Factors of Access Control Management in Electronic Healthcare: The Patients' Perspective

Thomas Trojer, Basel Katt, Tülay Özata, Ruth Breu
Institute of Computer Science
University of Innsbruck, Austria
{thomas.trojer, basel.katt, ruth.breu}@uibk.ac.at

Patrick Mangesius, Thomas Schabetsberger
ITH-icoserve technology for healthcare, Austria
{patrick.mangesius, thomas.schabetsberger}
@ith-icoserve.com

Abstract

Information systems in electronic healthcare have the potential to support a variety of medical stakeholders in performing their regular daily working activities. Still with the growing amount of electronically available health-related data on patients, aspects of data privacy have to be considered, e.g., by improving the transparency of healthcare processes or by offering methods to allow patients to self-determine controls for their data. In this work we present the results of a study we conducted in Austria about the general desire of patients to self-control access to their health records as well as to elicit typical factors for access control they personally consider as important. The results we present in this work are intended to support the requirements analysis and development of patient-centric healthcare management applications. As our results clearly indicate that patients have varying conceptions regarding privacy we also elaborate on the proper integration of access control factors to satisfy individual informational requirements.

1. Introduction

Today, information systems in electronic healthcare play an important role to support the daily working activities of medical personnel. These information systems, in order to be effective, have to consolidate and provide medical data on patients that have typically been collected at a number of different medical institutions. Maintaining such a holistic view about patients' individual health status, poses, besides others, several privacy-related challenges.

As privacy represents a personal concern and added by the high sensitivity of health-related data, we believe that the principles of patient-centric care [1], especially regarding the maintenance of health data, have to be fostered. This means taking into account the individual desires of patients to control access to their data by themselves [2]. We assume that the integration of such patient-related aspects is a key enabler for the success and wide acceptance of healthcare information systems [3].

Nevertheless healthcare related processes typically involve a multitude of different stakeholders, like patients, practitioners, care personnel or pharmacists, all having different informational needs. Reaching the state where an electronic healthcare information system reflects these needs properly it can be attributed with a high degree of effectiveness and targeting high quality of care, potentially lowering costs of healthcare services [4] and also offering better transparency for patients. In this specific work we tackle the latter attribute by evaluating the patients' needs and desires regarding data privacy and access control management. In order to obtain the patients' viewpoints we conducted an empirical study.

1.1. Online Questionnaire

The study is based on an online questionnaire and involves a two-step approach to elicit access control requirements for electronic health records:

First, general opinion-based questions are asked to establish a basic demography of participants regarding their conception of privacy. We were e.g., interested how sensitive patients consider their personal health data or if patients would be willing to use an online portal application to maintain their health data and control access to it.

In the second step, our goal was to determine protecting measures for personal health data in the context of specific use-case scenarios. Here we intended to collect a set of generic access control factors that are important to patients and furthermore to estimate how they would actually employ these factors when managing access control for their data.

For each of the provided use-case scenarios we asked the survey participants to make free-text statements (i.e. via open-ended questions) about access protections they individually feel implied in these situations. These statements allowed for analysis and interpretation by means of reflecting the individual privacy conceptions of patients.

978-1-4799-2504-9/14 $31.00 © 2014 IEEE
DOI 10.1109/HICSS.2014.369

Each of the received statements has been evaluated manually and coded according to common attributes they describe. The set of attributes has been built incrementally as we proceeded with the provided answers. This eventually yielded an overview of access control factors of different granularity based on the perceived importance of factors to patients.

The survey has been distributed at the end of 2012 in Austria and has been accessible for about one month. The survey language has been German. In total we received 719 responses of which 513 have been completed, giving a dropout rate of 28.7% (n = 719). Further due to the extensive use of open-ended questions in the scenario-related part of the questionnaire, not all completed responses were evaluable. Still only a minority of respondents (on average 3.12%, $\sigma = 0.58\%$) left these questions blank or provided unclear or internally conflicting answers. The obtained low percentage of missing answers signals that the topic has been generally perceived as important by the respondents.

The decision to extensively use open-ended questions was made as it allowed us to combine both, quantitative value due to the ease of disseminating online surveys and increased data quality and reliability due to the minimized influence of respondents by our own opinion as researchers [5].

On the other hand open-ended questions are sensitive to bias, as each answer has to be interpreted and related to a coding schema. In order to minimize bias we avoided broadly scoped questions, therefore narrowing the range of possible answers. This way we mostly received unambiguous answers which we were able to map directly or at least code without difficulty.

1.2. Research Questions

The following research questions have mainly driven the design of the survey:

1. To what degree do patients wish to have control over their health data?
2. How strongly does the general conception of privacy vary between patients?
3. What are typical factors for access control management which patients feel comfortable with?

