Journal of Engineering Science and Technology
Vol. 4, No. 2 (2009) 154 - 170

A PRIVACY MANAGEMENT ARCHITECTURE FOR PATIENT-CONTROLLED PERSONAL HEALTH RECORD SYSTEM

MD. NURUL HUDA*, NOBORU SONEHARA, SHIGEKI YAMADA

National Institute of Informatics, 2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430, Japan
*Corresponding Author: huda@nii.ac.jp

Abstract

Patient-controlled personal health record systems can help make health care safer, cheaper, and more convenient by facilitating patients to 1) grant any care provider access to their complete personal health records anytime from anywhere, 2) avoid repeated tests and 3) control their privacy transparently. In this paper, we present the architecture of our Privacy-aware Patient-controlled Personal Health Record (P^3HR) system through which a patient can view her integrated health history, and share her health information transparently with others (e.g., healthcare providers). Access to the health information of a particular patient is completely controlled by that patient. We also carry out intuitive security and privacy analysis of the P^3HR system architecture considering different types of security attacks. Finally, we describe a prototype implementation of the P^3HR system that we developed reflecting the special view of Japanese society. The most important advantage of P^3HR system over other existing systems is that most likely P^3HR system provides complete privacy protection without losing data accuracy. Unlike traditional partially anonymous health records (e.g., using *k*-anonymity or *l*-diversity), the health records in P^3HR are closer to complete anonymity, and yet preserve data accuracy. Our approach makes it very unlikely that patients could be identified by an attacker from their anonymous health records in the P^3HR system.

Keywords: Health privacy, Personal health record, Healthcare service, Data sharing, Anonymization, Pseudonymization

1. Introduction

Electronic form of personal health records is both a problem and an opportunity. It opens new kind of threats to information leakage because electronic data are easy to

This project was financially supported by the Japan Society for the Promotion of Science (JSPS).

Abbreviations

NHS	National Health Service
PCHR	Patient-Controlled Health Record
PHR	Personal Health Record
P^3HR	Privacy-aware Patient-controlled Personal Health Record
PING	Personal Internetworked Notary and Guardian

copy, especially when the records are online. Thus, most Personal Health Records (PHRs) are kept local and specific to one point of care [1]. As such, most existing PHRs only provide the patient with limited insight into parts of the patient's health care information. On the other hand, electronic health records help make health care safer, cheaper, and more convenient by providing complete health history, avoiding repeated tests, and allowing appropriate authorities to have ready access to PHRs anytime anywhere. Researchers at RAND Corporation have estimated that full adoption of electronic health record systems in the USA would save $81 billion annually [2]. Emergency room physicians can avoid duplicating diagnostic tests when they can see instantly from digital records that a patient's regular doctor has already ordered the necessary tests. This one efficiency measure alone could save upwards of $60 billion each year in the USA [3].

People usually go to the healthcare centers nearby their residence for health services and their health information is kept secured in the local databases of those healthcare centers. However, patients sometimes may need to get services from different healthcare centers for various reasons, including but not limited to (i) unavailability of service on holidays, (ii) need for specialized care at specialized centers, (iii) travelling away from usual residential area, and (iv) moving residence. The stored health information in a healthcare center is usually accessible only to healthcare personnel of that center. For every healthcare center, there are separate systems to record patients' health information, and information flow between systems is limited as illustrated in Fig. 1. For example the patient in Fig. 1 has health records in three different hospitals (A, B and C). Doctors of a particular hospital cannot access the patient's health records that are stored in two other hospitals. As a consequence, patients often need to retell their medical history and redo tests whenever they encounter a new health care provider.

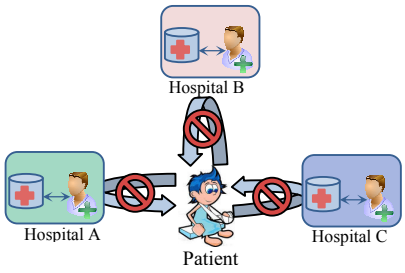

Fig. 1. Health Records Stored in Local Systems in Different Healthcare Centers are Not Easily Available to Others, When Desired.

Consider the scenario where Adrian generally gets treatment from the eye hospital A1, nearby his residence, for his eye problem. On a Tuesday morning, he

noticed his left eye was blood-red and itching. He went to the eye hospital A1 and found it closed due to one week national holiday. Thus, he visits a new eye hospital A2. The doctor at A2 wants his previous records but he can't recall them. He wishes he could have his records with him. In another scenario, Adrian has been treated for about one month for his ear problem by a doctor of hospital B1. The doctor changed his medicine several times and yet he doesn't feel better. Now, Adrian is thinking of going to a different hospital B2 but feels that he should have all his diagnostic and treatment records from B1 for the new hospital B2. However, he hesitates to ask for his records from hospital B1 because he doesn't want hospital B1 to know that he wants to go to a new hospital.

Each time a patient visits a new healthcare center, she may need to request for her old health records from several previously visited healthcare centers, which is a time consuming and tedious job. If the patients can have full control over their own health records, they can share the appropriate part of their health records with appropriate caregivers when necessary. Thus, a patient-controlled health record (PCHR) system is necessary. The goal of a PCHR [4] is to assemble the patient's complete health history and let the patient control whom to give access to this information and when.

Our devised Privacy-aware Patient-controlled Personal Health Record (P^3HR) system allows a patient to view her integrated health history, and share her health information transparently with any healthcare providers. The patient controls who would be allowed to access which part of her health records and for what duration. In P^3HR database, no quasi-identifiers are stored and it uses patient created secret pseudonym for linking records with their respective patients. The resulting database becomes most likely completely anonymous. Unlike *k*-anonymity [5] or *l*-diversity [6] method, attribute values of a record are not generalized or modified and hence the accuracy of the stored data is preserved. The relationship between a patient and her pseudonym is known only to the patient. A patient lets healthcare professionals access her anonymous health records without revealing her secret pseudonym. Even if the records are exposed to unauthorized parties it is very unlikely that they would be able to identify the respective patients from their health records i.e., patients' privacy is preserved.

The rest of the paper is organized as follows; in section 2 we briefly present related previous works by others. Section 3 presents the framework and system security architecture in details. Section 4 illustrates basic operational steps for using the P^3HR system. Section 5 describes security and privacy analysis of P^3HR system considering different types of attacks. Section 6 briefly describes a prototype implementation of P^3HR system. Finally, section 7 concludes the paper with discussions on various related issues.

2. Related Works

Electronic health records are widely used in developed countries. However, most of them are stand alone and gives patients limited or no control over their health records. According to the scope of this paper, we discuss only the systems that allow patient to control their own health records and use some privacy protection technologies.

General anonymization methods such as *k*-anonymity [5] provides a degree of privacy protection in a way that a person in the record cannot be distinguished from at least *k*-1 individuals whose information also appears in the record set. The strength of this method depends on the value of *k*. However, the higher the values of *k* the more the data lose accuracy. The *l*-diversity [6] method of anonymization is an improvement over the *k*-anonymity method for special type of attacks which may identify a person if only *k*-diversity method is used. The strength of this method also depends on the value of *l* (and *k*) and data accuracy is not preserved.

The National Health Service (NHS) of UK [7] is evolving towards a comprehensive electronic record that provides secure and accessible health information to professionals and patients across the nation. Health smart cards have been implemented in many European countries and they store health information in the card themselves. iHealthRecord [8] was designed to facilitate online access to information and care for more than 90,000 physicians, their practices and their patients. Patients retained control and responsibility to initiate their own iHealthRecord. It improved access to records and sharing them with others in a more convenient way. The Indivo [9], formerly Personal Internetworked Notary and Guardian (PING), is the world's first patient-controlled web-based record system, enabling a patient to own a complete, secure copy of her medical record, integrating health information across multiple care centers. Reference [10] presents a set of usage scenarios to explore the concept of a PCHR and outline an initial access control model for a PCHR.

Google and Microsoft launched Google Health [11] and HealthVault [12] respectively. They allow individuals to store and manage all of their health information in one central place. One can import her health records from her doctors, hospitals, labs, prescription drug plans, and other healthcare providers. She can also input them by herself or upload data from personal health monitoring devices such as glucose or blood-pressure monitors.

Most of the above health record management services incorporate health-specific search engines and have health information services. Those implementations provide mechanisms for making a patient's health record available from one hospital to another. They vary in the type of utilities/services that they offer and the extent the patients get control over their health records. Most of them don't give full control to the patient. The smart health card systems that are implemented in many European countries are not strongly privacy preserving because any healthcare professional can read most of the health information from patient cards without the patients' consent. The main limitation of all of the existing works is that they are not strongly privacy preserving. A patient can easily be de-identified from the attribute that links the records with specific individuals. Thus, an intruder, who gets access to the health database, can associate the records with an individual, resulting in poor privacy control.

3. P^{3}HR System

The devised Privacy-aware Patient-controlled Personal Health Record (P^{3}HR) system is not meant to be an alternative to healthcare centers' usual local health records system. Instead, it is intended to provide a convenient, easy, secure and

privacy-preserving way of making patient's personal health history available to any healthcare center at any time according to the patient's desire.

Disclosure of some personal information to unauthorized parties doesn't necessarily mean privacy loss. If the unauthorized party cannot link or associate the disclosed information to the specific individual (to whom the private information belongs to) we do not say it is privacy loss [13]. Based on this principle, P^{3}HR database is made anonymous by removing all quasi-identifier information. None, except the data subject (patient), can link a particular record of P^{3}HR database to the respective patient because the patient's unique ID (digital pseudonym [14]) in a record that links the record with the specific patient and is known to the respective patient only.

Figure 2 illustrates the simplified framework for P^{3}HR system. A patient can personalize/customize her privacy control policy through the web based service from her home. The P^{3}HR site hosts anonymous personal health records, provides mechanisms for personalizing privacy control policies and provides access control module for doctors and patients. A hospital is equipped with IC card readers for authentication and browsers for browsing patients' health records.

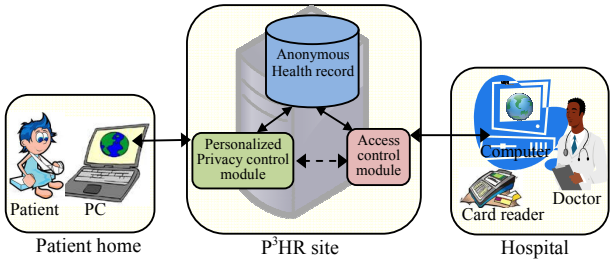

Fig. 2. The Framework for Privacy-aware Patient-Controlled Personal Health Record (P^{3}HR) System.

The P^{3}HR security system architecture consists of an anonymization module, an anonymous health record database, the patient's profile, access control modules for patients, access control modules for third parties, and a privacy control module as shown in Fig. 3. The functionality and operation of each module of the architecture have been described in the following subsections.

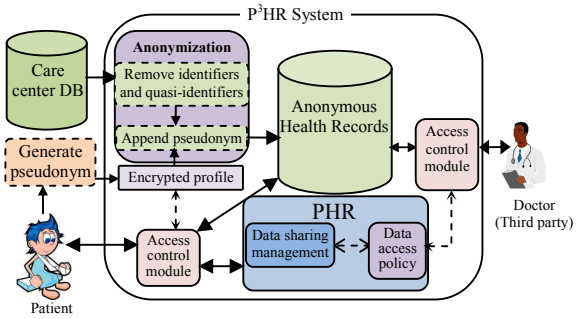

Fig. 3. Architecture of Privacy-Aware Patient-Controlled Personal Health Record (P^{3}HR) System.

3.1. Anonymization module

To preserve patient's privacy from intruders, P^{3}HR system stores patient's health records in an anonymous form. Before storing health records from a care center database (or from patient's direct input) into the P^{3}HR database, the anonymization module removes all identifiers and quasi-identifiers [15] from the records so that a particular record cannot be associated with a specific identifiable individual. Thus, even if an intruder gets access to the P^{3}HR anonymous health database, he cannot determine which record or set of records belongs to a particular patient.

To allow an authorized party (e.g., doctor) to access a set of records of a particular patient legitimately, the system needs to associate each record to the respective patient. To achieve these two conflicting goals of anonymization and keep each record associated with the respective patient, the patient creates her unique ID (known as digital pseudonym) using Unique User-generated Digital Pseudonyms mechanism [16]. A patient can generate her pseudonym locally in her personal security environment, e.g. in her smart card or her personal digital assistant. There is no need for any information interchange between the patient and P^{3}HR system, except P^{3}HR supplies a unique identifier for each request (e.g., auto increment number). The digital ID is long enough and randomized so that one cannot guess it from the patient's background or personal information (e.g. name) obtained through other channels/sources. The patient also doesn't need to remember her digital ID.

A patient's digital ID (pseudonym) is appended to all of her records during the record adding process. Thus, a record in the anonymous P^{3}HR database contains the respective patient's pseudonym along with her health information. No one can reveal the association of a pseudonym with its holder, unless the holder explicitly discloses it. Figure 4 shows the process of making an anonymous personal health record.

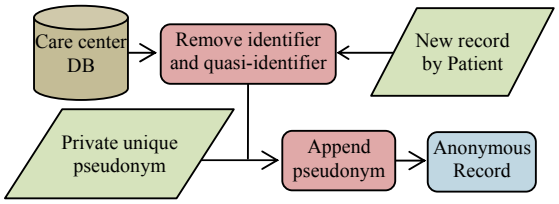

Fig. 4. After Identifiable Information is Removed, a Patient Appends Her Private Pseudonym with her Records.

A patient stores her pseudonym into her encrypted profile. The system accepts a new pseudonym that is not already in use by others. The patient needs to decrypt her pseudonym when she wants to add (or accept from an external source) a new health record. The system takes the decrypted pseudonym and appends with her new records. A pseudonym is created for the system use only and is visible to its holder only.

3.2. Patient's profile

Security and privacy researchers have identified many items, which are used in different healthcare centers, as personally identifiable information (e.g., telephone numbers, fax numbers, e-mail addresses, social security numbers, health plan beneficiary numbers, vehicle identifiers and serial numbers etc. [17]). Most of the personally identifiable information does not change frequently with time and they can make up a patient's profile.

Patients sometime require personally identifiable information to be provided to the new healthcare centers that they visit for the first time. For providing general personal information conveniently to newly visited centers, P^{3}HR system allows a patient to store her profile, consisting of general identifiable information, encrypted with a shared key. General identifiable information includes the information that is usually stored in a paper based health card, such as name, address, date of birth, phone number, and blood group. A patient can provide her shared key to the caregiver where she visits a care center for the first time. The care centers store needed general personal information into their secure local system. Some additional private information (e.g., patient's pseudonym), which is used for database anonymization, is also kept encrypted with the patient's public key. The extended profile is not shared with others. Figure 5 depicts the technological aspect of a patient's encrypted profile.

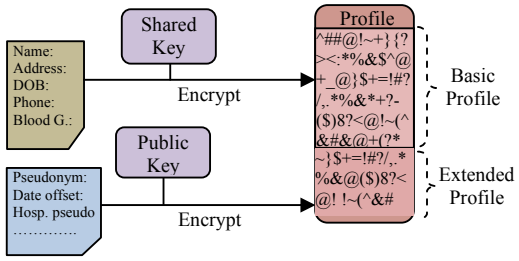

Fig. 5. Personally Identifiable Information is Kept Encrypted into Profile.

3.3. Access control module

There are separate access control modules for patients and healthcare professionals. Each patient and health care professional who wants to use the system needs to register into the system. The access control module for patients controls access to a patient's personal health records, personal privacy policy management data, and personal data sharing list. After the system verifies the authentication of a patient, a patient can retrieve her pseudonym with her private key to access her health records. A patient can view only the records containing her pseudonym. In the registration process of healthcare professionals, their true identity is verified by external means. A healthcare professional has very limited rights. He can only have access to the records of a patient which are allowed by patient's personal policy and her list of shared records.

Strong authentication

Smart cards can provide strong authentication. They are engineered to be tamper resistant. The embedded chip of a smart card usually implements some cryptographic algorithm. Each patient is issued a personalized smart IC card which stores patients profile information (such as name, address, date of birth, telephone number, health insurance number, blood group etc) in encrypted form. Also, healthcare providers are issued Healthcare Professional Cards. Card readers (installed at healthcare centers) can decrypt and read the information from a card. Smart card readers are used as a communications medium between the smart card and a host. Data stored on the cards cannot be read without going through a strict authorization and mutual authentication process. The security access module of the card reader verifies the identity of healthcare providers to read the content of patient's IC card. The healthcare professional can't read beyond the basic medical information without cardholder's input of the PIN number.

Patients usually want to access their health records from home. On the other hand, doctors usually want to access a patient's health records from their working place when the patient visits the doctor. It is feasible to install card readers at healthcare centers, but not at every patient's home. Thus, patients need a web-based authentication mechanism. For strong authentication of patients, P^3HR system requires a patient to know her private key. Since, only the respective patient (who has the knowledge of her private key) can decrypt her secret pseudonym, identity theft is effectively protected. A patient interface retrieves health records based on her private pseudonym which is stored encrypted into her profile.

Accessing PHR by a doctor requires correct identification of the doctor as well as the patient. This is done at the doctor's workplace by using both the patient's smart IC card and the doctor's smart IC card through a card reader. Figure 6 sketches strong authentication mechanisms of P^3HR system. The patient's smart card supplies patient's pseudonym to identify and supply only the respective patient's health records. However, this pseudonym is not disclosed to healthcare professionals.

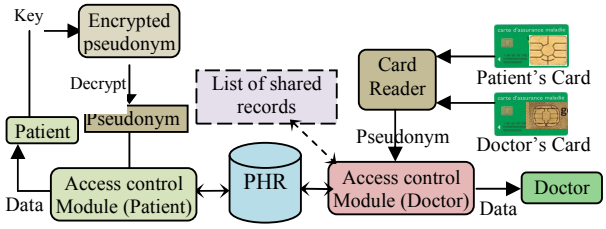

Fig. 6. Strong Authentication Mechanism Protects PHR from Unauthorized Access.

3.4. Privacy control module

Each patient is allowed to create/update the policies for accessing her health records by third parties (e.g., the healthcare professionals who are not the creators of the records). In her profile, a patient sets general access rules for healthcare professionals for accessing her health records. For example, a profile may specify

that a doctor can view only the records of the respective patient that are created by the doctor himself. Another profile may set that a doctor can view only the records of the respective patients that are created by any doctor in the same department (or hospital) where the accessing doctor belongs to. Allowing an individual patient to create her own privacy policies gives flexibility and freedom controlling her privacy independent of others.

Apart from the general access policies, a patient can select individual records or group of records based on the type of associated disease (skin disease, eye disease, coronary disease etc.) and create/update/delete lists of health records for sharing with others. Data sharing management allows a patient to select health care professionals (based on individual or role) for granting access to her selected health records. The patient can also specify specific time duration for which the shared data would be accessible to the selected healthcare professional. Finally, the patient can have a doctor's view over her records through her data sharing management console and check which of her records is going to be accessible to the doctor. The doctor's view provides complete transparency on her privacy control. Figure 7 illustrates data sharing through the privacy control module.

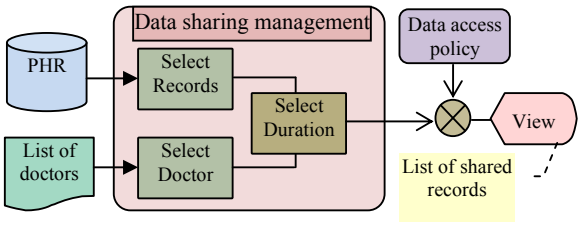

Fig. 7. Illustration of Data Sharing through Privacy Control Module.

4. Operations

We briefly describe three important operations in P^{3}HR system: (i) adding new personal health records into the database, (ii) sharing the basic profile with a new healthcare center, and (iii) accessing shared records by a third-party healthcare professional.

4.1. Adding new records

New health records may be inputted by the patient herself or can be sent from external sources like any care center where the patient had been treated. When new data comes from external sources, all identifiable information is removed and the patient is notified about the arrival of new data. She checks the validity of the data, verifies the data source, and accepts (or declines) them as her personal health record. As said before, a patient's pseudonym is kept into her profile encrypted with the patient's key. The system asks for the decryption key to extract the patient's pseudonym, appends the pseudonym with her new records, and stores the anonymous record into the P^{3}HR database. Figure 8 shows the flowchart of adding new records into the P^{3}HR database.

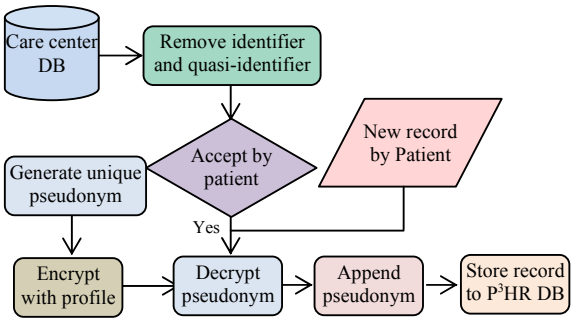

Fig. 8. Flowchart for Adding New Health Records in the P^{3}HR Database.

4.2. Sharing basic profile

A patient may need to provide her basic profile info when she visits a hospital for the first time. The patient may use a shared key if the hospital (third-party) doesn't have a card reader installed. Figure 9 illustrates a sequence diagram for this scenario. However, in this case the healthcare professional at the hospital needs to know some kind of patient ID by which he can search in the system. Since a patient pseudonym is private and secret, the health professional cannot use it. So, we create the patient ID with a one-way hash function over some personal information of the patient. This ID must be linkable with her encrypted profile and is used to search the encrypted profile (which will be decrypted with the shared key). Even though this ID might be known by unauthorized parties, they cannot decrypt the patient profile without her shared key.

An obviously better or safer way of sharing basic profiles is through the patients' smart IC cards which needs card readers to be installed at the hospital. The sequence diagram in Fig. 10 includes this case. The card reader reads the basic profile information and shows it to the party who has been authorized with her own smart IC card.

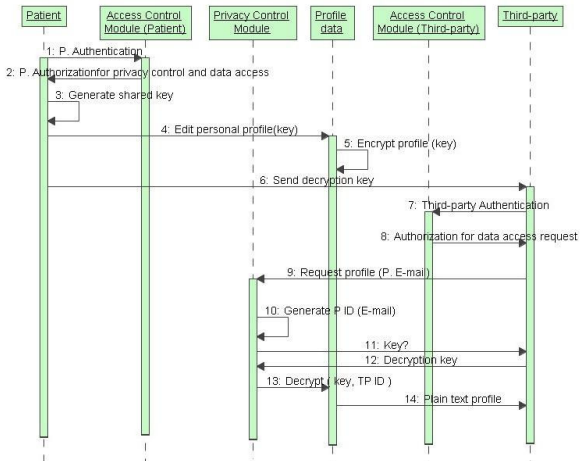

Fig. 9. Sharing Basic Profile with a Newly Visiting Hospital (Third-Party) That Doesn't Have Card Reader Installed.

4.3. Accessing shared records by third-party

In order to access some health records of a specific patient, the accessing party must identify the records that are associated with a specific patient. In the P^{3}HR system, health records are linked with their subject by a private pseudonym which is kept encrypted into the smart IC card of the patient. A patient should keep her pseudonym secret even from the healthcare professionals. The card reader reads the pseudonym and sends it to the server without disclosing it to the healthcare professional. Figure 10 shows a sequence diagram for accessing a patient's health record by a doctor when the patient (with her smart card) visits the hospital that has a card reader.

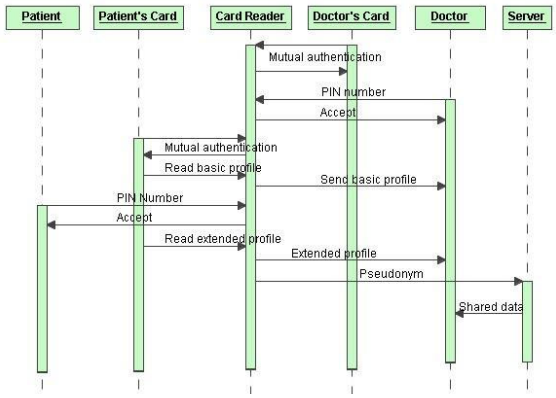

Fig. 10. Process of Accessing Shared Personal Health Records By a Doctor when a Patient Visits a Hospital with her Smart Card.

5. Security and Privacy Analysis

We assume that each module of the P^{3}HR system works properly and the described policies are enforced by the trusted service provider. Here we carry out an intuitive privacy analysis of the P^{3}HR system.

Attacker model

Internal treats from the service provider cannot be eliminated/removed completely in reality. So, our attacker model takes partial untrustworthy service providers into account in which individual employers may try to breach patient privacy. We omit discussing eavesdroppers of the user's network as attackers, since secure communication between hosts can be achieved. We assume that an attacker cannot break cryptographic primitives and does not control the communication network.

Identity theft: The access control module allows a patient to view only the records that have the same pseudonym as her own. A patient's pseudonym is not editable and a patient cannot modify it once it is stored. Thus, a patient is forced to see her own records only. Besides, a patient needs to decrypt her pseudonym to view her health records. Even if the identity of a patient is stolen and used by

another malicious patient, he cannot decrypt the pseudonym without knowing the key i.e., cannot view the respective patient's records.

Malicious database administrator or intruder: The database administrator (or an intruder) may get full access on the stored health records. However, since the relationship between the pseudonym in a record and the respective patient is secret and known to the respective patient only, the database administrator cannot find out who is the holder of the pseudonym. Thus, the records are most likely to be completely anonymous to him. This is true for any attacker.

If the database administrator takes two snapshots of the database at two instances and a single logged in patient adds new records in between the snapshots, then the database administrator can find out the relationship of the logged in patients username and her pseudonym. However, this requires the administrator to find out who was logged in and a single patient needs to be logged in, which is very unlikely. Even though the administrator can find out the username of the pseudonym holder, no other personal information is revealed to him. The victim patient still remains anonymous to the administrator unless the administrator has prior knowledge who is the holder of the username.

Malicious collaborative patients and database administrator: When all of the patients (except one) and the database administrator are malicious, they can collaboratively find out the pseudonym of the non malicious patient. In this case, the malicious team should have the prior knowledge that the subject patient is a registered member in the system and all of them need to be collaborative. However, the case where all of the registered members would be malicious is very unlikely.

Malicious healthcare professional: A healthcare professional can access the selected records of a patient that the patient grants him access to. The pseudonym of the patient is read through the smart IC card reader and is not visible to the healthcare professionals. A malicious healthcare professional may try to access the records for which he is not authorized. Even though he came to know the basic personal information of the patient from her smart card, he cannot know the pseudonym of the patient. However, if he gets complete access to the database (say, with collaboration of the database administrator) he can search for the treatment information of the known patient and then find the patient's pseudonym.

From different attack models, we can see that collaborative attack by malicious healthcare professional and malicious database administrator may result in privacy breach in P^3HR system. All other types of attacks are not effective. However, healthcare professionals are generally trusted and not intuitively malicious. Besides, such unauthorized access can be detected by maintaining a proper/effective access log. So, we can conclude that the privacy protection capability of P^3RH system is very strong.

6. Prototype Implementation

We have developed a prototype of our P^3HR system. The prototype implementation has not included authentication by using smart IC cards and uses only username/password based authentication as shown in Fig. 11. However, in practical deployment, smart IC card based authentication must be included.

During its development, we consulted with the healthcare professionals of Kochi University Hospital in Kochi prefecture, Japan, which has electronic health records of its patients for over 25 years.

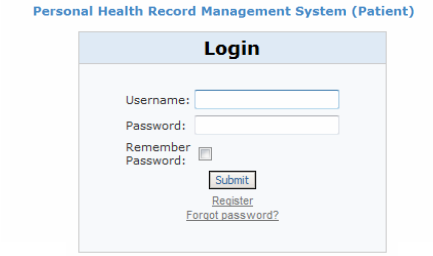

Fig. 11. Patient Authentication Screen of P[3]HR System.

The main menu of patient (Fig. 12) provides links to the general information of different hospitals in Japan and to the healthcare professionals (doctors) of those hospitals. It gives notification of new health records available from external sources where the current logged-in patient was treated recently.

Fig. 12. Main Menu (Patient).

The patient can view her encrypted profile (Fig. 13) and can edit parts of the profile that are not static (like address). It also has the patient's private pseudonym accessible through the patient's private key.

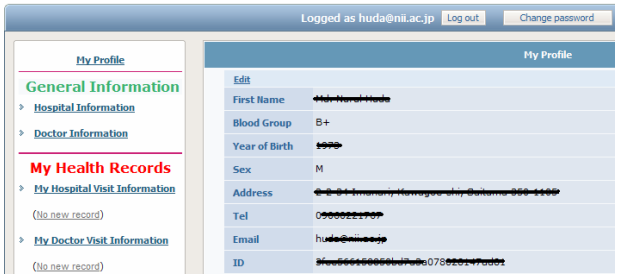

Fig. 13. Decrypted Profile of the Patient.

Figure 14 shows part of data access policy that the patient sets for doctors. It specifies which records, from her record-set, a doctor can view.

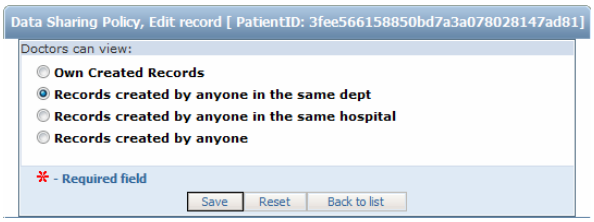

Fig. 14. Part of Data Access Policy where the Patient Sets What of her Record Set a Doctor Can View.

Figure 15 shows a simple data sharing management page where the patient has selected a doctor, selected a group of records based on the type of disease and the duration for which this share will be effective.

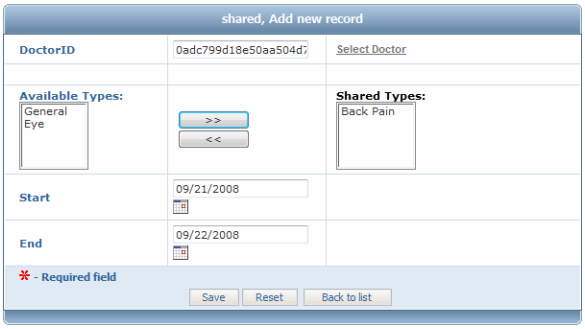

Fig. 15. Adding New Share.

Figure 16 shows the list of shares of the current patient. The patient can transparently view which records are shared to whom for what duration.

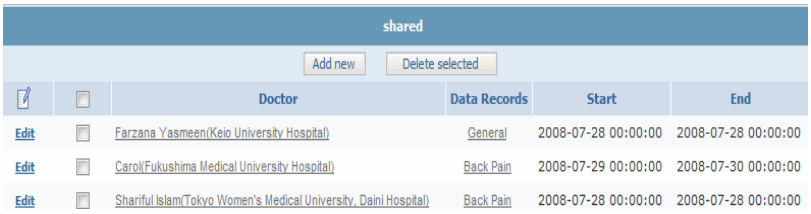

Fig. 16. List of Shared Records.

Figure 17 illustrates the doctor's screen in which the doctor is trying to access a patient's profile. The system asks for the shared key to decrypt the basic profile. Figure 18 shows the patients health records that are shared with the current logged in doctor.

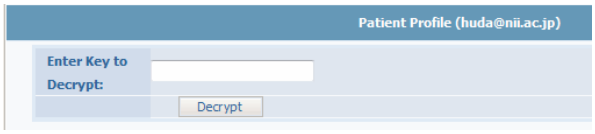

Fig. 17. Doctor Trying to Access Patient's Basic Profile.

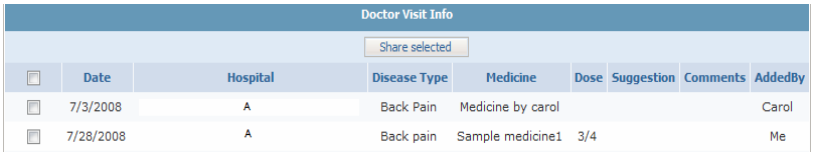

Fig. 18. Patient's Treatment Info Shared with the Logged in Doctor.

In our implementation, a patient can replace the hospital name, that she visited, with a pseudonym and can maintain the list of hospital pseudonyms encrypted into her extended profile. This is done because we think that the actual hospital name info is not important to third-party doctors, but may be important to the patient himself. Also, the actual date value, on which the patient visited a hospital, is not stored in the database. The patient selects an offset value, stores dates that are away by the offset from the original date and encrypts the offset value into her encrypted profile. During display, to an authorized party, actual date value is displayed by adjusting the offset value. This is done to keep the accuracy of the displayed data but to anonymize date values to intruders.

Healthcare professionals of Kochi University hospital suggested that sometimes it is necessary to know all of a patient's health history. But a patient may not share all of her records. How to solve this problem? To make a balance between the freedoms of the patient and the necessity of information by the doctor, our system shows the doctor what percentage of health records of the patient is being shared with this doctor. Thus, a doctor knows if there are any other records that are not shared with him and the patient fully preserves the right to control over her records.

They also pointed out that many Japanese people don't want to know actual disease name when it is a serious disease (e.g. cancer). This is because perhaps, patients may get emotionally weak when they come to know about their serious disease. In response to this, we keep two columns for disease name, one describing disclosed disease name and the other one actual disease name. Disclosed disease name is visible to the patients and disclosed disease name as well as actual disease name is visible to the doctors.

7. Discussion

We have devised novel privacy management architecture, called P^3HR, for a patient-controlled personal health record system. It uses strong authentication mechanisms using smart IC cards. The IC card stores personal information in an encrypted form. If the card is lost, it must be reported to the system administrator. The lost card should immediately be blocked by the authentication module and

the respective patient should be issued a new card. Also, a patient should be able to use multiple pseudonyms and all of them need to be included into her encrypted profile so that all of her records remain associated with the patient.

In P^3HR system, the stored data is made anonymous so that an intruder cannot associate a record with a specific individual. We use patient created secret pseudonym that is known by the patient only to associate records with the respective patient. However, the relation between a physical patient and her pseudonym remains secret and does not need to be disclosed to anybody in order to use the system. The advantage of our system is that our stored database becomes most likely completely anonymous and it is highly unlikely that the data subject could be identified from the stored records. Thus, our system allows patients to have control over their health records which in turn helps makes health care safer, cheaper, and more convenient. Most of all, it supports the necessary functionalities for current healthcare industry with a complete privacy protection mechanism for patients. We have intuitively analyzed the privacy aspect of our system and have shown that it can tolerate almost all common attacks. We have developed a prototype system to illustrate the architecture and its functionalities.

References

1. Kim M. I. and Johnson K. B. (2002). Personal health records: evaluation of functionality and utility. *Journal of the American Medical Informatics Association*, Vol. 9(2), 171–180.
2. Hillestad R., Bigelow J., Bower A., Girosi F., Meili R., Scoville R., and Taylor R., (2005). Can electronic medical record systems transform health care? Potential health benefits, savings, and costs, Health Affairs, Vol.24(5), 1103-1117.
3. Willey V.J. and Daniel G.W. (2006). Healthcare: an economic evaluation of use of a payer-based electronic health record within an emergency department, http://event.on24.com/event/35/62/1/rt/1/images/player_docanchr_5/study.pdf.
4. Mandl, K.D., Szolovits P., and Kohane I. S. (2001). Public standards and patients' control: how to keep electronic medical records accessible but private commentary: Open approaches to electronic patient records commentary: A patient's viewpoint. *BMJ*, Vol. 322(7281), 283–287.
5. Sweeney L. (2002). *k*-anonymity: a model for protecting privacy. *International Journal of Uncertainty, Fuzziness and Knowledge-Based Systems*, Vol. 10(5), 557 – 570.
6. Machanavajjhala A., Kifer D., Gehrke J., and Venkitasubramaniam M. (2007). *L*-diversity: Privacy beyond k-anonymity, *ACM Transactions on Knowledge Discovery from Data (TKDD)*, Vol. 1(1), Article No.3.
7. National health Service, NHS Choices homepage, last accessed on October 25, 2008 from (http://www.nhs.uk/Pages/homepage.aspx).
8. iHealth Alliance, Interactive Personal health records, last accessed on October 25, 2008 from (http://www.ihealthrecord.org/).
9. Indivohealth, personally controlled health records, last accessed on October 25, 2008 from (http://www.indivohealth.org/).

10. Røstad L. (2008). An initial model and a discussion of access control in patient controlled health records. *The Third International Conference on Availability, Reliability and Security*, 935 – 942.
11. Google, Google health, last accessed on October 25, 2008 from (https://www.google.com/health).
12. Microsoft Corporation, HealthVault, last accessed on October 25, 2008 from (http://www.healthvault.com/).
13. Huda M.N.; Kamioka E.; and Yamada S. (2007). An efficient and privacy-aware meeting scheduling scheme using common computational space. *IEICE - Transactions on Information and Systems*, Vol. E90-D(3), 656-667.
14. Chaum D.L. (1981). Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM*, Vol. 24(2), 84 – 90.
15. Ferrari E.; and Thuraisingham B. (2005). Analysis of information security objects under attacks and processed by methods of compression, IRM Press.
16. Schartner P; and Schaffer M. (2005). Unique user-generated digital pseudonyms. *Springer LNC* ,Vol. 3685, 194-205.
17. Brook J.M.C. (2008). Pseudonymization methodologies: personal liberty vs. the greater good. *The Last HOPE Conference*, New York.