision template for "other reasons ", as it does in other EHR's [1]. End users in the Delphi survey wanted the ability to create custom decision templates (factor A2-3). Although the goal should be minimal use of exception mechanisms, such an alternative may be useful, and the system managers or others in the health enterprise may log its use. The log can be reviewed and one may be able to be proactive and ensure that frequently used reasons can be ordered as a new template.

Over a period of two months, exception mechanisms were used 33,397 times. Amongst these, only 180 were stated as emergency access. In addition, none of the major factors are related to directly hampering patient care as a result of limited access, and none of the experts believe that too wide permissions are the main challenges of access control. It is possible that this is due to the end users by using the green light access, and deciding access, basically have access to what they need.

Conclusion

This is a study of access control in the dominant EHR used in specialist health care in Norway. To carry out this study of existing access control was needed to understand the weaknesses of, and possible improvements in how decision based access is implemented and in use today, seen from both end users and system administrators' viewpoints.

Decision based access is implemented in a number of the country's health enterprises, and will soon be introduced in all, but challenges that have been identified in previous studies, are still present.

The Delphi survey also revealed factors that previous studies have not shown. To better protect patient safety and patient privacy, the interface for both end users and system administrators need to become more user friendly.

On the basis of the Delphi survey and extractions from the EHR database, the following administrative and technical challenges and possible improvements have been highlighted according to the two main categories of administrative and technical security from the extended InfoSec model:

Administrative Security Problems:

- Insufficient knowledge and understanding of access control
- Procedures for ordering and closing of user accesses are not complied
- Lack of communication of the need for new decision templates
- Access control is different in each health enterprise

Technical Security Problems:

- The access control is not sufficiently tailored to patient care
- Time consuming and cumbersome to decide access
- Excessive use of the exception mechanisms

Administrative Security Improvements:

- Education of end users on access control
- Communication between end users and system administrators to clarify the need for new decision templates
- Standardization of access control at regional and national level

Technical Security Improvements:

- The access control should be tailored to treatment processes by developing more implicit decision templates
- Systematic monitoring of event logs, possibly by using pattern recognition
- Simpler interface for end users using exception mechanisms
- Simpler interface for system administrators monitor for administration of access control
- Integration between personnel systems and EHR for automatic creation and closing of user access

The Extended InfoSec model has been useful to visualize the areas in which challenges and improvements of access control can be placed, showing that both administrative and technical challenges exist. It is according to the InfoSec model essential that all parts of the model where challenges have been identified must be followed up in order to obtain information security in the EHR. Administrative actions both inside and outside the organization that utilizes an EHR must be designed in a workable way, and they must also be complied with by well-functioning technical security measures.

Acknowledgements

The authors would like to thank Sørlandet Hospital health enterprise, and all respondents willing to participate in the study.

References

[1] Røstad L. Access Control in Healthcare Information Systems. PhD thesis. Norwegian University of Science and Technology; 2009

[2] Ferreira A, Cruz-Correia R, Antunes L, Chadwick D. Access control: how can it improve patients' healthcare? Stud Health Technol Inform 2007;127: 65-76

[3] Nystadnes T. EPJ Standard del 2: Tilgangsstyring, retting og sletting Vol. 6/05, 2007

[4] Helsedirektoratet. Norm for informasjonssikkerhet. http://helsedirektoratet.no/lover-regler/norm-for-informasjonssikkerhet/Sider/default.aspx (accessed 4 Jan 2014)

[5] Schmidt R. Managing Delphi surveys using nonparametric statistical techniques. Decision Sciences 1997;28(3): 763-774

[6] Okoli C, Pawlowski SD. The Delphi Method as a research tool: an example, design considerations and applications. Information & Management 2004;42(1): 15-29

[7] Hsieh HF, Shannon SE. Three Approaches to Qualitative Content Analysis. Qualitative Health Research 2005;15(9): 1277-1288

[8] Åhlfeldt RM. Information Security in Distributed Healthcare. PhD Thesis. Stockholm University; 2008

[9] Skulmoski, G.J, Hartman, F.T, Krahn, J. The Delphi method for graduate research. Journal of Information Technology Education 2007;6: 1–21.

[10] Andresen H. Tilgang til og videreformidling av helseopplysninger. PhD Thesis. University of Oslo; 2010

[11] Faxvaag A, Johansen TS, Heimly, V, Melby L. Grimsmo A. Healthcare Professionals' Experiences With EHR-System Access Control Mechanisms. Studies in Health Technology and Informatics 2011;169: 601-605.

[12] Innomed. Mønstergjenkjenning som metode for å oppdage taushetspliktbrudd ved bruk av pasientjournal. http://www.innomed.no/media/media/prosjekter/rapporter/56_-_Monstergjenkjenning.pdf (accessed 8 Feb 2014)

[13] Andresen H & Aasland OG. Helsepersonells håndtering av pasientopplysninger. Tidsskrift for den Norske legeforening 2008;128(24): 2823 – 7.

[14] Økland S. Haumann K.. & Christiansen RS. Urettmessig tilegnelse av taushetsbelagte opplysninger fra kliniske IT-systemer. Msc thesis. University of Agder: 2011

[15] DIPS. Forenklet brukeradministrasjon. http://dips.mediabok.no/113/index.html#14/z (accessed 10 Mar 2014)

[16] Andresen Ø. Moglegheiter for kvalitetsregister gjennom ny IKT. http://www.helse-bergen.no/fagfolk/forskning/Documents/kvalitetsregisterkonferansen%202013-%20postere%20foredrag/Registerkonferanse2013%20%C3%98rjan%20Andersen.pdf (accessed 21 Feb 2014)

[17] Finborud IM. Prosjekter gjennom tidene – hva har vi lært http://www.nasjonalikt.no/filestore/Arrangementer/Prosjektledersamling_2014/IngerM.Finborud_ProsjektarbeidiHelseSrst.pdf (accessed 18 Mar 2014)

Address for correspondence
Rune Hystad
Klomreheia 13B
4885 Grimstad
runeh11@student.uia.no