1.3. Demographics

Gender, corresponding age groups as well as individual levels of computer literacy have been evaluated as basic demographic attributes of respondents.

Table 1. Respondents by age group

Age group [years]	*Count*	*Percentage*
< 20	79	15.4%
20 – 29	272	53.0%
30 – 39	88	17.2%
40 – 49	46	9.0%
50 – 59	18	3.5%
≥ 60	10	1.9%

54.6% of responses (n = 513[1]) were received by female, 45.4% by male participants. We set individual age groups in steps of 10 years and encountered frequencies of responses as listed in Table 1.

Because of the initial distribution via online platforms, like Facebook and due to the use of our university survey distribution facilities, the resulting median age group is relatively low at 20 – 29 years. Still even for ages above 60 years, yielding the lowest response rate, we received in total 10 completed survey responses.

As no restrictions to the target group of potential survey participants applied, we further intensively used word-of-mouth advertising and arbitrary mailing lists we have access to in order to distribute the questionnaire.

Besides gender and age we asked all participants to state how computer literate they consider themselves and if they are using the internet on a regular basis. 57.5% expressed this by choosing the option regarding good computer knowledge. All other respondents at least described themselves as averagely experienced computer and internet users. This picture has been expected and is to some extent obvious due to the online nature of the conducted survey.

2. Patient-specific Results

In the following section we present results about the individual conceptions of privacy as well as the desire of patients to self-determine access control for their health data (cf. Research Question 1).

2.1. Healthcare Demographics

In order to determine the need of healthcare portal applications to control and maintain personal health data, we were interested how often individual patients visit different healthcare institutions. Specifically we asked about the number of institutions that have been visited within the last 10 years. Our assumption here

[1] If not explicitly stated the number of responses (n) is 513.

was that the more different healthcare institutions are visited, healthcare data management can increasingly benefit from central administration. Employing applications that connect healthcare related stakeholders to patients' health data may then in turn contribute to the effectiveness of the provided healthcare services, as the sharing of data can be greatly simplified.

While for respondents of age between 20 and 29 years it is more common that no medical institutions have been visited at all (9.93%), this changes as participants grow older – e.g., in the group of respondents of age 40 years or above, only one out of a total of 74 responses (1.35%) stated that no medical practitioners have been visited within 10 years. Further in the same group we received 3 responses stating exceptionally high amounts of visits, namely 20 or above. The highest reported value of visitations of unique medical institutions was 43.

For younger age groups (i.e. below 30) a median visitation of 1 to 5 different institutions has been reported. Respondents of age 30 years and above visit a median of 6 to 10 different medical institutions. Only age group 50 to 59 years has been an exception to this, also reporting a lower median of 1 to 5 practitioner visits. In total close to half of all responses (42.3%) stated that 6 or more unique medical institutions have been visited. These numbers clearly show that individual patients receive medical care at different institutions, underlining the need for transparency and effective control of privacy and corresponding access control settings.

Further we directly asked the survey participants about their actual desire to have a dedicated portal application for health data management. Here, 84% described that they would be willing to use such an application to manage their personal health records. Within this specific group many (43%, n = 480) reported that they support the idea of a healthcare portal application, as they are already used to other electronic services provided by the government, such as to make their annual tax declarations. Prior experience with these kinds of national service applications in Austria may have contributed to the high percentage obtained. Further in Austria all citizens are mandatorily health insured with public insurers; no personal choices about the basic level of medical care are possible. Therefore the healthcare domain is usually strongly associated with the government and so it can be assumed that shifting control of health data towards patients may be received positively. We are aware that this specific result may vary across countries. Still the purpose of this work about revealing patient-intended access control requirements is not necessarily influenced by this.

Additionally we were interested in differences between age groups and potentially different desires to have patient-centric portal applications. Therefore we conducted a one-way analysis of variance (ANOVA) with age group being the independent variable. This analysis revealed that the desire of patients to have portal application in place is not significantly different across age groups ($F(5,474) = 0.804$, $p = 0.58$).

2.2. Management of health data

By assuming that healthcare portal applications are in place already, we asked participants whether it would be important for them to control how their data is going to be used. For only 3.1% of respondents personal control is not important at all. On the contrary, 83.4% explicitly mentioned that self-control of their data is an important aspect to them.

As health records are generally considered sensitive (cf. Article 8 (1) of the EU Directive 95/46/EC [6]), knowing who accessed personal data is important. Respondents expressed that having knowledge about occurred accesses to their data is similarly important (85.9%) than control is to them. Further 38.3% (n = 441) within this group mentioned that information about accesses are valuable in order to derive measures of control for future accesses to personal data.

