Emergency Access Authorization for Personally Controlled Online Healthcare Data*

Tingting Chen Sheng Zhong
Computer Science and Engineering Department
State University of New york at Buffalo
Amherst, NY 14260, U. S. A
Email : {tchen9, szhong}@cse.buffalo.edu

Abstract

Personally controlled health records (PCHR) system has emerged to allow patients to control the medical data of their own. All the data access privilege is given by the patient herself. However, in many emergency cases, it is impossible for the patient to grant the access right but she needs immediate medical treatment. To solve the emergency access authorization problem in the absense of patients, we consider two cases, i.e., a) the access requester is inside the PCHR system but does not have the access priviledge of the patient's health records, and b) the requester does not even have an account in the PCHR system to submit its request. For each of the two different cases, we present a method for emergency access authorization. The key idea of our design is that the patient can choose some trustworthy parties who are in the PCHR system and already have the access priviledge. When the patient is not present, the requester can ask for help from the patient's trusted parties, even if the requester is not inside the PCHR system. In the methods, we respectively utilize weighted voting and group authentication techniques, to guarantee that our emergency access authorization method is secure and effective.

1 Introduction

Traditionally, physicians keep the records of patients, such as progress notes, prescription history and test results, on papers. Local paper-based medical records are difficult for the communications between different physicians and healthcare institutions. Recently, the notion of electronic health record (EHR) has been brought forth. Achitectures for ubiquitous communications of EHR

*Correspondence Author: Sheng Zhong, Department of Computer Science and Engineering, State University of New York at Buffalo, Amherst, NY 14260, U. S. A. Phone: +1-716-645-3180 ext. 107. Fax: +1-716-645-3464. Email: szhong@cse.buffalo.edu

between clinics has been studied, which facilitates the high quality health care with all pertinent clinical data on a patient.

As a special type of EHR, personally controlled health records (PCHRs)[1, 2, 3] enable individual patients to aggregate, securely store and access their own electronic health records from various places. PCHRs are stored in third parties outside medical care system, for example, online repositories such as Google Health[], Microsoft Vault [], or large companies willing to keep PCHRs for their employees, such as Dosssia []. Each individual patient can subscribe to her health care records from physicians, clinics, laboratories and pharmacies, aggregating them into her own PCHRs. When a medical center requires the most updated pertinent clinical information of the patient in order to give health care, patients can grant the PCHRs access to the medical center. In general PCHRs motivate patients to collaborate actively in their medical care by taking control their medical information. Moreover, the ubiquitous and shared access to PCHRs improves the efficiency of the medical care system and lowers the cost of communication.

Some system architectures for using PCHRs in the medical care system have been studied, e.g., a web-based system Indivo []. Like other PCHR systems, Indivo for example, enables a patient to indicate in the system which other users (such as treatment sites) have particular privileges on specific portions of her record. Usually, if a patient goes to a certain medical center for the first time, after scheduling a treatment appointment, she grants this medical center with the access of the related health information in the PCHR system, such as her syndrome and allergy history. In this way, the patient can receive good treatment given that medical center has the information needed. However, in many cases, treatment need is urgent and it is impossible that the patient herself has the time or ability to get connected to the internet and grant the access to the clinics. For instance, a patient who has passed out is sent to the emergency room where she has never been. In this case, the more medical care information about the patient, the better for the consequential health care. Unfortunately, since the clinic does not have the privilege to any portion of the patient's data in the PCHR system, it is extremely difficult to perform high quality treatments. Moreover, it is also almost impossible to obtain the pertinent information from other health care centers where the patient has been to, under the coverage of the privacy and security regulations of HIPAA []. Now consider an even worse case, in which the medical center does not have the account in the PCHR system to log in, and thus it does not have a place to send its request for the patient's medical care data. Creating a new account usually takes a lot of time. It usually has a long and secure procedure to verify the identity and gather all the information to build a database entry for a newly joined medical center. Indeed, making sure the security of the PCHR system is necessary and important. However, it significantly impedes the process of emergency medical treatment, which may cause severe consequence to the patient. Hence we can see that restricting the access control to the individual patient may cause serious problem when the patient's participation is impossible.

