一般口演
# 一般口演11
# セキュリティとプライバシー保護2
2017年11月21日(火) 16:00 ～ 17:30 H会場 (10F 会議室1008)

## [2-H-3-OP11-2] Reducing Patient Privacy Concerns via Access Control to EHRs

Kensuke Morris[1], Goshiro Yamamoto[2], Shosuke Ohtera[2], Michi Sakai[2], Shusuke Hiragi[1,2], Kazuya Okamoto[1,2], Osamu Sugiyama[4], Naoto Kume[3], Masayuki Nambu[4], Tomohiro Kuroda[1,2] （1.Department of Social Informatics, Graduate School of Informatics, Kyoto University, 2.Division of Medical Information Technology and Administration Planning, Kyoto University Hospital, 3.Department of Electronic Health Record, Graduate School of Medicine, Kyoto University, 4.Preemptive Medicine &Lifestyle-Related Disease Research Center, Kyoto University Hospital）

Many countries including Japan are facing the challenge of obtaining meaningful use of the Electronic Health Record (EHR) systems on a national level partly due to privacy concerns of patients. These concerns are related to who is accessing the medical record, when the access taking place is, why the access taking place is, where the access occurring is and what part of the medical record is being accessed. In order to reduce these concerns, we focus on increasing control and awareness of patients. The purpose of our research is to find a suitable approach for access control that can reduce the privacy concerns of patients for both conscious and unconscious situations. We designed an approach that can provide availability of patient’ s clinical data to doctors via control of the patient. In the case where the patient is unconscious (not in a mental state to make their medical decisions), we introduced an idea that our system includes a representative who can grant access to the requesting doctor instead of the patient. In this paper, we show how the patient or their representative can control access to the patient’ s medical record. To validate the feasibility of our system design, we made a questionnaire to survey members of the Japanese society to get feedback about their privacy concerns as patients and their willingness to include their representative in controlling access to their medical record when they are unconscious. We will report the results of the survey and discuss its suitability from several aspects.

# Reducing Patient Privacy Concerns via Access Control to EHRs

Kensuke Morris[*1], Goshiro Yamamoto[*2], Shosuke Ohtera[*2], Michi Sakai[*2], Shusuke Hiragi[*1,2], Kazuya Okamoto[*1,2], Osama Sugiyama[*4], Naoto Kume[*3], Masayuki Nambu[*4], Tomohiro Kuroda[*1,2]

*1 Department of Social Informatics, Graduate School of Informatics, Kyoto University,

*2 Division of Medical Information Technology and Administration Planning, Kyoto University Hospital,

*3 Department of Electronic Health Record, Graduate School of Medicine, Kyoto University,

*4 Preemptive Medicine & Lifestyle–Related Disease Research Center, Kyoto University Hospital

Many countries including Japan are facing the challenge of obtaining meaningful use of the Electronic Health Record (EHR) systems on a national level partly due to privacy concerns of patients. These concerns are related to who, what, why and where the access is occurring. To reduce these concerns, we focus on increasing control and awareness of patients. We aim to find a suitable approach for access control that can reduce the privacy concerns of patients for both conscious and unconscious situations. We designed an approach that can provide availability of patient's clinical data to doctors via control of the patient. In the case where the patient is unconscious, we introduced an idea that our system includes a representative who can grant access to the requesting doctor instead of the patient. In this paper, we show how the patient or their representative can control access to the patient's medical record. To validate the feasibility of our system design, we obtained feedback through a survey from members (n=310) of the Japanese society about their privacy concerns as patients and their willingness to include their representative in controlling access to their medical record when they are unconscious. We report the results of the survey and discuss improvements needed based on the survey.

Keywords: Access Control, EHRs, Patient Centred Authorization, Privacy Concerns

## 1. Introduction

Privacy concerns are important issues to address when creating national and international Electronic Health Record (EHR) systems. These concerns are related to who is accessing the medical record, when the access taking place is, why the access taking place is, where the access occurring is and what part of the medical record is being accessed. These privacy concerns are related to the heart of the definition of privacy[1)] and these were present long before the implementation of electronic information systems[1) 2)]. Mistrust of third party use of confidential information exists among individuals[3)]. This mistrust is one component that needs to be removed to have an effective national EHR system.