However the overall success of electronic healthcare services does not only depend on the implementation of patient-desired data protection. Their effectiveness – already improved due to the modern ways of using electronic services and digital data [7] – relies on a balance between various informational requirements of all participating stakeholders. As we have seen, privacy by means of access-protecting personal data is specifically a requirement from a patients' perspective. But in order to guarantee effectiveness, health data has to be accessible to medical personnel; namely for a range of reasons, like to support regular medical treatments, the creation of prescriptions or in emergency situations where practitioners need to more or less freely act upon available medical data.

Interestingly, the importance of this balance between privacy and effectiveness seems to be well-understood by our survey respondents. A total of 97.8% stated that they are willing to share their data with practitioners and other medical institutions, at least under certain conditions. Only 9 respondents (1.8%) made a general statement about refusing to share any of their health data.

The results presented in this section indicate that sharing health data between medical stakeholders is broadly supported by patients as long as healthcare portal applications provide appropriate data access

management functionality and allow patients to perform audits on occurred accesses to their data.

2.3. General Perception of Privacy

All survey respondents stated that they perceive either all or some parts of their personal health record as sensitive. Related to this, nearly all (95.5%) respondents consider the protection of their personal health data as important.

The importance of data protection is rooted in this high sensitivity of health data, but this is even further increased as the majority of respondents state that they are concerned about potential misuse of their data by unauthorized persons (66.6%). Employers and private insurers have been mentioned as examples where granted access to data is unwanted.

In order to determine if these concerns are stronger for the group of people not supporting the idea of electronic health portals in general, we conducted a correlation analysis (Spearman's rank coefficient between concern and desire to have a healthcare portal application). This analysis yielded a significant result indicating no correlation ($r_S = 0.078$, $p = 0.044$) between the groups.

Therein, together with the high percentage of responses supporting the idea of patient-centric healthcare portals, we see that although people are concerned they also feel that the potential benefits overweigh.

2.4. Types of Access Control Factors

We asked participants about certain factors of access control they find more or less appropriate to protect personal health documents. These factors are based on various related work [8–11] that describe potential factors for access control in electronic healthcare systems. The specific set of factors we selected for this questionnaire intends to cover a range from being strongly related to healthcare domain knowledge towards being entirely patient-related.

Figure 1 depicts these access factors in the order of importance stated by respondents, which is determined by the sum of percentages for *"important"* and *"very important"* answers. Each factor in the table is labeled with either *"P"* representing a patient-related factor, *"H"* marking a healthcare domain related factor and *"0"* for factors somewhere in-between *"P"* and *"H"*. These labels have been hidden in the published survey itself.

Based on all of these factors access control management functionality can be implemented. E.g., restricting access to data according to its type can be considered a management feature, although less

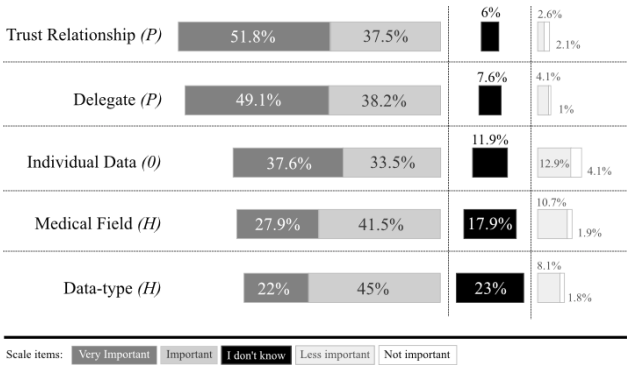

Figure 1. Types of access control factors

important to respondents than determining access decisions based on selected individual records or the assigned level of trust to a practitioner.

Figure 1 clearly shows that patient-related factors are in favor over healthcare domain related factors for managing access control. Hence the lower percentages for individually selectable data (37.6% said this factor is very important), medical field of expertise (27.9% responded very important) and types of data (22%) can possibly be explained due to the increased amount of healthcare domain knowledge a patient is required to have in order to determine access decisions appropriately. Typically patients cannot be considered medical experts and therefore lack required knowledge about the degree of usefulness of (certain types of) health data to a specific practitioner. On the other hand we see that patients are easily able to draw conclusions about who they trust or not, as approximately 50% of respondents stated that both trust and delegation is very important.

The fact that respondents feel less comfortable with healthcare domain related factors due to the potential absence of required domain knowledge can also be seen in the increasing number of answers where respondents stated that they do not really know if the factor is important or not (cf. Figure 1, *"I don't know"*).

The factor most often mentioned has been trust relationship. 89.3% of respondents consider it important. This factor summarizes answers to a variety of questions we asked about trust: We wanted to know about the importance of deciding on a family practitioner, what specialists are regularly visited or even if it is considered important to define what practitioners are no longer visited.