In this study we solve the on-demand, especially emergent, access to PCHRs

problem in the absense of the PCHR owner. Our work can be viewed as an important complementary to the existing PCHRs systems. Our emergency access authorization method, which leverages the online group authentication technique in cryptography, provides a secure and private solution.

2 Challenges

To design the emergent authorization method for personally controlled health care data, we must overcome some challenges raised by the requirements of the existing PCHR systems and HIPAA regulations, so that our solution can be incorporated and become practical for real cases in health care systems. In particular, we mainly discuss the three most important factors as follows.

- **Security:**

  The system should be able to verify the claimed identity of an entity, either a person or an organization, in the absense of the PCHR owner. In emergency cases, if the entity is not recognized by the existing system (or the PCHR owner), the PCHR system should still be able to grant the right of temporal access to the entity, if some strict constraints are met to guarantee that the usage of the health care data is necessary and entity will use it appropriately.

- **Privacy:**

  The system should preserve the privacy of the patients. In particular, when a medical center inquires about the health care data of a patient, it should be that no one but the patient herself can know what kind of health data is being requested.

- **Timely Response:**

  The authentication and access privilege granting process should be done within reasonably short period of time, because otherwise the emergent access authentication method will lose its advantage of timely response in providing high quality on-demand treatment. Furthermore, the PCHR owner will eventually be able to recover all the control over her health care data, without timely response, the value of the emergent access authorization no longer exists.

3 Methods

To allow the emergency access authentication to the PCHRs without the presense of the patient, we present a secure and privacy-reserving emergency authorization method. We provide solutions for two different case: a) the emergency access requester can be recognized by the PCHR system (has an account), but is not allowed to read the patient's health care data; b) the requester is not

recognized by the PCHR system. The key idea of both solutions is to distribute the right of granting access privilege, to some other trusted parties, such as clinics and physicians that the patient is familiar with and thus trust. In the remaining of the paper, we call them the emergency contact group for each particular patient.

When emergency access authorization is needed by a certain medical care center, it sends a request to the PCHR system to access the PCHR of the particular patient, if the medical center has an account in the PCHR system where the medical care data of the patient stores. In this case, the PCHR system applies a weighted voting algorithm to verify the requester among the emergency contact group members. If the voting result indicates that all or most of the emergency contact group members recognize the requester as trustworthy, then the PCHR system grants it with a temporary access to the patient's data, otherwise it rejects the request. For this part of solution, we choose not to directly grant some medical centers with the temporary acess right by the patient herself within the existing PCHR system beforehand. It is mainly due to two reasons: a) the patient herself does not know when and where she will need the emergency health care treatment. Hence, if the temporary access right is given in advance, there must be cases that some temporary access is actually never needed in the real world. Then it increases the probability of abusing the temporary access by some medical care providers that the patient is not familiar with; b) it is difficult to define rules for granting temporary access as the patient does not know who are trusted by the parties that her trusts. On the other hand, the trust relationship between two particular medical care providers is a type of privacy and should be protected from the patient. Therefore, we present an emergency authorization solution within the PCHR system, which is on demand and privacy preserving. Certainly, after the emergency medical treatment, the patient is able to view the temporary access history recorded in the PCHR system. We will describe the weighted voting algorithm used in our method in Section 3.1 and discuss the design details of this on-demand method in Section 4. The issues to be addressed include, for example, how the emergency contact group is formed; and what is the relationship between the access-requiring party and the emergency contact group members; how this emergency access authentication method affect the exisiting PCHR systems.

