

# Enabling Distributed Addition of Secure Access to Patient's Records in A Tele-Referring Group

Mingyan Li and Radha Poovendran  
Network Security Lab

Department of Electrical Engineering, University of Washington  
email: myli, radha@ee.washington.edu

**Abstract**—Protecting the privacy of patients' Electronic Health Records (EHR) while providing timely health care is an important issue in e-medicine. In this paper, we introduce an emerging problem of secure access to EHR added by the patient directly or by a physician who is not primary. We identify the design requirements, propose our solutions, and demonstrate that our solutions satisfy the design requirements.

**Keywords**— medical system security, privacy, electronic health records (EHR), access control, tele-referring

## I. INTRODUCTION

With advances in computer and networking technologies, vast medical records now exist in digital format. Compared to paper-based records, *Electronic Health Records* (EHR) are easy to transmit, store and share among medical professionals for high quality of health care. Meanwhile, the convenience of accessing and copying EHR imposes a threat on privacy protection of EHR.

The importance of patient privacy is highlighted by the federal legislation, Health Insurance and Practice Accountability Act (HIPAA), that was enforced in the United States in April 2003 [1]. Considerable research efforts have been conducted to propose approaches and build prototypes to ensure the confidentiality, authenticity and integrity of EHR. As a representative of research efforts, *Digital Imaging and COmmunication in Medicine (DICOM)* standard [2] provides guidelines in securing and integrity protecting EHR during transmission and in storage. However, the standard mainly focuses on safeguarding EHR against non-intended access in an entity-to-entity based communication. In a clinical environment, treatment of a patient often involves a team of medical personnel, such as a primary physician, specialists, and nurses. In such a group environment, it is a challenge to ensure only the valid medical personnel have access to the patient's EHR, so that patient's privacy is guaranteed, while the records can be retrieved to provide best possible treatment for the patient.

When a patient visits his/her primary physician, the primary physician forms a team of referring physicians/specialists<sup>1</sup> who collaborate on the patient's case. Together, the primary and referring physicians constitute a *referring group*, or a *tele-referring group*. Only the patient and referring group members have access to the patient's file. However, in some cases, additional specialists will be added to the referring group to provide better treatment. While the primary physician can add suitable specialists to the group, there are scenarios that a patient may directly contact a specialist of his/her choice, without consulting the primary physician. For these scenarios, we must develop mechanisms that allow a specialist to be added directly by the patient. Any such new addition must be verifiable during the access to EHR to protect patients' privacy. Other challenges arise when a referring physician may need to refer the patients case to additional specialists. To enable such secondary referrals, i.e., adding specialists by a referring physician, the referring physician can contact the primary physician. If the primary physician is always available to process the request from a physician, the secondary referral will not be an issue. However, availability of the primary physician cannot be assumed all the time. Therefore, in order to ensure timely treatment to the patient, we need to build the mechanism so that a primary physician can delegate the right of adding new physicians to referring physicians.

As illustrated in Figure 1, the access permission given directly by a patient  $T$  to specialist  $S_A$  (scenario b), and that by specialist  $S_A$  to specialist  $S_B$  (scenario c), without compromising patient's privacy are the focus of the study in this paper. To the best of our knowledge, there is no prior research on addressing these scenarios.

The structure of the paper is as follows. Section II states the problem addressed in this paper and defines system requirements. In section III, we present several

<sup>1</sup>In this paper, we use referring physicians, specialists, secondary physicians interchangeably.

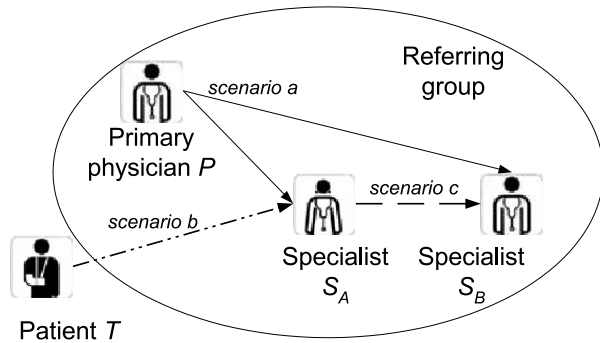


Fig. 1. Adding specialists into the referring group. The solid line indicates the current practice of EHR access (scenario a). The dotted lines are the new problems addressed in our paper: How a specialist is added to the EHR access list by a patient (scenario b) or by a secondary physician (scenario c)?

potential solutions to the patient’s authorizing a specialist to obtain his/her EHR, and compare the advantages and disadvantages of these solutions. In section IV, we address the issue of a secondary physician adding one or more specialists to the referring group, on behalf of the primary physician. In section V, we present related work. Finally, we conclude our paper with future research directions in section VI.

## II. PROBLEM STATEMENT AND DESIGN REQUIREMENTS

A referring group is associated with an *Access Control List (ACL)* that defines the access right of the group members. The primary physician owns the ACL and configures security parameters such as time duration of access in the initial phase. During the course of the treatment, additional referring physicians may need to be consulted and hence, be granted the access to EHR by the primary physician, the patient, or by a specialist. Such additions require the modification to the ACL.

In this paper, we address the problem of *how to enable multiple authorized entities, rather than only the primary physician, to manage the ACL*. We first determine what actions towards the maintenance of the ACL are allowed for the primary physician, the patient, and referring physicians. We also consider the exception to handle the emergency access.

- **Primary physician** is the owner, and responsible for the management of the ACL. He/she has the right to modify the list, including add and delete a referring physician. Note that more than one physician may be primary at different times, but at any given time only one physician fills the role of primary physician.
- **Patient** is allowed to see any specialist with or without consulting the primary physician. Hence, a

patient must be able to add access to his/her records without referring the primary physician, i.e., adding a specialist of his/her choice to the ACL directly; But a patient is never allowed to write into EHR or delete/replace a record in the ACL.

- **Referring physician** cannot add additional specialists, unless there is an approval from the primary physician (in real-time, or offline, or prior approval).
- **Emergency access** overrides the need to get any prior permission for EHR access, and hence, allows additions to the ACL. However, any deletion/replacement in the ACL is never allowed. At any given time, the authenticity of the additions must be verifiable. The entity performing additions to the ACL must be at least at the same level of the primary physician in terms of the security hierarchy.

The following security properties need to be achieved by any solution to the management of the ACL:<sup>2</sup>

- Except in an emergency situation, only the medical personnel with permission from a patient or the patient’s primary physician, have access to EHR.
- Integrity and authenticity of patients’ EHR can be verified by any valid entity.
- Access/modification to the ACL should be traceable by using auditing, as well as by verification at any time.

The following are a set of implementation requirements.

- Adding new physicians can be performed either by physical interaction, in which person-to-person authentication is possible, or online, where there is no physical interaction.
- A patient is not required to have any special skills.
- The implementation should be low cost to enable scalable deployment.
- The implementation should be fault tolerant, and robust against machine failure.

Before proposing solutions for access granting in a distributed fashion in a tele-referring group, we first state our assumptions in the following. As a physician often needs to sign on a document to admit his/her approval, a digital signature [3] serves as a proof of authenticity and authorization in the electronic world. A digital signature requires the signer to possess a unique pair of public and private keys [3]. We assume that each physician holds such a unique public/private key pair, which is also a requirement in DICOM [2], for authentication, secure transmission, and integrity verification of EHR. The patient’s EHR are stored in a central database, and a

<sup>2</sup>We note that anonymity or pseudonymity of a patient is not an issue here, since the patient’s name will be revealed once the file of a patient is retrieved.

TABLE I  
NOTATION

$P$	Primary physician	$S_j$	Specialist $j$
$T$	Patient	$C$	Central server
$\parallel$	Concatenation	$\rightarrow$	Sending
$K_i/K_i^{-1}$	Public / private key of entity $i$		
$\{m\}_{K_i^{-1}}$	Message $m$ signed using $i$ 's private key $K_i^{-1}$		
$\{m\}_k$	Message $m$ encrypted using symmetric key $k$		

central server verifies the ACL before allowing the access to EHR. We also assume that integrity and confidentiality of the ACL are well protected. For example, the ACL can be stored in a tamper-resistant device. Due to page limit, we do not discuss authenticity and integrity protection of patients' records, which have been discussed in [4], [5].

Notations used in this paper are listed in Table I. We will also use  $P$ ,  $S_j$  and  $T$  to denote the identity (ID) of the primary physician, specialist  $j$  and the patient, respectively.

### III. ADDITION OF A SPECIALIST BY A PATIENT

To enable a patient to directly assign the access right to a specialist, a proof of permission from the patient must be presented. Additionally, the authenticity of the proof must be verifiable. Also the intended specialist needs to authenticate himself/herself.

#### A. Smart-card-based solution

A *smart card* is a credit-card size device with a micro-processor and memory embedded. It can securely store a key that is not extractable from the card, or can be revealed only when a correct *personal identification number* (PIN) is entered. A smart card can also perform digital signing. If every patient can be equipped with a smart card, (which is the case in Germany), then the card can carry a private key. The patient  $T$  can add a specialist to the ACL by using the private key  $K_T^{-1}$  to digitally sign the message that contains a verifiable, unique ID of the specialist,<sup>3</sup>  $S_j$ , the action to the ACL, and valid period of access as follows:  $\{S_j \parallel \text{addition to the ACL} \parallel \text{start and expiry date of the access}\}_{K_T^{-1}}$ . The explicit specification of expiration date prevents any attempt to reuse the signed message for unintended time duration by *message replay attack*, and also facilitates the management of the ACL in case of revocation.

The drawback of smart-card-based solution is that its deployment cost. Every access point must include a smart

<sup>3</sup>We assume that the patient is able to obtain the specialists ID either from a published list on the web or by verifiably communicating with the specialist in advance.

card reader. In fact, the associated cost for distribution of smart cards and deployment of card readers has been a major factor in preventing the smart-card-based solution from being globally deployed.

#### B. Password/PIN-based solution

Another approach to allow a patient to add to the ACL is by logging in using password. The weakness associated with the approach lies in password protection, which is subject to password guessing. The length of a password/PIN is limited by a human's memory, therefore, the search space of a password/PIN is too small to provide high security [6]. Enforcing a hard-to-guess password/PIN yet easy-to-remember for users has been a challenge in practice [3].

#### C. Token-based solution and Token-PIN-based solution

A token is a random string. The primary physician can issue a token, or *random identifier* (RI), to the patient. Compared to the password/PIN, machine-generated RI enlarges the search space for a guesser, due to the longer length and stronger randomness in the identifier. The RI can be printed out on a piece of paper as barcode [7], or can be stored in a magnetic stripe. Compared to smart cards, both barcode and magnetic cards are low cost, and their readers are more widely used.

To ensure the robustness against reader failure, we employ the backup as in [7]: an alphabetical representation of the RI is printed out and given to the patient. This printout can be used to enable authorization when the token reader is not available. To protect the integrity of identifiers issued, error-correcting code-based techniques can be employed in generating identifiers. With the checksum of an identifier attached, the integrity of the identifier can not only be verified but some errors can be corrected.

However, the problem with the token-based solution is its vulnerability to theft and loss, due to the fact that the possession of the token gives the right of adding a specialist. To defend against a theft and loss, additional secret information to identify the patient, such as a biometric, or patient's generated PIN, should be provided in order to complete the procedure of adding a referring physician by the patient. Social security number of the patient cannot be used as the PIN, as it can be retrieved by medical professionals. A barcode or magnetic card based authentication token, combined with a light-weighted PIN, resists token theft and forgery, and is robust against password guessing. At the same time, the token-PIN-based solution satisfies the low-cost deployment requirement, and the alphabetic printout of the RI plus error-correcting code techniques enhances robustness against device failure. Therefore, we

propose to use the token-PIN-based solution for adding a specialist directly by a patient.

#### D. Adding a specialist by means of a token-PIN with/without physical interaction

In a clinic, after a specialist successfully authenticates himself/herself, the token carried by the patient is read and the PIN has to be entered by the patient, before the addition of a specialist to the ACL is approved. Once the token and PIN are verified to be valid, the specialist is granted the access to the EHR with the access period taking a default value configured by the primary physician during the initialization of the ACL.

To add a specialist  $S_j$  online, the patient  $T$  inputs both the PIN and the RI, to authenticate himself/herself and to prove his/her right to add a referring physician, and sends the following message encrypted by the RI, to the central server  $C$ .

$T \rightarrow C: \{ S_j \parallel \text{addition to the ACL} \parallel \text{start and expiry date of access} \}_{RI}$

At the same time, the patient notifies  $S_j$  through an email. The specialist can then access the patient's EHR after successful authentication.

#### IV. ADDITION OF A SPECIALIST BY ANOTHER SPECIALIST

When a referring physician  $S_A$  needs to add another specialist  $S_B$  to the referring group,  $S_A$  can contact the primary physician  $P$  to issue the specialist  $S_B$  the access to the patient's records. The primary physician can digitally sign a message as  $\{S_B \parallel \text{addition to the ACL} \parallel \text{start and expiry date of the access}\}_{K_P^{-1}}$ . This approach of adding a specialist may not always be possible or desirable, due to the non-availability of the primary physician and/or the delay in gaining the approval from the primary physician. In order to guarantee timely treatment even in the absence of the primary physician, it is desirable that the primary physician is able to provide a signed delegation *certificate* to the referring physician  $S_A$  with which,  $S_A$  can add a set of necessary specialists on behalf of the primary physician by sending a *request* to the central server  $C$ .

The delegation process must satisfy the following properties:

- *Non-forgeability*: no one can forge a valid delegation certificate, and only the authorized specialist can make use of the delegation certificate from the primary physician to add new specialists to the ACL.
- *Non-repudiation*: a delegated specialist cannot deny adding a specialist to the ACL, and the primary physician cannot deny delegating the designated specialist to add new specialist. Both of these must be provable.

- *Identifiability*: The identity of both the primary physician and the designated specialist can be verified from the request.
- *Verifiability*: With public parameters, the authenticity and the integrity of the certificate and the request can be verified by anybody.

#### A. Solution using digital signature

A solution to the delegation problem is to employ *proxy signing* [8], in which the designated specialist, as a proxy signer, can sign the request to add another specialist on behalf of the primary physician. One approach to proxy signing is that the designated specialist generates a pair of public and private keys and has the primary physician certify the newly generated public key. The designated specialist can then sign an adding request using the corresponding private key. However, we notice that the actions that are delegated by the primary physician to a specialist is restricted to only adding a specialist in our case, rather than general signing on any message. The restriction allows for the use of a much simpler strategy than proxy signing as a valid solution to the delegation problem here.

Our solution, which requires no generation of key pair, and hence, reduces the complexity of key management, is presented as follows.

- 1) The primary physician  $P$  issues a secondary physician  $S_A$  a *certificate*, which specifies the delegation policy digitally signed by  $P$ . The policy parameters include the ID of the designated specialist  $S_A$ , the actions allowed, the reference number of the ACL related to the patients case, and the valid period of delegation.

$P \rightarrow S_A$ : the certificate =  $\{S_A \parallel \text{allowed to add} \parallel \text{index of ACL} \parallel \text{start and expiry date of the delegation}\}_{K_P^{-1}}$

- 2)  $S_A$  sends the central server  $C$ , a *request* to add another specialist  $S_B$  to the ACL,

$S_A \rightarrow C$ : the request =  $\{P \parallel S_A \parallel \text{the certificate} \parallel \text{adding } S_B \text{ to the ACL} \parallel \text{valid access period}\}_{K_{S_A}^{-1}}$

#### B. Proof of correctness

Now we prove the correctness of the solution proposed, by demonstrating that the solution satisfies all the properties defined.

- *Non-forgeability*: the request contains two signed messages, with one from the primary physician  $P$  and the other from the designated specialist  $S_A$ . Neither of the two physicians individually or no one else can generate such a request message. Since the certificate

contains the ID  $S_A$ , only the request digitally signed by  $S_A$  will be accepted, and no one else can make use of the certificate.

- Non-repudiation: the certificate indicates  $P$ 's consent to delegate  $S_A$ , and the request signed using  $S_A$ 's private key ensures non-deniability from  $S_A$ .
- Identifiability: since the IDs of  $P$  and  $S_A$  are prefixed to the certificate and contained in the signed request, they can be verified.
- Verifiability: using public keys of  $P$  and  $S_A$ , the authenticity and integrity of the certificate and the request can be verified.

Due to the format of the proposed digitally signed certificate, a specialist added by a patient directly cannot add another physician without communicating with the primary physician. This is a desirable feature since it allows aggregation of the treatment summaries to one location by preventing a specialist from building an autonomous referring group and denying information to the primary physician.

## V. RELATED WORK

To the best of our knowledge, problem of enabling multiple authorized entities to issue the access to a patient's EHR in a referring group has not been investigated before. In [7], [8], the access transfer of the electronic prescription has been discussed. In [7], a barcode-based solution is proposed to transfer the e-prescription access to the pharmacy chosen by a patient. However, as shown in section III-C, the token-only-based solution is vulnerable to theft and loss. Moreover, in e-prescription, reuse of the same token is not allowed to prevent the patient from using the same prescription multiple times. However, in the referring procedure considered in this paper, to attain low complexity, it is preferred that a patient can add more than one physician by using the same token. Therefore, reuse of a token needs to be addressed in a tele-referring group. In [8], a smart-card-based anonymous e-prescription system is presented that requires generation of proxy signing keys. Since anonymity is not an issue in adding referring physicians, we can employ much simpler solutions without requiring expensive smart card and complicate proxy signing. In the Poket Doktor System (PDS) [9], a patient carries a wireless communication capable device containing the EHR, and enables only the legitimate personnel to access the EHR. The salient feature of the PDS is wireless accessibility to EHR in emergency situation, even without physical access to the device. The PDS solution that requires a special device for each patient is suitable for homecare of elderly people, but may not

be feasible for all applications in the near future due to deployment cost.

## VI. CONCLUSION AND FUTURE WORK

The access control to a patient's EHR has to be performed to protect patients privacy. At the same time, the access should be enabled in a distributed manner in order to provide timely treatment and allow the flexibility of the patient in choosing specialists. In this paper, we introduced and addressed the problem of granting a specialist the access by a patient directly, or by another specialist who is not the primary physician. As a solution for direct authorization of a specialist by a patient, we proposed the token-PIN-based approach, which is robust to token forgery, theft, PIN guessing, while having low complexity and cost. For delegation of enabling access to EHR, by the primary physician to a specialist, we propose a simple solution that satisfies non-repudiation and non-forgeability, while being easily implementable.

As future work, we will address the problem of restricting the access so that a physician can retrieve only the *part* of the patients' records to which the physician's current treatment activities are related. We will also investigate the problem of the ACL consistency when the identity of primary physician changes over time.

## REFERENCES

- [1] United States Department of Health & Human Services, "HIPAA: medical privacy - national standards to protect the privacy of personal health information," [Online], Available: <http://www.hhs.gov/ocr/hipaa/>.
- [2] HEMA, "DICOM: digital imaging and communication in medicine," [Online], Available: <http://medical.nema.org/>.
- [3] C. Kaufman, R. Perlman, and M. Speciner, *Network security: private communication in a public world*, 2nd ed. Prentice Hall PTR, 2002.
- [4] F. Cao, H. K. Huang, and X. Q. Zhou, "Medical image security in a HIPAA mandated PACS environment," *Computerized Medical Imaging and Graphics*, vol. 27, pp. 185–196, 2003.
- [5] M. Li, R. Poovendran, and S. Narayanan, "Protecting patient privacy against unauthorized release of medical images in a group communication environment," *Computerized Medical Imaging and Graphics*, 2005, accepted.
- [6] M. van der Haaka, A. C. Wolffa, R. Brandnera, P. Dringsb, M. Wannenmacherc, and T. Wetter, "Data security and protection in cross-institutional electronic patient records," *International Journal of Medical Informatics*, vol. 70, pp. 117–130, 2003.
- [7] E. Ball, D. W. Chadwick, and D. Mundy, "Patient privacy in electronic prescription transfer," *IEEE Security and Privacy*, vol. 1, no. 2, pp. 77–80, 2003.
- [8] Y. Yang, X. Han, F. Bao, and R. H. Deng, "A smart-card-enabled privacy preserving e-prescription system," *IEEE Transactions on Information Technology in Biomedicine*, vol. 8, no. 1, pp. 47–58, 2004.
- [9] E. S. Hall, D. K. Vawdrey, C. D. Knutson, and J. K. Archibald, "Enabling remote access to personal electronic medical records," *IEEE Engineering in Medicine and Biology Magazine*, vol. 33, no. 3, pp. 133–139, 2003.