The factor second most often selected has been about defining a delegate. Delegation is the process of selecting an individual person, e.g., a relative, who in turn replaces the patient in controlling her health data. This is useful in exceptional situations, like disability or in cases where legal guardians are responsible for

patients, e.g., in the context of mentally ill, elderly or underage people.

Results presented in this section show that individual factors of access control can be associated with different stakeholders. As this association describes how well a factor is comprehended by a group of users, it is important to develop access control management functionality accordingly.

2.5. Granularity of Control

For the two patient-related access factors, trust relationships and delegation abilities, we further provide detail about the granularity of control which patients requested. For each of these factors an extensive enumeration of options has been provided to the respondents.

245 responses have been received that describe a desire to further detail access control decisions related to trust relationships. Table 2 lists all factors of granular control ordered by their number of occurrences.

Table 2. Granular access control related to trust relationships (n = 245).

Granular control	*Count*	*Percentage*
Frequency of visitations	156	63.7%
Incident-based	149	60.8%
Individual data	95	38.8%
Medical field	94	38.4%
Types of data	93	38.0%
Location-based	53	21.6%
Time-based	46	18.8%

Most of the respondents (63.7%, n = 245) mentioned that they would consider the frequency of visitations to decide about appropriate trust labels and their implied access decisions for health records. A similar amount of responses (149) describe that it would be useful to base access decisions on certain incidents, like e.g., an upcoming treatment session or the change of a family practitioner. Granular access decisions based on individual data, types of data or medical field have been named by approximately a third of all respondents. Only a minority found location (21.6%, n = 245) or time-based attributes (18.8%, n = 245) useful to detail trust-based access decisions.

Respondents who found the definition and use of delegates important were asked, besides granular access control factors, who they would consider as appropriate subjects for delegation. Family members ranked first with 92.9% of selections by respondents. Both, family practitioners and friends were chosen in about half of the responses (56.3% and 45.2% respectively). Only a minority of about 10% describes medical or care institutions as prospective delegates. Other potential delegates some respondents named were custodians, psychotherapists or ministers of a church.

Clearly delegation implies a strong trust relationship between delegators and delegates which may explain the frequent reference to family members as the most appropriate candidates.

We again asked respondents to provide potential factors for granular control of delegation rights. 68 responses were received and summarized in Table 3.

Table 3. Granular access control for delegates (n = 68).

Granular control	*Count*	*Percentage*
Time-based	38	55.9%
Incident-based	21	30.9%
Types of data	9	13.2%
Location-based	4	5.9%

Mostly participants requested restriction to the control of health data by delegates within a certain time period (55.9%, n = 68). Also emergency hospital stays, or sick leaves from work have been frequently named (30.9%, n = 68) and constitute the incident-based factors for access control decisions. Only a small minority of respondents found that delegation rights restricted by types of data (13.2%, n = 68) or in a location-based manner (5.9%, n = 68) are desirable.

3. Use-case Scenario-based Results

The second part of our online survey consisted of questions regarding the individual conception and actual application of access control settings in different contexts. Therefore we defined three use-case scenarios that are common to the medical domain and which usually imply certain access control considerations. The use-case scenarios we selected represent the

- Selection of a family practitioner
- Removal of a trust relationship
- Creation of a medical referral

The first two scenarios reflect activities that are typically carried out by patients, i.e. our survey respondents. Here we intended to find out about specifically articulated access decisions which are desired to be in place. Another goal was to determine factors of access decisions which are shared by

respondents and those which vary and have a less common understanding by respondents.

The third scenario, creation of a medical referral, defines an activity related to medical practitioners. Here we intended to find out how patients would design the process of medical referrals and to see what they imagine being important factors for the protection of their data.

The questions for all of these scenarios have been designed open-ended. For each scenario we provided a sketch of a possible user interface, together with some textual description about the actual activity and its purpose. We then asked the participants what access decisions they desire. Some guidance the participants received noted that their answers should list all stakeholders which they think play a part in the scenario, all health data that is managed and arbitrary factors of control which should apply.

3.1. Patient-specific Stereotypes

After evaluating all free-text statements provided by the respondents, we were able to roughly assign and relate participants according to their general willingness to share their data to one of the following three stereotypes (cf. Research Question 2):

- Responsible patient
- Balance-advocating patient
- Privacy-sacrificing patient

Individuals related to the first type propose that due to the sensitivity of health-related data, self-determination is to be put first. Some responses shared the phrase *"responsible citizen"* to indicate their desire to have full control. We therefore re-used this phrase to name this group.

Balance-advocating patients care about data privacy, but additionally find that not all decisions can be made by themselves without consequences regarding an optimal medical treatment. This group implicitly supports the idea of having a balance between privacy and effectiveness.