When the medical center does not have an account in the PCHR system where the patient's medical care data stores, it becomes even more challenging to design a authorization method. The idea of our method is that the requester broadcasts its emergency need message using a secure and privacy preserving algorithm through other platforms, for example, Internet or the internal network built by some medical care association or administrations. Our method guarantees that only the trusted parties by the requester are able to read the request message and they can verify the identity of the requester. If they are in the emergency contact group of the patient, they requests to be a proxy of the requester in the PCHR system. When the request of becoming a proxy for an outside medical provider has reached a certain amount, the PCHR randomly pick one of them to be the proxy of the requester to read and update

the medical care data of the patient. Our method is based on a core component of group authentication algorithm, []. Now we first describe this secure and privacy-preserving authentication algorithm 3.2, and then in section 4, we present in detail how this algorithm can be adopted in our method.

3.1 Weighted Voting

When the emergency access requst is sent to the PCHR system by a certain medical center, there will be a weighted voting scheme running among the patient's emergency contact group. A weighted voting scheme is characterized by three components: the voters, the weights and the threshold. The N voters $(P_1, P_2, \cdots, P_N)$ are the emergency contact group members for a particular patient. A voter's weight w represents the importance of the vote by this voter when aggregating the votes. The patient assigns a weight to each emergency contact group member when it joins the group, based on how trustworthy the group member is and how the patient values the vote by this member when making the emergency access authorization decisions. The threshold q is the minimum voting score overall to pass the access request, and it can be assigned by the patient in the PCHR system.

Formally, we have

$$t = \sum_{i=1}^{i=N} w_i V_i,$$

where for each voter i, V_i is the vote towards a request and w_i is the weight of voter i. In Section 4, we will discuss how the vot for each voter V_i can be computed in an reliable and efficient way. t is the final voting score for a request. We can see that t is the weighted sum of all the votes from the voters. If the final voting score is above the threshold q, (i.e., $t > q$), the request is passed and then the requester can have a temporary access to the patient's medical care data in the PCHR system. Otherwise, the request will be rejected.

3.2 Group Authentication

Now we describe a group authentication algorithm [] applied in our method to deal with the case that the emergency access requester is not in the PCHR system. The group authentication is used when the access requester sends the help messages to its partners, outside the PCHR system. Its partners may have the privilege to the patient's data in the PCHR system and can perform as a proxy for the access requester. Here we define that all the partners and the access requester form a group. A group authentication scheme is used when a parner receives a help message (containing the patient information) from the requester, to make sure that the message is indeeded transmitted from one of his partners and the receiver knows who is the sender. Moreover, only the partners can understand the content of the help message; The help messages are just meaningless data to other receivers who are not in the partner group.

In the following we describe group authentication technique used in this paper.

- **Initialization**
  The group uses a set of primary keys $< s_1, s_2, \cdots, s_l >$. $l = O(w\log(1/q))$, where w and q are security parameters defined in the group. Each key s_i defines a pseudo-random function f_{s_i}. Each partner u in the group holds a subset R_u of the primary keys, such that the probability of each primary key s_i to be included in R_u is $1/(w+1)$. R_u will be used to verify the message when the partner u receives one. Each partner u also has a set of secondary keys $< f_{s_1}(u), f_{s_2}(u), \cdots, f_{s_l}(u) >$. The secondary keys are used when the partner u intends to send a help message to other partners in the group.

- **Message Authentication**
  When a partner u sends a message M, it computes an authentication using each secondary keys, and attaches all the l authentications to the message M. u sends out the message and authentications sequence, denoted as $M, MAC(f_{s_1}(u), M), \cdots, MAC(f_{s_L}(u), M)$.

  When a partner v receives a message, it computes all the secondary keys of u with primary key that v holds, using the psudo-random function for each primary key. It then verifies all the MACs which are computed using these keys.

4 Results

In this section, we present our emergency access authorization method in details which utilizes the weighted voting and group authentication techniques which has been discussed. In Section 4.1, we describe the emergency contact group and requester's partners group, and their relationship as well. In Section 4.2 and Section 4.3 we respectively present our emergency access authorization method for two different cases, i.e., the requester has an account in the PCHR system and otherwise.