Studies have been done to quantify privacy concerns which are subjective by nature[1) 2) 4)]. Malhotra et al. [4)] were of the view that "when applied to information privacy, social contract (SC) theory suggests that a firm's collection of personally identifiable data is perceived to be fair only when the consumer is granted control over the information and the consumer is informed about the firm's intended use of the information" (p.338). The collection factor is considered central theme of information exchange based on the SC theory. This factor was seen to be like the collection dimension of the Concern for Information Privacy (CFIP) scale[4)] and thus it remained a dimension in the IUIPC scale. The control factor represented individuals' freedom to voice their opinions and opt-out. The individual can be able to control the collected information about them. The awareness factor indicates the understanding about existing conditions and organizational practices. Within our study, we focus on concern for control and awareness of patients since their clinical data is collected and centralized in EHR systems.

## 2. Purpose

Motivation for this research originated from recognition of the need for patients to have less concern and more trust in digital health care systems. These concerns, although subjective, have a huge impact on the objective goal of healthcare technologies including EHR systems which aims to centralize and store better integrated health care information which can aid in decision making by doctors.

The system we propose entails each patient having access control that enables doctors' access to a patients' medical record when authorized by the patient or by the patient's designated representative when the patient is incapable of such authorization because mental or physical impairment that prevents direct patient authorization. Access cannot be granted without awareness of the request and activities regarding use of the patients' medical data. This design is based increasing access control and awareness for concerned patients which in turn can reduce privacy concerns that can affect the trusting beliefs of patients in EHR systems.

A key component in creating trust in accessing records is individual control over who can gain access to described personal information[4)]. The introduction of systems that include access control like 'My Health Record' and Social Health Assist Chiba (SHACHI) system are attempts to overcome patient concerns and create patient control over releasing medical information[5) 6)]. A shortcoming of these solutions is that patients with concern for control and awareness of their medical record cannot assign control to other trusted representatives who can then be able to continue access control in the event the patient becomes unconscious.

In this research, we determine the feasibility of the use of the representative by designing a system with the representative as a stakeholder. The patient-centred nature of

our research requires us to get feedback from members of the Japanese society to further justify and make changes to our system design if required. We believe that patients concerned about control and awareness of their medical information should have the option to choose a trusted representative to preserve such control and health care involvement when said patient is unable to do so due to mental and physical constraints.

## 3. Method

The inclusion of the representative gives the patient flexibility of choice; thus, a representative can be a family member or even a family doctor. A representative is the emergency contact the patient chooses to make medical decisions on their behalf in the event of an emergency[7]. We designed a system that includes the representative as an alternative person who can grant access to the requesting doctor if the patient is unable to do so. This is patient centred access control approach for patients, concerned about control and awareness of their medical data, to opt-into if desired. The studies done previously led us to consider some means by which the patient can have the flexibility to choose a trusted individual; thus, we chose the representative as the person to act on behalf of the patient when they are not in a state to do so. Therefore, the three actors determined to be involved within the scope of this research are the doctor, patient, and representative.

### 3.1 Design

#### 3.1.1 System Design

The control and awareness of the patient is the core of this research to reduce privacy concerns since these factors ensure the privacy of concerned patients[8]. Towards this goal, our approach was designed as shown in Figure 1. When applied to healthcare, our approach is based on the authorization of a doctor accessing a patient's clinical data with permission from the patient or their trusted representative. The design of our approach is supplementary to conventional EHR systems instead of replacing these systems.