The third group represents respondents who believe that medical personnel know best and who consider the healthcare domain generally to be a trustful one. This group unifies respondents who e.g., mentioned that they do not really care to decide or who do not feel comfortable in making access decisions by themselves.

3.2. Selection of a family practitioner

The use-case scenario representing the selection of a family practitioner is common to healthcare in general and allows a patient to express a high level of trust in a medical practitioner. We asked patients to describe their personal desire regarding protections and control of their health data in this specific context.

Table 4. Granular access control for selected family practitioners (n = 191).

Granular control	*Count*	*Percentage*
All data	119	62.3%
Consent-based	45	23.6%
Relevancy	15	7.9%
Types of data	15	7.9%
Time-based	13	6.8%
Never all data	11	5.8%
Frequency of visitations	10	5.2%
Delegate	4	2.1%
Other restrictions	13	6.8%

We received 495 responses containing valid free-text statements about individual access control decisions. For example one participant responded *"How can a family practitioner work efficiently, if not provided with all data on a patient?"* (i.e. privacy-sacrificing citizen).

Another statement was *"I don't think that my family practitioner needs to know everything at any time. If I have a cold, e.g., why should unrelated clinical data be visible too?"* (i.e. balance-advocating citizen).

Each of the responses has been evaluated and categorized manually and the results are provided in the following paragraphs.

Obviously all valid statements contained a decision on whether the selected family practitioner should be permitted, at least partially, to access health records of the patient. Only 7 respondents (1.4%, n = 495) stated that a family practitioner should not receive any rights at all to access data. We interpret these responses as reflecting the opinion that the scenario of selecting a family practitioner, for them, is undesirable in the context patient-centric electronic healthcare.

488 responses (98.6%, n = 495) grant access rights to trusted practitioners and therein 191 participants (38.6%, n = 495) additionally mentioned granular access control factors they would want to be in place. These granular factors, ordered by their number of occurrences, are listed in Table 4.

The majority of respondents (62.3%, n = 191) said that they can imagine that their family practitioner has access to their entire health record, potentially under certain conditions. Such a condition would be that the trust label a practitioner earned is still valid at the given time of access (6.8%, n = 191).

Another condition factor for access that has been frequently mentioned is consent (23.6%, n = 191). Two

Table 5. Granular access control for creating medical referrals (n = 168).

Granular control	*Count*	*Percentage*
Relevance	64	38.1%
Time-based	39	23.2%
Types of data	37	22%
Consent-based	28	16.7%
All data	23	13.7%

different meanings of consent have been encountered. Roughly 93% (n = 49) described consent as their unique right to eventually decide about each attempt of access or sharing of data. 7% (n = 49) stated that they do not want to approve each individual request, but want to get notified about data accesses performed by the family practitioner. In Table 4 we did not count the latter definition of consent as it does not represent an actual factor for access control.

Few responses proposed to use the type of data or the relevance of data for a specific kind of medical treatment as granular control factors. 6.8% of responses stated the desire to have some sort of restricted access for family practitioners, but did not make any clear statements about the type of restriction they intend to be applied.

3.3. Creation of a medical referral

The creation of a medical referral is an activity carried out by a practitioner and reflects the suggestion made to a patient to visit another physician, typically a specialist, for the purpose of further medical consultation. We assumed that electronic medical referrals allow a practitioner to access data of a patient and potentially share it with the target practitioner. This specific aspect of sharing data was explained to survey participants within the published survey. Again each respondent has been asked about her personal desire regarding access control measures and was allowed to openly share an opinion with us.

Some statements we collected were as follows:

"I want both practitioners to have a complete view on all of my health records. But I want to be informed about what data they actually access." (i.e. privacy-sacrificing citizen, although notification about accesses is requested).

A statement clearly related to the responsible-patient stereotype has been *"I am feeling responsible for all of my actions, this, of course, includes health-related matters. It should be my decision what data is shared with whom, at any time"*.

Another participant wrote *"Why should my dentist see data from my oncologist? I want him to only access the records which are relevant in my actual case."* (i.e. balance-advocating citizen).

Table 6. Granular access factors when removing trust relationships (n = 81).

Granular control	*Count*	*Percentage*
Authorship	58	71.6%
Consent	29	35.8%
Time-based	10	12.3%

The question regarding access control requirements for this type of scenario yielded in total 497 responses. A multitude of stakeholders may be involved in a medical referral process and respondents granted them access rights differently.

A majority of 85.1% (n = 497) stated that the targeted practitioner should gain access to health data. On the contrary only two respondents (0.4%, n = 497) explicitly stated the opposite. Both similarly described that they would like to print the referral together with self-selected health data and bring it with them to the target practitioner. We again interpret this as the opinion that electronic medical referrals are not considered useful by this specific group of respondents to be implemented.