4.1 Emergency Contact Group and Requester's Partners Group

An important component in our method is introducing an emergency contact group (ECG) for each patient, storing in the PCHR system. The initialization of an emergency contact group include the following steps.

- **Picking up ECG members** From the actors in the PCHR system (e.g., doctors, medical centers, physicians) who have the access authorization to the patient's health record, the patient picks up several trustworthy actors to be in her emergency contact group.

- **Assigning weights to each ECG member.** After choosing ECG members, the patient assigns a weight w_i for each ECG member i, such that the sum of all the weights equals to 1, i.e., $\sum_i w_i = 1$. The weight represents that the patient values the ECG members defferently. Some members may be more familiar to the patient and thus more trustworthy to her. A ECG member with a higher weight will play a more important role in the access decision making when the patient is absent.

- **Assigning vote threshold.** The patient also needs to assign a threshold to the voting results. The vote threshold indicates overall to what extent the patient trusts the decision by her emergency contact group.

Requester's partners group can be formed outside the PCHR system. For example, if two medical care center have cooperations, or they are simply within the same association, they can form a partners group.

Figure 1 illustrate the relationship between patient's ECG members and the requester's partners. As we can see, the requester may be a partner with some of the ECG members of the patient. Although the requester does not access privilege to the patient's health record in PCHR system, it can get help from those who are at the same time the ECG members of the patient and partners with the requester, based on the trust between the patient and the ECG group members.

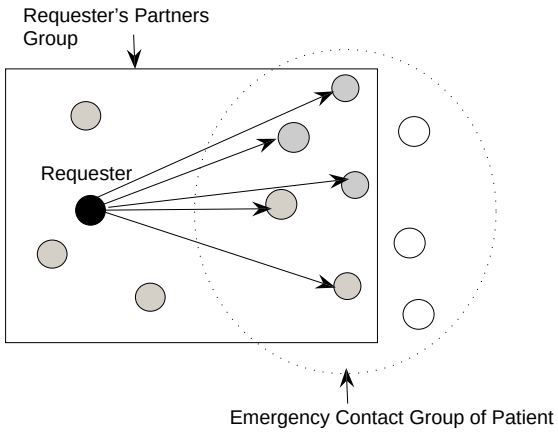

Figure 1: Illustration of the relationship among the Patient, Emergency Contact Group (ECG) and the requester's partners group.

4.2 Emergency Access Authorization for Insiders

Figure 2 summerizes the work flow of emergency access authorization for the PCHR system insiders. Within the PCHR system, requester fist sends its request to the authorization module, asking for emergency access authorization

for patient A. Then the authorization module looks up the emergency contact group members of patient A. It sends the patient and requester's information to the weighted voting scheme, which will perform a weighted voting scheme, as described in Section 3.1, to sends back the voting result to the authorization module. If the final voting score t is above the threshold set by the patient beforehand, then the authorization module grants the requester with the temporary access privilege, which will become expire in a short period of time. After that, the PCHR system makes a record of this emergency access authorization.

How the ECG group members vote. One major problem in the weighted voting scheme is how the ECG members compute their votes in an reliable and efficient way. The vote is defined within a finite field. For example, a valid vote can only an integer in the range between 0 and 10. The voting can actually take place with the interaction between ECG members and the PCHR system, but it may take a lot of time to wait for a ECG member's response. A simpler but more efficient way is that within the PCHR system, it stores the information about parters group relationship between the requester and the ECG members. For example, for each ECG member, its vote can be computed as 1 if the requester and itself are within one same partner group. Otherwise, its vote will be 0.

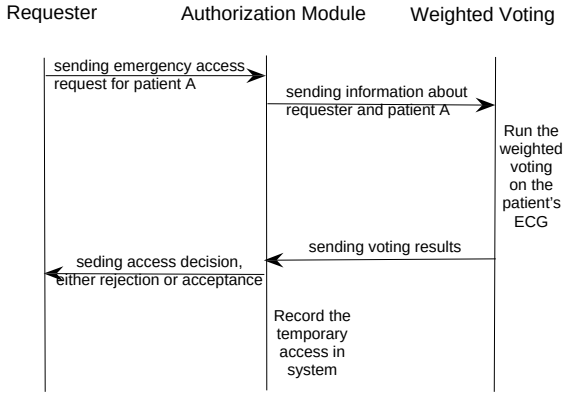

Figure 2: Work flow of emergency access authorization for the PCHR system insiders.