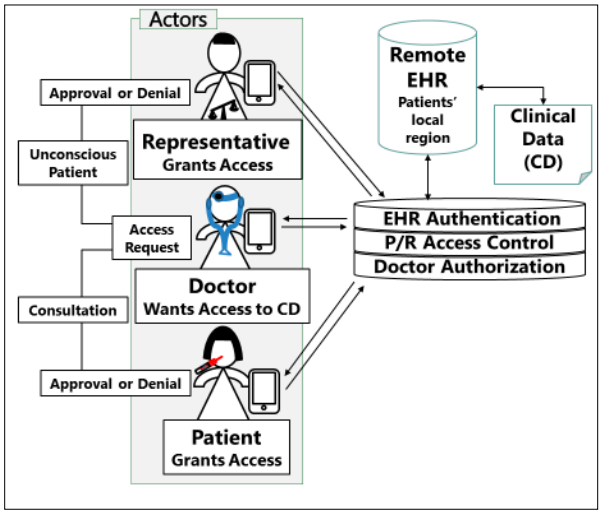


**Figure 1 – Overview of our approach which is opt-in access control for concerned patients**

Design of this system is based on whether the patient is capable or incapable of controlling access to medical record. To consider the scenarios where system design can be realized, two scenarios were identified as the main decision point from which the individual receiving the access request is decided by the doctor wanting to view the patient's record, as shown in Figure 2 and 3 respectively.

#### 3.1.2 Scenarios

Within the scope of this research, these two scenarios with appropriate alternatives were designed to test the concept of our approach with the actors involved. The actors are assumed to be registered and logged into the system before the beginning of each scenario.

**Scenario One (S1)**: The patient and doctor are the main actors with the patient initiating the process. There is no need for the representative since the patient is conscious and can make their access decisions about their medical data (Figure 2). The patient is also physically close to the doctor during the consultation. The random code (RC) can be used by patients who do not want to use their ID information. They can use this code to assist the doctor in identifying their basic information (name, age etc), as shown in figure 3.

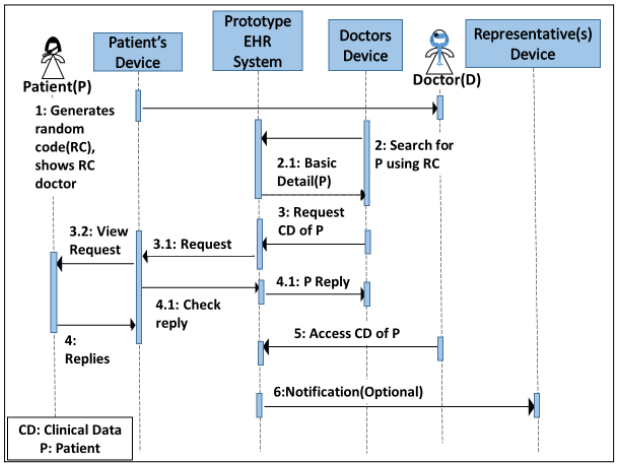


**Figure 2 - Process flow between patient and doctor in S1**

**Scenario Two (S2)**: The representative and doctor are the main actors with the doctor being the first actor to initiate the process because patient is unconscious. The representative is in a remote area (Figure 3). The number of representatives the patient can have is not defined because it is outside the scope of our approach; however, a minimum of one representative is needed for S2 to be realized.

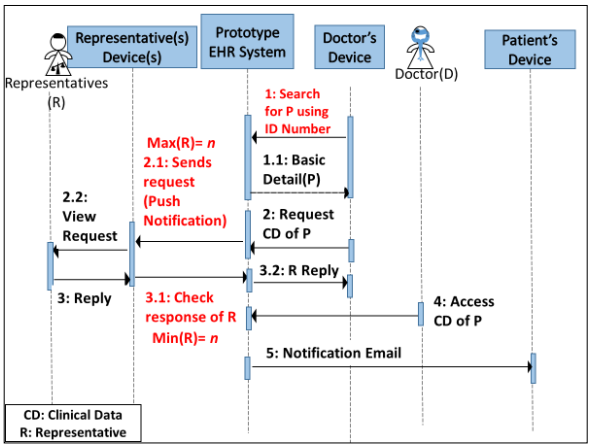


**Figure 5 - Process flow between Doctor and Representative in S2**

## 3.2 Evaluation Design

To determine the feasibility if our system design, feedback was required from a sample of the Japanese society (n=310). Since patient privacy concerns are subjective, a quantitative measurement scale was needed to evaluate patients' privacy concerns[2) 9)]. We chose the dimensions proposed by Malhotra et al. which are concerns for collection, control and awareness. The focus of our system is to provide access control and awareness to patients about their medical data, and thus we chose to focus on the factors of control and awareness in the context of our system design.