81.3% of responses (n = 497) contained that patients have to receive access privileges in order to make the referral process transparent. Finally only 22.6% (n = 497) explicitly requested access for the referring practitioner. The relatively small percentage regarding permissions for a referring practitioner may indicate that this is less obviously considered by patients compared to defining access decisions for themselves and the target practitioner.

The granular control factors, provided by 168 respondents, are listed in Table 5. In the context of medical referrals these factors are much more distributed compared to access factors regarding selected family practitioners. Still a relative majority (38.1%, n = 168) of respondents pointed out that the relevance of shared data in an actual treatment is important. The lowest rate of responses described the setting in which all data is shared with the involved practitioners (13.7%, n = 168).

Time-based constraints (23.2%, n = 168) for access have been encountered in two kinds: The majority of responses in this category described that access shall be restricted once the specific treatment ends or when a certain time period has passed after ending the treatment. A few respondents mentioned an arbitrary fixed time period in which the data shall be accessible for the practitioners.

Again, also different types of consent definitions have been received: 29.7% (n = 36) said that the

referring practitioner together with the patient should decide what data to be shared. 47.6% (n = 36), reflecting the relative majority of responses regarding consent, stated that only the patient should have control what data is shared. Finally 22.6% (n = 36) requested to be notified about the sharing of data and accesses to it as part of the referral activity. Again these responses have not been added to the consent-based factor of granular control as provided in Table 5.

Besides these granular factors, many respondents additionally pointed out that default rules should apply for this scenario initially. This indicates, potentially also supported by the high distribution of responses across the different factors, that patients do not feel comfortable to decide about appropriate settings in this practitioner-related scenario.

3.4. Removing trust labels

Another scenario we found interesting to be evaluated is the case a trust relationship changes or is not present anymore. Change in trust occurs e.g., if the patient selects a new family practitioner or a patient decides not to visit a physician again.

500 valid responses have been received for this scenario. One respondent said *"I want to have my current family practitioner to keep access rights until I have visited a new one."*

Another response stated that *"[the practitioner] shall keep accessing all data he created, but no future data anymore."*

We rate both statements as reflecting balance-advocating patients, as they explicitly consider situations in which access is required together with ones where access may not be necessary anymore.

5% (n = 500) of the respondents did not find the scenario to be required, stating that the removal of access rights shall not be performed by patients at all.

70.1% (n = 500) explicitly stated that the respective practitioner shall be restricted in accessing data in some way. Further, granular factors of control have been mentioned by 81 respondents and are listed in Table 6.

Time-based granular control has been mentioned least frequent (12.3%, n = 81). Here respondents intended to provide a formerly trusted practitioner with access rights valid at least till some time into the future. It has been stated that e.g., when moving to a new home it would be useful to still have the former family practitioner being able to access data during this transition period; emergencies have been mentioned as main reason for this. 35.8% (n = 81) stated that whether they want to establish restrictions to all of their data, only to parts of it or no restrictions at all depends on the actual case and that they want to decide individually (i.e. consent). The majority (71.6%, n = 81) of responses granted access permissions to the practitioner as long as data was originally created by her (i.e. authorship).

3.5. Taxonomy of Access Control Factors

In Figure 2 we provide a taxonomy summarizing all access control factors that were named by respondents and which we collected and coded as part of our study (cf. Research Question 3). We group them according to their relationship between stakeholders being part of electronic healthcare processes (*within-subjects* group), their reflection of properties of health data (*within-resources* group), correlations between stakeholders and health data (*between-subjects-resources* group) as well as *external* factors. Further each factor is again tagged by its relatedness to either the healthcare or patient domain. The newly introduced type *"-"*, means that the factor is generic in the sense that it is either implicit or cannot specifically be related to patient domain or the healthcare domain.

4. Related Work

Only little work has been done so far which empirically derives what access control actually means to non-expert stakeholders, like patients in electronic healthcare. Access control models are typically designed in a way to cope with domain characteristics.

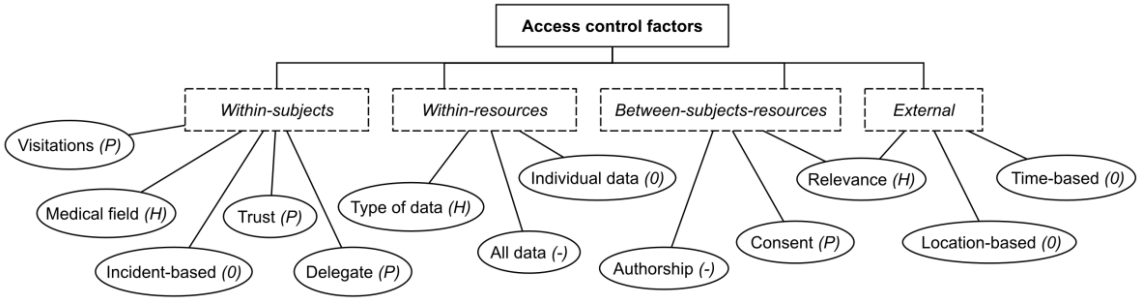

Figure 2. Taxonomy of Access Control Factors.

