A Privacy Management Architecture for Patient-Controlled Personal Health Record System

Md. Nurul Huda, Noboru Sonehara, and Shigeki Yamada
National Institute of Informatics
2-1-2 Hitotsubashi, Chiyoda-ku, Tokyo 101-8430
Email: {huda, sonehara, shigeki}@nii.ac.jp

Abstract- Patient-controlled personal health record system can help making health care safer, cheaper, and more convenient by facilitating patients to 1) grant any care provider to access 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 devised Privacy-aware Patient-controlled Personal Health Record (P3HR) 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 P3HR system architecture considering different types of security attacks. Finally, we describe a prototype implementation of P3HR system that we developed reflecting the special view of Japanese society. The most important advantage of P3HR system over other existing systems is that most likely P3HR system provides complete privacy protection without losing data accuracy. Unlike traditional partially anonymized health records (e.g., using k-anonymity or l-diversity), the health records in P3HR are closer to completely anonymity, yet preserve data accuracy. Our approach makes it very unlikely patients could be identified by an attacker from their anonymous health records in P3HR system.

I. 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 is easy to copy and leak, 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 his 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 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 [3] in the USA.

People usually go to the healthcare centers nearby their residence for health services and their health information is kept secured in local databases of those healthcare centers. However, patients sometimes may need to get services from different healthcare centers for various reasons such as unavailability of service on holidays, need for specialized care at specialized center, travelling away from residential area, and moving residence. The stored health information in a healthcare center is usually accessible only to the healthcare personnel of that center. For every healthcare center there are separate systems to record patient health information, and information flow between systems is very limited (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.

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 eye blood-red and etching. 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 to appropriate caregiver 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 anonymized. 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 let healthcare professionals to access her anonymized health records without revealing her secret pseudonym. Even if the records are exposed to unauthorized parties it is very unlikely that they would 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 II we briefly present related previous works by others. Section III presents the framework and system security architecture in details. Section IV illustrates basic operational steps for using P^3HR system. Section V describes security and privacy analysis of P^3HR system considering different types of attacks. Section VI briefly describes a prototype implementation of P^3HR system. Finally, section VII concludes the paper with discussions on various related issues.

II. RELATED WORK

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 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 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 not preserved.

National Health Service (NHS) of UK [7] is evolving toward a comprehensive electronic record that provides secure and accessible health information to professionals and patients across the nation.

iHealthRecord [8], was designed to facilitate online access to information and care for more than 90,000 physicians, their practices and their patients. More than 10,000 Americans built an iHealthRecord during the first few weeks of its initial availability. Patients retain control and responsibility to initiate their own iHealthRecord. It improved access to records and share 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.

Google and Microsoft launched Google Health [10] and HealthVault [11] respectively. They allow individual to store and manage all of his/her health information in one central place. One can import his health records from his doctors, hospitals, labs, prescription drug plans, and other healthcare providers. He can also input them by himself or upload data from personal health monitoring devices such as glucose or blood-pressure monitors.

Reference [12] presents a set of usage scenarios to explore the concept of a PCHR and outline an initial access control model for a PCHR.

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 a 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 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 individual, resulting in poor privacy control.

III. P^3HR SYSTEM

The devised Privacy-aware Patient-controlled Personal Health Record (P^3HR) 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 with the specific individual (to whom the private information belongs to) we do not say it is privacy loss [13]. Based on this principle, P¹HR database is made anonymous by removing all quasi-identifier information. None, except the data subject (patient), can link a particular record of P¹HR 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 is known to the respective patient only.

Fig. 2 illustrates the simplified framework for P¹HR system. A patient can personalize/customize her privacy control policy through the web based service from her home. The P¹HR site hosts anonymized personal health records, provides mechanism for personalizing privacy control policy and access control module for doctors and patients. A hospital is equipped with IC card reader for authentication and browser for browsing patients’ health records.