### 3.2.1 Hypotheses

Concern for control of information by patients is well established[10) 11)]. A patient who is concerned about use of their medical data will want to act, which in this case will be access control. A conscious patient can make their individual medical decisions and should have the freedom to choose options relating to their medical data if desired. This led us to the creation of the following hypothesis:

*H1-1: Patients concerned about control when they are conscious will choose access control*

Some situations arise where the patient may need medical care but may not be in a mental or physical state to decide about release their medical data. An emergency can affect patients' decision-making ability[12) 13)]. Thus, we assumed that with the assistance of a trusted patient representative, our system can provide the option to preserve access control choice of patients when they are unconscious. The need to know the impact of our system design on situations in the event the patient is unconscious but may still want access control led to the following hypothesis:

*H1-2: Patients concerned about control in the event they fall unconscious will choose access control via a trusted representative*

The need to know the impact of our system design on situations where the patient is unconscious but may still want to be aware of activities relating their medical record after when they become conscious led to the following hypotheses:

*H2-1: Patients concerned about awareness of activities regarding their medical data will choose to be informed about those activities*

*H2-2: Patients concerned about awareness of activities regarding their medical data in the event they fall unconscious will choose to be informed about those activities*

These hypotheses (H1 and H2) formed the foundation of the design and intention to evaluation our design. Since our system design was based on assumptions derived from literature, the opinion and feedback from a sample of the Japanese population were required to further customize our system design for implementation in Japan.

### 3.2.2 Survey Method

A commercial online survey organization was chosen to administer the survey. The survey period was from June 29th to June 30th, 2017. The sample consisted of four groups based on their frequency of visit to hospitals; these were frequent visitors (n=94), not so frequent visitors (n=94), seldom visitors (n=94) and people who never visit hospitals (n=19).

## 4. Results

A total of 310 respondents (age range: 19-91, mean age: 47.79, male: 50.3%, female: 49.7%) respondent to the survey. Figure 4 and 5 show the percentage of responses from patients for S1 and S2.

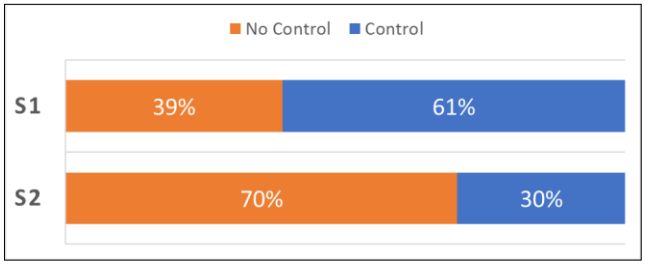


**Figure 3 - Percentage of Respondents' Preferences for Control of clinical data(S1) and representative control (S2)**

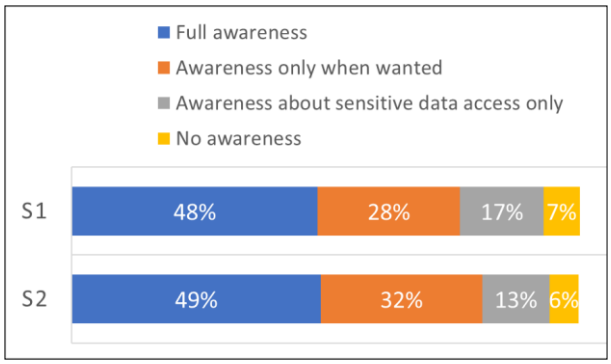


**Figure 4 - Percentage of respondents' preferences for awareness**

## 4.1 Preference for Control

Figure 4 shows less respondents who choose control of their clinical data in scenario one, chose representative control in the event they become unconscious. More respondents chose no representative control using an alternative method of access control (Figure 6).