For instance Role-based Access Control (RBAC) [12] reflects working roles together with their privileges to access data and also considers the concept of separation of duties. Attribute-based Access Control (ABAC) [13], on the other hand, allows defining access decisions based on arbitrary domain predicates and relations between them. Although the usefulness of these models is beyond any doubt from an application's perspective, it is not always clear how access control management is intended and performed, especially by non-expert users [14].

The work of Kumaraguru and Cranor [15] discusses study results of Alan Westin, who has conducted over 30 privacy surveys since 1970 in order to establish privacy indexes. Similar to our work Westin used these indexes to classify people into groups, namely *"Fundamentalist"*, *"Pragmatist"* and *"Unconcerned"*. Our survey, on the other hand, targets the electronic healthcare domain and intends to group patients according to their desire to self-determine access control measures, rather than reflecting their general attitude towards privacy. Furthermore we aim at studying particular access control factors that can be considered important when developing patient-centric healthcare applications.

The work of Caine and Hanania [16] provides evidence that patients want to decide which information about them is shared with whom. Whereas their work focuses on specific types of less or more sensitive information items, our goal is to determine actual factors for protecting arbitrary health-related data. Still similar conclusions about the preference of patients to have control about their data are drawn.

Finally the study by Pyper et al. [17] also revealed that the majority of patients want to decide about access to their data, but opposed to our work, they encountered this fact to be decreasing with age. Especially within older age groups there may be a large discrepancy between actual participants of our online survey and other potentially less computer literate persons. Therefore this specific result has to be treated with increased caution, as it depends on the actual survey method which in turn defines and limits the set of prospective participants.

5. Conclusion and Future Work

Clearly, while the main access control factors regarding individual access decisions have shown to be similar across the survey, different scenarios ultimately yield different desires in data protection measures. We consider scenario-based software development [18], especially by integrating the underlying authorization characteristics [19] to be a potentially useful methodology applicable during the design of patient-centric portal applications.

Another promising method is context-aware access control (like described by Kulkarni and Tripathi [20]). Here access control decisions can be defined in ways to depend on the actual stakeholder and therefore reflect individually desired factors of access control.

In the second part of the survey, we intentionally mixed a medical-practitioner related scenario (namely the creation of a medical referral), with patient-specific ones. Although not comparable by their individual goals, it still gets visible that intended access control decisions for the practitioner-related scenario have greater variability than the ones which are patient-related. Based on this we derive that the design of healthcare applications has to be driven by concepts and terminology which are familiar to each individual stakeholder (cf. the work of Brodie et al. [21]). In the case of patient-centric applications, besides considering different use-case scenarios, our taxonomy of access control factors (see Figure 2) can be used to determine the factors which will be most suitable for patients to be self-determined (i.e. factors tagged with *"P"* and additionally the ones with *"0"*). We further propose that if healthcare domain related factors (tagged with *"H"*) are additionally required in the context of a patient-specific scenario, good defaults should replace or support the manual administration otherwise performed by a patient.

Besides stakeholder-related characteristics we also believe that staged and alternative designs of portal applications are required.

By staged design [22] we intend a process where patients can gradually evolve by deciding about the range and complexity of access control factors they want to use. In a first stage patients may, e.g., simply be able to select a family practitioner and this in turn would automatically lead to access permissions for all of the patient's health data. Optionally, a patient may select that consent-based access to her data should be initiated. In this stage the two factors that have been most frequently stated for this scenario would be covered. In a second stage the setting of a time period could be allowed and in a third one only individually selected data would be made accessible to the chosen practitioner. A staged design of patient-centric portal applications will therefore allow to incrementally cover all access control factors desired by patients.

By suggesting alternative designs on the other hand, our goal is to satisfy privacy conceptions of the three stereotypical groups of respondents we were able to classify. Patients e.g., can be asked on first login to their personal health record application whether they want to have full control, balanced access decisions or

if they feel it is sufficient when default rules apply, respectively.