The P¹HR security system architecture consists of anonymization module, anonymous health record database, patient’s profile, access control module for patients, access control module for third party, and privacy control module (Fig. 3). The functionality and operation of each module of the architecture has been described in the following subsections.

A. Anonymization Module
To preserve patient’s privacy from intruders, P¹HR system stores patient’s health records in an anonymized form. Before storing health records from a care center database (or from patient’s direct input) into the P¹HR 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 P¹HR 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) access to 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 keeping each record associated with the respective patient, the patient creates his unique ID (known as digital pseudonym) using Unique User-generated Digital Pseudonyms mechanism [16]. A patient can generate his pseudonym locally in his personal security environment, e.g. in his smart card or his personal digital assistant. There is no need for any information interchange between the patient and P¹HR system, except P¹HR 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 patient’s background or personal information (e.g. name) obtained through other channel/source. The patient also doesn’t need to remember his digital ID.

A patient’s digital ID (pseudonym) is appended to all of his records during the record adding process. Thus, a record in the anonymous P¹HR database contains the respective patient’s pseudonym along with his health information. None can reveal the association of a pseudonym with its holder, unless the holder explicitly discloses it. Fig. 4 shows the process of making anonymized personal health record.

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

Security and privacy researcher 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 sometimes require personally identifiable information to be provided to the new healthcare centers that visit for the first time. For providing general personal information conveniently to the newly visiting centers, P3HR system allows a patient to store his 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 name, address, date of birth, phone number, and blood group. A patient can provide her shared key to the caregiver where he 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 (extended profile), which is used for database anonymization (e.g., patient’s pseudonym), is also kept encrypted with the patient’s public key. The extended profile is not shared with others. Fig. 5 depicts the technological aspect of a patient’s encrypted profile.

![Figure 5. Personally identifiable information is kept encrypted into profile.](image)

C. 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 need to register in 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 his pseudonym with his private key to access his health records. A patient can view only the records containing his 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 access only the records of a patient which the patient’s personal policy and his list of shared records allow him.

**Strong Authentication**

Smart card 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 provider 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 web based authentication mechanism. For strong authentication of patients, P3HR system requires patient to know his private key. Since, only the respective patient (who has the knowledge of his private key) can decrypt his secret pseudonym, identity theft is effectively protected. A patient interface retrieves health records based on his private pseudonym which is stored encrypted into his profile.

![Figure 6. Strong authentication mechanism protects PHR from unauthorized access.](image)

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. Fig. 6 sketches strong authentication mechanisms of P3HR 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.
D. Privacy Control Module

Each patient is allowed to create/update the policies for accessing his health records by third parties (e.g., the healthcare professionals who are not the creators of the records). In his profile, a patient sets general access rules for healthcare professional for accessing his 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 patient that are created by any doctor in the same department (or hospital) where the accessing doctor belongs to. Allowing individual patient to create his own privacy policies gives flexibility and freedom to a patient in controlling his 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, heart 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 his 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 his records through his data sharing management console and check which of his records is going to be accessible to the doctor. The doctor’s view provides complete transparency on his privacy control. Fig. 7 illustrates data sharing through the privacy control module.

Figure 7. Illustration of data sharing through privacy control module.

IV. OPERATIONS

We briefly describe three important operations in P3HR system: adding new personal health record into the database, sharing basic profile with a new healthcare center, and accessing shared records by a third-party healthcare professional.

E. Adding New Records

New health record may be inputted by the patient himself 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. He checks the validity of the data, verifies the data source, and accepts them as his personal health record. As said before, a patient’s pseudonym is kept into his profile encrypted with the patient’s key. The system asks for the decryption key to extract the patient’s pseudonym, appends the pseudonym with his new records, and stores the anonymous record to the P3HR database. Fig. 8 shows the flowchart of adding new records into the P3HR database.

Figure 8. Flowchart for adding new health records in the P3HR database.