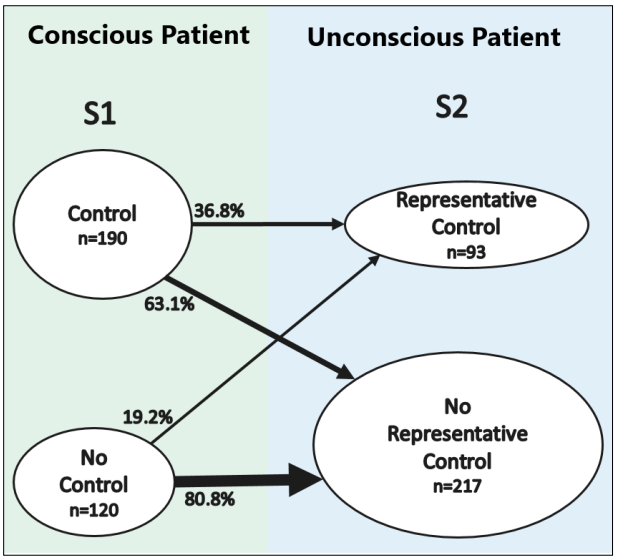


**Figure 7 - Relationship between the respondents' choice for control among scenarios; it shows the percentage of respondents who switched their preference for control in the event they become unconscious**

Respondents who chose no representative control, in the event they become unconscious, did so because of various reasons including their belief that life is more important than control over their information, their trust in the doctor, their belief that using the representative is 'troublesome'. Some respondents chose no representative control because they believe that the alternative method (emergency card), is safer, easier and reliable. These respondents need to be considered in our system design since they do not prefer a trusted representative but want to use an alternative form of control.

Some respondents who chose representative control mentioned trust in the representative as their reason. Other respondents mentioned security concerns, safety concerns and that the representative gives them a level of certainty and peace of mind. The reasons expressed by this group of respondents support the design of our access control approach.

## 4.2 Preference for Awareness

Based on Figure 5, the respondents who chose awareness of any form instead of no awareness were considered as supporters of awareness (Figure 7).

## 4.2 Overall Observations

Less respondents concerned about control when they are conscious preferred representative control in the event they fall unconscious (Figure 4). The focus of our research was the patients who choose representative control in the event they fall unconscious.

The preferences of patients for awareness suggest that patients who do not prefer representative control may prefer awareness after recovering from unconsciousness. The results lend stronger support to hypothesis H2 since a larger percentage of respondents chose awareness for both scenarios.

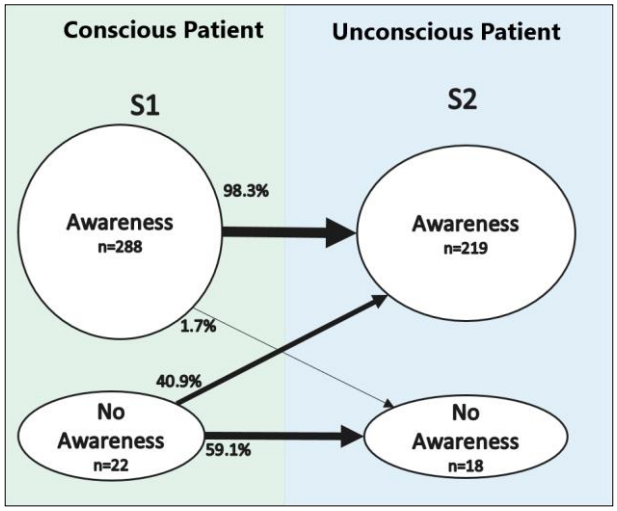


**Figure 6 - Relationship between the respondents' preference for patient awareness throughout the scenarios; it shows that the choices of most respondents are consistent throughout the survey for questions relating to patient awareness**

## 5. Discussion

### 5.1 Patient Privacy Concerns in Japan

Our survey gives new insight about the privacy concerns and perceptions of Japanese citizens. Differences found in preferences highlight the need for greater flexibility of our system design. The overall preference for the use of an emergency card for people who are not concerned about control suggests that our approach needs to be updated to facilitate the varying preferences of members of society.