The first two alternatives are challenging as we have to assume that settings predominantly managed by patients increase the risk of lowered effectiveness of particular healthcare services due to data potentially rendered inaccessible or proper privacy protection of patients. Therefore an inherent part of non-expert managed access control is sophisticated analysis of authorization settings. Regardless of the corresponding stereotype of a patient, the portal application has to provide warnings if access control diverges from a privacy – effectiveness balance. E.g., a patient sharing her entire health data with practitioners not having a certain trust level should be warned to consider employing more restrictive settings. On the other hand restrictions for practitioners who will require access to certain data as part of a treatment should be highlighted and questioned as well. This form of analysis and feedback may educate users over time about the appropriate handling of sensitive health data, both, regarding privacy and to properly comply with the informational demands of the healthcare personnel.

Based on the results of this work we started to actually implement patient-centric healthcare portal applications both allowing patients to maintain access rights to their data as well as providing interfaces for practitioners. In these applications all implemented administration functionality will rely on factors of our taxonomy of stakeholder related access control. Usability is a specific concern in this ongoing work. Therefore a user study evaluating our implemented prototype will be a complement to this work. This future study will also show the actual applicability of the proposed factors and describe our experiences with the applied development process involving staged and alternative designs.

6. References

[1] C. Bechtel and D. L. Ness, "If you build it, will they come? Designing truly patient-centered health care.," *Health affairs (Project Hope)*, vol. 29, no. 5, 2010.

[2] T. Rindfleisch, "Privacy, information technology, and health care," *Communications of the ACM*, vol. 40, no. 8, 1997.

[3] L. Buccoliero, E. Bellio, and A. Prenestini, "Patient Web Empowerment Index (PWEI): 2009-2011 Evaluation of Italian NHS Hospitals Web Strategies," *46th Hawaii International Conference on System Sciences*, 2013.

[4] R. Hillestad, J. Bigelow, A. Bower, F. Girosi, R. Meili, R. Scoville, and R. Taylor, "Can electronic medical record systems transform health care? Potential health benefits, savings, and costs.," *Health affairs (Project Hope)*, vol. 24, no. 5, 2005.

[5] U. Reja, K. L. Manfreda, and V. Hlebec, "Open-ended vs. Close-ended Questions in Web Questionnaires," in *Developments in Applied Statistics*, 2003.

[6] European Commision, "Directive 95/46/EC" 1995.

[7] T. Schabetsberger, E. Ammenwerth, S. Andreatta, G. Gratl, R. Haux, G. Lechleitner, K. Schindelwig, C. Stark, R. Vogl, I. Wilhelmy, and F. Wozak, "From a paper-based transmission of discharge summaries to electronic communication in health care regions.," *International journal of medical informatics*, vol. 75, no. 3–4, 2006.

[8] B. Blobel, "Authorisation and access control for electronic health record systems," *International Journal of Medical Informatics*, vol. 73, no. 3, 2004.

[9] L. J. Muzzin, "Understanding the Process of Medical Referral," *Canadian Family Physician*, vol. 37, 1991.

[10] ISO/HL7, "ISO/HL7 27932:2009 - Data Exchange Standards - HL7 Clinical Document Architecture, R2".

[11] L. Zhang, G.-J. Ahn, and B.-T. Chu, "A role-based delegation framework for healthcare information systems," *SACMAT*, 2002.

[12] R. Sandhu, E. Coyne, H. Feinstein, and C. Youman, "Role-Based Access Control Models," *Computer*, vol. 29, 1996.

[13] L. Wang, D. Wijesekera, and S. Jajodia, "A logic-based framework for attribute based access control," *FMSE*, 2004.

[14] T. Whalen, D. Smetters, and E. F. Churchill, "User experiences with sharing and access control," *CHI*, 2006.

[15] P. Kumaraguru and L. Cranor, *Privacy indexes : a survey of Westin's studies*. 2005.

[16] K. Caine and R. Hanania, "Patients want granular privacy control over health information in electronic medical records.," *JAMIA*, vol. 20, no. 1, 2013.

[17] C. Pyper, J. Amery, M. Watson, and C. Crook, "Access to electronic health records in primary care-a survey of patients' views.," *Medical science monitor : international medical journal of experimental and clinical research*, vol. 10, no. 11, 2004.

[18] J. M. Carroll, "Five reasons for scenario-based design," *Interacting with Computers*, vol. 13, no. 1, 2000.

[19] T. Trojer, B. Katt, R. Breu, T. Schabetsberger, and R. Mair, "Scenario-based Templates supporting Usable Privacy Policy Authoring," *IWEES*, 2012.

[20] D. Kulkarni and A. Tripathi, "Context-aware role-based access control in pervasive computing systems," *SACMAT*, 2008.

[21] C. A. Brodie, C.-M. Karat, and J. Karat, "An empirical study of natural language parsing of privacy policy rules using the SPARCLE policy workbench," SOUPS, 2006.

[22] A. Whitten, "Safe Staging for Computer Security," in *In Proceedings of the Workshop on Human-Computer Interaction and Security Systems, CHI,* 2003.