4.3 Emergency Access Authorization for Outsiders

The work flow of emergency access authorization for the PCHR system outsiders is illustrated in Figure 3. First, using group authentication method discessed in Section 3.2, the requester broadcasts its help message, which contains the identity of the patient and the health record it requests, together with the authentication codes of the message to all his partner group members. When receiving the message, its partner verifies that the message is indeed sent by the requester. After looking at the content of the message, if the partner is one of

ECG members of the patient, it sends a request to the PCHR system asking to be a proxy for the requester in getting access to the patient's health records. When the PCHR system receives enough such proxy request from the ECG members of a particular patient, the system randomly picks one of them as the proxy for the requester, and authorize such proxy function for a limited period of time. In this way, the proxy can first access the patient's health records which are requested by the requester and then transmit the data to the requester in a safe way, such as using asymmetric crypto-system.

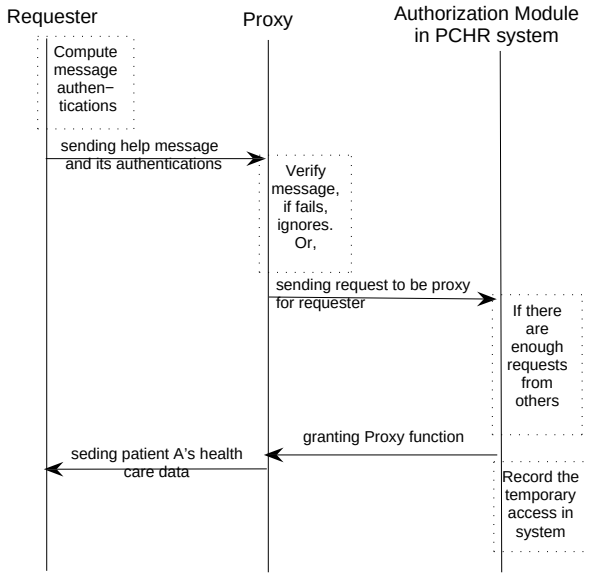

Figure 3: Work flow of emergency access authorization for the PCHR system outsiders.

5 Conclusion

PCHR system has emerged to allow patients to control the medical data of their own. All the data access privilege is given by the patient herself. However, in many emergency cases, it is impossible for the patient to grant the access right but she needs immediate medical treatment. To solve the emergency access authorization problem in the absense of patients, we consider two cases, i.e., a) the access requester is inside the PCHR system but does not have the access priviledge of the patient's health records, and b) the requester does not even have an account in the PCHR system to submit its request. For each of the two different cases, we present a method for emergency access authorization. The key idea of our design is that the patient can choose some trustworthy parties who are in the PCHR system and already have the access priviledge. When the

patient is not present, the requester can ask for help from the patient's trusted parties, even if the requester is not inside the PCHR system. In the methods, we respectively utilize weighted voting and group authentication techniques, to guarantee that our emergency access authorization method is secure and effective.

References

[1] The Personal Health Working Group. The Personal Health Working Group Final Report. Washington, DC: Connecting for Health: A Public-Private Collaborative, 2003.

[2] Committee on Data Standards for Patient Safety, Board on Health Care Services. Key capabilities of an electronic health record system. Washington, DC: Institute of Medicine of the National Academies, 2003.

[3] Thompson TG, Brailer DJ. The Decade of Health Information Technology: Delivering Consumer-centric and Information- Rich Health Care. Available at: http://www.hsrnet.net/nhii/ materials/strategic_framework.pdf. Accessed Aug 24, 2004.