Overall, the percentage of patients who prefer no representative control in the event they are unconscious supersedes the percentage of people concerned about control of their medical record if they were to become unconscious. This does not dismiss the argument that the concerned respondents make up a considerable percentage of the population of Japan. The results suggest that awareness is more useful in our system if it were to be realized in society as an opt-in access control option for concerned patients. The diversity in the choices for awareness needs to be included in our system to support the patients varying concerns for awareness.

The problem presented in the introduction cannot be addressed with a technical solution only. This is because privacy concerns have a social and legal overlap that are tied deeply into the culture of Japan.

### 5.2 Impact of Proposed System

Our proposed approach was designed with informational privacy as the dimension of focus. However, the effects of our

proposed design cannot be measured based on informational privacy alone since the other dimensions of privacy defined by (14) will be also affected through and compounded by the many stakeholders involved in the successful functioning of EHR systems.

Our system would have potential political impact. This system requires that it be overseen by a non-governmental organization with the guarantee to the public that there is no direct government interference. Possible restructuring of government components for greater public scrutiny may be a way for partial involvement of government in our implemented system. Policies to support the implementation of our approach are needed to realize our approach similar to other countries[15)16)]. Some respondents mentioned that they will prefer an emergency card if it does not have the recently implemented 'myNumber' system. This suggests that political concerns are covariates to patient privacy concerns. Twenty-one percent of respondents in the survey mentioned lack of trust as the reason for choosing control in S2. A further forty percent of the respondents choosing the representative mentioned reason that are related to trust as an outcome e.g. security concerns, safer choice, certainty, access control, and concerns for control. This supports previous claims that privacy concerns affect trusting beliefs[3) 4)].

The system we proposed may require modification in clinical practice and administrative procedures. This may in some instances change the decision time and protocol of the doctor when trying to determine the appropriate patient treatment[17)]. It also gives rise to the argument about privacy concerns versus saving a patient's life since an individual must be alive in the first place to be concerned. The design of our system also contributes to the discussion of family medicine in Japan and other countries because it involves a trusted representative who can be a family member[18)]. Family medicine is concerned with each family having a dedicated doctor. In this case, the doctor can be the representative of the patient and can grant access to other doctors using our approach in family medicine. Some hospitals adhere to informed consent where the doctor needs permission of patients to perform a treatment, but individuals may not be able to give consent because of various physical constraints that include being unconscious[17)]. For the patient's trusted representative, who already serves a role in the patients' medical care, the position is a stakeholder in the design of an opt-in access control approach can add value to the flexibility of end-user use of the EHR systems.

## 5.3 Limitations

Limitations of this research include the availability of representatives which cannot be clearly measured. In design of our approach, it is assumed that multiple representatives for one patient can increase the likeliness of the doctor obtaining a response; yet the challenge of the availability of the representatives remains present and cannot be clearly measured. The reliability of internet based frameworks cannot be controlled since there are many external influences inherent in the internet general use. This shortcoming needs to be addressed to include an alternative method of notifying representatives in the design of our approach.

The design of our patient-centred approach is focused on justifying the feasibility of our idea before defining functionality of the system. Furthermore, the registration of a representative by patients requires both parties to understand the importance of their role in our system before registration. The representative must be aware of their role before accepting it. In the future, our approach needs be updated to include three abstractions of control before implementation; these are access control policies, mechanisms to support the policies and models to theoretically define the mechanism[19)]. In our design, the control and awareness given to patients and their representative is part of the mechanism. However, this is not sufficient to provide control to concerned patients. Our research scope must be expanded to include a more precise access control approach for patients and their representatives.

To date, it is difficult within an EHR system to identify if a patient is unconscious. We included the representative in our patient-centred design to have access control in the event a concerned patient falls unconscious. Sixty-three percent of the patients concerned about control in S1 did not choose representative control in S2. These respondents need to be considered in the design of our approach. Alternative methods of access control need to be explored for the patients who may be concerned about control in the event they fall conscious but do not prefer the use of the representative. Additionally, the varying preferences for awareness for patients and their representative need to be considered since some patients did not want representative control but preferred representative awareness in the event they fall unconscious.