F. Sharing Basic Profile

A patient may need to provide his basic profile info when he 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. Fig. 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, patient pseudonym is private and secret, we 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 his 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 his shared key.

An obvious better or safer way of sharing basic profile is through the patient smart IC card which needs card reader to be installed at the hospital. The sequence diagram in Fig. 10 includes this case. The card reader reads basic profile information and shows it to the party who has been authorized with his own smart IC card.
G. 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 P³HR 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 his 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. Fig. 10 shows a sequence diagram for of accessing a patient’s health record by a doctor when the patient (with his smart card) visits the hospital equipped with a card reader.

![Sequence diagram for accessing shared personal health records by a doctor](image)

Figure 10. Process of accessing shared personal health records by a doctor when a patient visits a hospital with his smart card.

V. Security and Privacy Analysis

We assume that each module of the P³HR system works properly and the described policies are enforced by the trusted service provider. We carry out intuitive privacy analysis of P³HR system.

A. Attacker Model

Internal threats 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 employer may try to breach patient privacy. We omit eavesdroppers of user’s network traffic as attackers, since secure communication between hosts can be used. We assume that an attacker cannot break cryptographic primitives and does not control the communication network.

Malicious patient and identity theft: The access control module allows a patient to view only the records that have the same pseudonym as his own. A patient’s pseudonym is not editable and a patient cannot modify it once it is stored. Thus, a malicious patient is forced to see his own records only. Besides, a patient needs to decrypt his pseudonym to view his health records. Even if the identity of a patient is theft 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 his 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 to access. 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 his 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 model, we can see that collaborative attack by malicious healthcare professional and malicious database administrator may result in privacy breach in P³HR system. All other types of attacks are not effective. However, healthcare professionals are generally trusted and not malicious. Besides, such unauthorized access can be detected
by maintaining access log properly. So, we can conclude that the privacy protection capability of P3RH system is very strong.

VI. PROTOTYPE IMPLEMENTATION

We have developed a prototype of our P3RH system. The prototype implementation has not included authentication by using smart IC card and uses only username/password based authentication (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 patient’s electronic health records of 25 years.

![Figure 11. Patient authentication screen of P3HR system.](image)

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

![Figure 12. Main menu (patient).](image)

The patient can view their 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.

![Figure 13. Decrypted profile of the patient.](image)

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

![Data Sharing Policy, edit record](image)

Figure 14. Part of data access policy where the patient sets what of his record set a doctor can view.

Fig. 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.

![Figure 15. Adding new share.](image)

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

![Figure 16. List of shared records.](image)

Fig. 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 basic profile. Figure 18 shows the patients health records that are shared with the current logged in doctor.

![Figure 17. Doctor trying to access patient’s basic profile.](image)
In our implementation, a patient can replace the hospital name that he visited with a pseudonym and maintain the list of hospital pseudonyms encrypted into his 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 that 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 his 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 and 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 his 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 his 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 mentally 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.

VII. DISCUSSION

We have devised a novel privacy management architecture, called P3HR, for patient-controlled personal health record system. It uses strong authentication mechanism using smart IC card. 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 be immediately be blocked by the authentication module and the respective patient should be issued a new card.

A patient should be able to use multiple pseudonyms and all of them need to be included into his encrypted profile so that all of his records remain associated with the patient.

In P3HR 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 physical patient and his pseudonym remains secret and does not need to disclose to anybody to use the system. The advantage of our system is that our stored database becomes most likely to be completely anonymous and it is very unlikely that the data subject could be identified from the stored records. Thus, our system allows patients to have their health records under their control and help making health care safer, cheaper, and more convenient. Most of all, it supports the necessary functionalities for healthcare industry with complete privacy protection of patients. We have intuitively analyzed the privacy aspect of our system and shown that it can tolerate almost all common attacks. We have developed a prototype system to illustrate the architecture and its functionalities.

REFERENCES

[8] iHealthAlliance. 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/