# 6. Conclusion

We proposed an authorization approach in health care to reduce privacy concerns and increase the Japanese' societal trust and involvement in the security. We chose use of a trusted representative of the patient in our system design to continue controlling access to the patients record. The patient concerned about control and awareness can use our system to reduce their privacy concerns about their medical data in EHR system.

Feedback received from a sample of the Japanese population suggests that within the group of patients concerned about control, some prefer alternative to using a trusted representative in the event they become unconscious. There is a need for an alternative method by a percentage of respondents since some patients choose patient control but are opposed to representative control. A small fraction of respondents was completely opposed to awareness which supports the need for the representative as one of their options in our system.

Our system design needs to be updated to include varying options of access control that patients may prefer since all patients do not prefer the use of a trusted representative. The results of this research contribute to the discussion about the balance between the patients' desires and doctors' freedom to treat the patient in a professional manner without fear or restrictions.

## References


1) Westin A. Privacy and freedom. 1967. Atheneum, New York. 1970;
2) Smith HJ, Milberg SJ, Burke SJ. Information privacy: measuring individuals' concerns about organizational practices. MIS quarterly. 1996;167–96.
3) Luo X. Trust production and privacy concerns on the Internet: A framework based on relationship marketing and social exchange theory. Industrial Marketing Management. 2002;31(2):111–8.
4) Malhotra NK, Kim SS, Agarwal J. Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. Information systems research. 2004;15(4):336–55.
5) Department of Health, Australia. My Health Record. 2017 May [cited 2017 Jun 7]; Available from: http://www.health.gov.au/ehealth
6) Doi S, Ide H, Takeuchi K, Fujita S. Development of Opt-in Agreement and Access Control System for Patients in a Personal Health Record. Transactions of Japanese Society for Medical and Biological Engineering. 2017;55(1):45–9.
7) Tiik M. Rules and access rights of the Estonian integrated e-Health system. Studies in health technology and informatics. 2009;156:245–56.
8) Foxman ER, Kilcoyne P. Information technology, marketing practice, and consumer privacy: Ethical issues. Journal of Public Policy & Marketing. 1993;106–19.
9) Stewart KA, Segars AH. An empirical examination of the concern for information privacy instrument. Information Systems Research. 2002;13(1):36–49.
10) Caine K, Hanania R. Patients want granular privacy control over health information in electronic medical records. Journal of the American Medical Informatics Association. 2012;20(1):7–15.
11) Jilka SR, Callahan R, Sevdalis N, Mayer EK, Darzi A. 'Nothing about me without me': an interpretative review of patient accessible electronic health records. Journal of medical Internet research. 2015;17(6).
12) Jones C. Glasgow coma scale. American Journal of Nursing. 1979;1551–7.
13) Wuerz RC, Travers D, Gilboy N, Eitel DR, Rosenau A, Yazhari R. Implementation and refinement of the emergency severity index. Academic Emergency Medicine. 2001;8(2):170–6.
14) Burgoon JK. Privacy and communication. Annals of the International Communication Association. 1982;6(1):206–49.
15) Centers for Disease Control and Prevention. HIPAA privacy rule and public health. Guidance from CDC and the US Department of Health and Human Services. MMWR: Morbidity and mortality weekly report. 2003;52(Suppl. 1):1–17.
16) Hudson KL, Holohan M, Collins FS. Keeping pace with the times—the Genetic Information Nondiscrimination Act of 2008. New England Journal of Medicine. 2008;358(25):2661–3.
17) O'Neill O. Some limits of informed consent. Journal of medical ethics. 2003;29(1):4–7.
18) Seifert B, Švab I, Madis T, Kersnik J, Windak A, Steflova A, et al. Perspectives of family medicine in Central and Eastern Europe. Family Practice. 2008;25(2):113–8.
19) Hu VC, Ferraiolo DF, Kuhn RD. Assessment of Access Control Systems [Internet]. 2006 [cited 2017 Aug 9]. Available from: http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf