J Med Syst (2012) 36:3103–3113
DOI 10.1007/s10916-011-9793-z

ORIGINAL PAPER

A Secure Integrated Medical Information System

Tsung-Chih Hsiao · Zhen-Yu Wu · Yu-Fang Chung · Tzer-Shyong Chen · Gwo-Boa Horng

Received: 11 August 2011 / Accepted: 12 October 2011 / Published online: 3 November 2011

Abstract The rapid rise and development of the internet has made digitization of our everyday life common. E-medicine, including electronic prescription records, electronic prescriptions, diagnosis information systems, and others are now being regarded as future trends. As development on the structure and format of electronic patient records and prescriptions matures, the implementation of a comprehensive medical information system is imperative, one which is constructed from integrating the various electronic information systems that is being developed. It is important to allow the implementation of such a system applicable to the present medical environment, which facilitates the integration of electronic patient record from all levels of medical centers and clinics, secures the transmission of these integrated patient records between them, enables the combined use of electronic prescriptions with patients' medications, and permits anonymous or confidential transmission of patients' private data. To put the ideas into practice, in this study, we would like to propose an Integrated Medical Information System.

T.-C. Hsiao · G.-B. Horng
Department of Computer Science and Engineering,
National Chung Hsing University,
Taichung, Taiwan

Z.-Y. Wu
Department of Information Management,
National Penghu University of Science and Technology,
Penghu, Taiwan

Y.-F. Chung
Department of Electrical Engineering, Tunghai University,
Taichung, Taiwan

T.-S. Chen (✉)
Department of Information Management, Tunghai University,
Taichung, Taiwan
e-mail: arden@thu.edu.tw

Keywords E-medicine · Electronic patient records · Electronic prescriptions · Comprehensive · Integrated medical information system

Introduction

A medical information system is generally composed of heterogeneous information systems from several medical departments. Based on relevant literatures, eight considerations for developing medical information systems are organized, including (1) the heterogeneous integration of information systems among departments, (2) individual requirements of information systems in departments, (3) the requirements of medical information systems from local to global, (4) the requirements of changeable medical information systems and medical environments, (5) the scalability of medical information systems, (6) the introduction of electronic medical record (EMR), (7) the scalability of the efficacy of medical information systems, and (8) the medical information system for the advanced generation. Based on these issues, four objectives for developing new medical information systems are further proposed, namely (1) adaptability and scalability, (2) heterogeneous system integration, (3) the introduction of electronic medical record (EMR), and (4) high system efficacy and the scalability of system efficacy.

Recently, with the rapid development of Internet, various technologies for applications are maturing, leading to the digitization and electronic orientation of our daily-life activities such as e-commerce, e-medicine, e-banking, e-government, and e-society. In e-medicine region, such developments include the use of the healthcare IC cards [4], digital certificates and signatures for medicine applications, electronic patient records (EPRs) and electronic prescriptions (e-prescriptions) [13,

25, 29, 30], and so on, the development of which, has come to mature and have been used in most hospitals or medical institutes during the last decade. This field nonetheless, remains as one of the most popular researches.

As research on the structure of healthcare cards and digital certificates, format of EPRs and e-prescriptions come to mature, there remains substantial room for breakthroughs in the construction of a medical information system that allows the exchange, and transmission of EPRs and e-prescriptions, such as in regard to format unification of the patient records of different medical institutes [9, 27], security agreements on medical information exchanges between different institutes [2, 8, 16], identity authentication in remote telecare [12, 18], etc. In the implementation of such a system that is applicable to the present medical enviorment and can integrate the current digitized medicine information, these remain as crucial issues.

This study proposes an integrated medical information system with Service-Oriented Architecture (SOA) to solve the issues related to tradition medical information systems as well as provides medical staff with a single and integrated patients' medical information. An appropriate and suitable Integrated Medical Information System (IMIS) should thus be concerned with some of the significant points as follows:

The first regards to the construction and use of the enhanced healthcare IC cards. Currently, all major healthcare cards used in the medical environment are based on IC-chip cards [17]. These have little memory space, and do not possess computational abilities. In actual application, they cannot assist the patient in their needs for digital signatures, or encryption in regard to their health records, prescriptions, physical examination results, or receipts. These cards may even have to employ and integrate with authentication systems for use, making them inconvenient and risky. Therefore, it is necessary to develop an enhanced healthcare card for solving the above mentioned problems. Considerations should be given to the material of the card, or medium of storage, etc., such as: Read Only Memory (ROM), Random Access Memory (RAM), Erasable Programmable Read Only Memory (EPROM), and so on. These in turn should be adopted according to their characteristics and advantages. Furthermore, there should be proper designs in regard to the information stored in the card, that they be classified and separated according to different levels, urgency (in case of emergencies), and also modes of access. More shall be discussed in Smart card section.

Second is to implement a complete e-prescription system combined with the medical system. In most countries, diagnoses and prescriptions are still largely filed in paper. With the current trend of EPRs, prescriptions have also come to be digitized [30]. In future, pharmacies and patients should be able to authenticate the accuracy, completeness, non-repudiation, and confirmation of the e-prescriptions with the use of digital signature technology. At the same time, pharmacies should be able to file with insurance companies using the receipts of e-prescriptions through authentication systems via the networks.

The third regards protecting the privacy of patients and physicians [1, 23]. There are two main points regarding protecting patients' privacy, one being the question of morality. From an empathy perspective, patients' condition or illness should not be publicly disclosed, no matter what disease they have or might have (especially sexually transmitted diseases, and mental illnesses); they would certainly like to keep them private, other than from their physicians. Secondly, stemming from privacy protection, a patient can be assured of the security of his clinical data for the public use for medical research by institutions in order to find better medical treatment to treat the illness [14, 26]. This is the biggest advantage that can be gained from ensuring patients' privacy [28].

In terms of protecting the privacy of physicians, there are two main points [31]. The first concerns how it allows healthy competition. When a patient is treated by a different physician from the same department, there are chances he may be prescribed a different prescription after diagnosis. To avoid duplication of prescriptions by authoritative physicians, which would be counter-productive to researching better treatments, we should be careful not to leak out the private information of physicians. The second concerns the possibility of market monopolies by pharmaceutical companies from copying prescriptions. If, today, a pharmaceutical company acquires a prescription from an authoritative physician or institution and develops it into a drug, this will inevitably cause a hot trend for buying the drugs, resulting in market monopoly. Therefore, a prescription that can be transmitted over the networks should be capable of protecting the physicians' privacy (either through encryption or anonymity) to prevent such incidents from happening.

In another matter, to claim an IMIS safe, secure, convenient, and complete, it should satisfy the following six conditions and characteristics.

(1) Mobility for the recent medical records

Recent diagnoses and e-prescription data should be stored in the healthcare card, so that no matter where the patient seeks for medical assistance, the medical staff can conveniently access previous diagnoses from the card after authentication, speeding the diagnoses for appropriate treatment, without the hassle of rerunning unnecessary physical examinations, and improve diagnosis rate. When the medical staff is met with cases of medical emergencies, easy mobility for the patients' medical records will be largely desired.

(2) Function of proxy prescription collection

For the patients' convenience in collecting prescriptions, storing the information of authorized agents for proxy prescription collection in patients' healthcare card allows patients who cannot collect them personally (due to physical or mental disabilities) to legally entrust agents to collect them on their behalf, assuring that the drugs will not be lost or being falsely claimed.

(3) Linkability and privacy protection

Based on the above mentioned, whether it is the privacy of patients, or of the physicians who see the patients, in the current trend toward e-medicine, they are both questions that have been given considerable attention. Therefore, before developing an IMIS, we established four principles:

(a) Anonymity: Patients and physicians should operate under different pseudonyms.
(b) Linkability: Other than health insurance companies, who will have information of patients' true identity, the pharmacies can only distinguish different e-prescriptions for the same patient, but will not know of his identity.
(c) Physicians' Linkability: Other than trusted medicine associations, who can know of the physicians true identity, health insurance companies can only distinguish different e-prescriptions prescribed by the same physician, but will not know of his identity.
(d) Physicians' Non-Linkability: Pharmacies will not be able to know from the contents of e-prescriptions of the physician who prescribed them.

(4) Prevention of patients' illegal refilling of prescriptions

When medical care become fully digitized, it will become relative easy to obtain e-prescriptions than hand-written ones. To prevent interested parties from duplicating the e-prescription and collecting them from pharmacies illegally causing wastage in medical resources, an accomplished IMIS should be capable of preventing such activity. For example, this can be prevented by inserting into the healthcare card the e-prescription details and the immediate serial number generated before the prescription is collected. After the prescription is collected, the data in the card is automatically deleted so that only the e-prescription number is retained for recording. This way, the prescription will not be refilled unauthorized.

(5) Prevention of pharmacies' extra claims by inflating the amount of drugs prescribed

In addition to the problem of unauthorized refills by patients, in the current trend of separating pharmacy from medicine, incidents of pharmacies making extra claims from insurance companies by inflating the amount and price of drugs prescribed are possible scenarios. For example, corrupt pharmacies may conspire with malicious parties to obtain e-prescriptions from physicians; such e-prescriptions are forwarded to the corrupt pharmacies and are then filled out without dispensing the drugs, thereby allowing the pharmacies from making illegal claims from insurance companies by inflating the amount and/or the price of the drugs dispensed. When the digital signature technology is integrated with the IMIS, with the help of insurance companies and quantity controls by pharmaceutical companies, such malpractices can be prevented.

(6) Conspiracies between physicians and patients/pharmacies

Even under the current medical and insurance system, conspiracies between medical staff with patients or pharmacies for profit are still difficult to prevent. For example, a patient who is not sick make visits to a physician and conspires together to allow the physician from making claims from insurance companies. In another case, the physician conspires with the pharmacy and prescribes expensive drugs, directing patients to collect them from specific pharmacies and thereby pocketing a cut from the profit derived. Therefore, public authorities should be involved in the development of an IMIS in order to set up a Trusted Third Party (TTP) to conduct investigations on unusual medical transactions in order to eliminate illegal activities. In addition, the unit can also be a fair and impartial arbiter for mediating disputes between physicians, patients, and pharmacies.

An IMIS that meets the above mentioned three significant points and six requirements is brought up below. The rest of this paper is organized as follows. Preliminary section introduces the corresponding techniques employed in our proposal. The proposed scheme section illustrates the proposed IMIS. Security analyses are done in Security analysis section, and finally, conclusions are drawn in Conclusions section.

Preliminary

The proposed IMIS employs several computer science techniques and products such as public-key cryptosystems, digital signatures, and smart cards. Among this, the digital signatures also can further be extended to become group signatures or proxy signatures to be employed in different regions of our scheme. They are explained as follows:

Public-key cryptosystem

The concept of public-key cryptosystems was first proposed by Diffie and Hellman in 1976 [7], which opened a new direction on cryptography development. Since then,

many researchers started proposing various types of public key cryptosystems.

Public-key cryptography is a kind of asymmetrical encryption technique. Each party in such cryptosystem holds two keys; one is the public key used to encrypt a datum and the other is the private key used to decrypt. Usually, a cryptosystem is used to protect the data transmitted through the Internet from tampering by an illegal third party. For instance, a document is encrypted by a receiver's public key before it is sent out. Thus, the encrypted document only can be derived by a receiver who uses his own private key. It is impossible for an illegal party to decrypt the contents of the document, except when the receiver's private key is obtained and used to decrypt the message. Although the cryptosystem can make data transmission become more confidential and convenient, both the sender and the recipient must hold each other's key sets at the same time in order to perform encryption and decryption tasks. This is not practical enough. Therefore, a Public-Key Infrastructure (PKI) method is proposed to solve this impractical problem [24].

A PKI scheme is constructed on the basis of the public-key cryptosystem framework so as to offer all the security requirements, including authentication, confidentiality, message integrity, and non-repudiation. Certificate Authority (CA) is a part of the PKI scheme. The CA is a TTP in the scheme that manages and issues the certificates to the requesters and provides services such as keeping public keys, offering directory service, and issuing certificates. Under the PKI scheme, both parties are capable of exchanging information securely and safely with each other on the network.

Digital signature

All specific digital contents are capable of being encrypted and decrypted to ensure their integrity and non-repudiation. With agreement from all related parties, digital signatures are valid to be used in private communication. The concept of digital signatures originally coming from cryptography is a way to encrypt or decrypt senders' text messages by applying a hash function to keep the messages secure when transmitted [10, 20, 21].

A one-way hash function is a mathematical algorithm, which takes any length of a text message as input and gives an output in a specific length. Its main function keeps the encrypted output impossible to be derived by a third party [24]. Based on one-way hash functions, a digital signature scheme can be done as follows.

Based on a Public-key cryptosystem, a sender firstly uses a one-way hash function to convert an electronic record into a text message of a specific length, which is called the message digest [20]. Then, the sender will use his private key to sign on the message digest generating a digital signature. As the recipient receives the message and its signature, he can use the sender's public key to verify the signature for the message through the hash function. If the calculated message is not the same as the message itself, it is possible that a wrong document is outputted because of tampering. On the contrary, it is the valid document that the recipient wants. Obviously, this method can help to ensure data transmission security.

In order to use the digital signatures appropriately in our proposed medicine environments, we use the extended forms of digital signatures, i.e. group signatures and proxy signatures in the IMIS. Below are some simple explanations about them.

Group signature

The concept of group signature was proposed by D. Chaum and E. van Heys in 1991 to permit legitimate members of every group to sign anonymously to the message on the behalf of the whole group [3]. Only in the event of a dispute, will the identity of the signer be made known through the verification by the TTP. Group signature is usually used in messages released by a group, where any group member can generate the group signature using the individual private key, i.e., multi-signing. Logically, multi-signing as well as the single corresponding public key comprises group signature [5]. To the applications under medical environment for example, a group can be regarded as a medical team that includes the attending physician, the residents, and other staff taking care of a patient. Through group signatures, users can verify that patients' medical record or e-prescription is indeed prescribed, signed, and completed by a member of the group against any attempt of recognizing which precise member was it, fulfilling the linkability characteristic mentioned in Introduction section. Should a medical dispute arise, the medicine association, a TTP, the signature of the physician who signed the documents can be made known.

Proxy signature

Proxy signature was first proposed by Mambo et al. in 1996 [19], whose signature method's participants include an original signer, proxy signer, and verifier. The proxy signer under the delegation of the original signer can sign on his behalf. The delegations can be classified into full delegation, partial delegation, and delegation by warrant. The most commonly used is delegation by warrant [6, 15], i.e., the appointment letter will have the identification codes of the original signer and the proxy signer, and also the terms and period of delegation, etc. In its application, it is desired to empower the IMIS with the ability to allow proxy prescription collections for the physically disabled, or

patients who cannot collect in person, to collect prescriptions through signatory authorization.

Smart card

Smart card is a plastic card that is similar in size to the credit card or the ATM card. The difference being there is an additional IC chip on smart card. Besides memory function, this IC chip can compute and process data, in addition to statistical functions. Therefore, this card can store the personal information of the cardholder, such as, in terms of medicine and healthcare, identity, private key, certificate, e-prescriptions and various related personal diagnostic records; in paired with the system operation, it can even acquire calculating, integrated, and statistical functions [11, 22].

In order to make the smart card more appropriate for the proposed IMIS, for example, in arriving at medical information mobility, putting an end to illegal refills, price and quantity inflation of drugs, and other unfair medical resource distribution problems, we provide some design suggestions of the card contents. This means, we classify the data in the card into four levels according to their importance and confidentiality. The components, users, and users' permission will differ with the level classified as will be explained below.

(1) Confidentiality Level

This level stores the private key used by the cardholder to encrypt or sign. The materials of the storage devices in this level are ROM. Due to the property of ROM and the especial hardware protection, once the key is written, it will be impossible to alter or copy the key through other means. Even the cardholder will not be able to obtain it, ensuring the safety of the key.

(2) Security Level

This level stores patient medical records of recent visits, including e-prescription, EPRs, and personal diagnostic records. The number of records that can be stored depends on the size of the card memory. The storage method applies the First In First Out (FIFO) order serial, i.e. data will be added to the front end of the queue, while the data at the back end will be deleted. This way, once a new record is inputted, the earliest inputted data will be written over and deleted from the card. Thus, the storage components use EPROM, a type of memory chip that retains its data when its power supply is switched off.

When accessing the data from this level, both the physicians and the physicians' identity will have to be authenticated to confirm that the current access had been authorized by the patient, and at the same time record the identity of the physician seeing the patient.

As mentioned in Introduction section, the intention of writing patients' medical records into the IC card is to achieve healthcare mobility. As most medical records belong to the custody of medical institutes, even patients themselves will have to go through numerous procedures in order to obtain fragments of their own records, consuming time and human resources. Although many hospitals aim to develop into medical information systems, but for obtaining information, many still requires patients' application, supplemented by electronic signatures and numerous other authentication procedures, during which some procedures may require the patient to be present in person to complete the information exchange between departments and institutions. Thus, inputting medical records into the IC card realizes the goal of medical information mobility efficiency.

(3) Proxy Level

This level primarily endows the proposed IMIS the function of proxy prescription collection. Patients who are physically disabled, or cannot collect prescriptions in person can authorize agents to make the collections on their behalf. Therefore, the information stored here will be the serial numbers of uncollected prescriptions. The storage method utilizes the queue system with the characteristics of FIFO. The storage devices will be of EPROM.

(4) Open Level

The public key certificates for authenticating the patients' signatures will be stored in this level.

The proposed scheme

This section illustrates the proposed IMIS, including its structures, main entities, and executing procedures. Note that the IMIS integrates the use of EPRs and e-prescriptions, simplifying complicated and time consuming medical care procedures such as making diagnoses, confirming physical examination results, collecting prescriptions, making insurance claims, etc. Furthermore, cryptology such as encryption and decryption, and digital signatures is used to protect the privacy of patients and physicians to prevent the occurrence of illegal activities. In addition, in the event of disputes, they can be mediated by the TTP in the system by verifying the messages and signatures.

Overview

The procedure in the proposed scheme consists of four phases, registration phase, diagnosis phase, prescription collection phase, and subvention phase. The structure and operation process of the proposed IMIS is demonstrated as shown in Fig. 1.

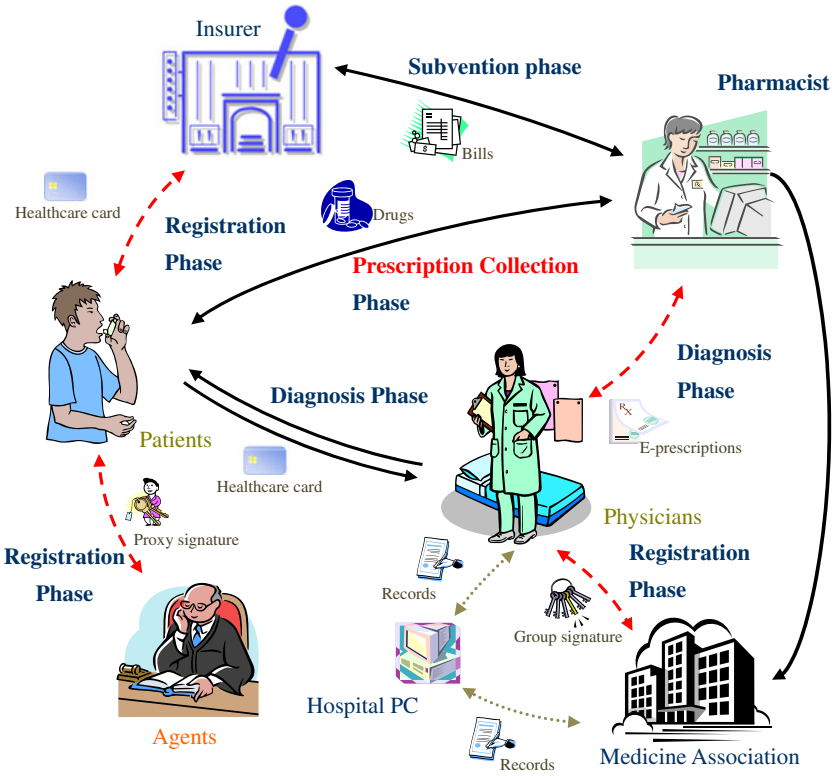

Fig. 1 Flowchart of the proposed IMIS

The main entities include insurer, medicine association, pharmacist, patients, physicians, and agents. Insurer, a trusted unit, is responsible for the national health insurance transactions, such as dispensing healthcare cards and medicine certificates to patients for consultations, assist in authenticating the eligibility of patients' agents, etc. In addition, it also handles drug subsidies and diagnoses and treatment subsidies. The medicine association, another trusted unit, is responsible for collecting, safekeeping, and renewing the national EPRs and e-prescriptions, allows each physician to use their group signature and certificate, and assists in mediating disputes between pharmacists, insurers, physicians, and patients. The pharmacist is responsible for authenticating e-prescriptions and verifying the correctness of the signatures, and thereafter, dispensing the drugs to the patients or agents. The patients, physicians, and agents, all play important roles in the proposed IMIS. The proposed architecture makes use of verification protocols for digital signatures and the recording of medical charts. These can not only be used to track the patients' history, but can be used to track suspicious or unusual events in order to enhance prevention of imposture and counterfeit. This also helps save medical resources from wastage, and cuts down on legal costs.

For protecting the privacy of patients and physicians, it is required for patients to register with the Insurer (IR) in the registration phase for a healthcare card with anonymity ability. As for the physicians, they are required to register with the Medicine Association (MA) to get a personal group signature private key that can fulfill the anonymity need by exploiting the characteristic of group signature. In addition, the IMIS assists in proxy prescription collections, so the private key of agent's signature will also be stored in the card.

In the diagnosis phase, when a patient holding his healthcare card visits a physician, the physician will first verify the signature of the patient to authenticate the patient is the cardholder. Following, the medical records registered with the institution will be accessed. If necessary, with verification, records of recent visits or relating records filed with the MA can also be accessed to assist the physician in understanding the patient's recent condition and treatments received.

After diagnosis, the physician will modify and update the patient's medical records and fill out the e-prescription for the patient to be collected from a pharmacy. All these actions require the physician's personal group signature key for signature, demonstrating his responsibility for the diagnosis made. In addition, the physician will input the diagnosis record and e-prescription data into the patient's healthcare card.

In the prescription collection phase, a patient holding his healthcare card visits the Pharmacist (PH) to collect his prescription in the pharmacy. The PH first verifies the data in the card with the data sent by the physician to authenticate the identity of the patient. If no error arises, the drugs will be dispensed to the patient, and a note will be

made about the collection. If the patient cannot collect in person, this will be collected by an authorized agent.

After the patient has collected the drugs and signed, signifying the end of his administrative procedures, the pharmacy can make the legible claims from the IR with the patient's or agent's signature, thereby completing all procedures between all parties involved in the medical care process, namely the patient and the physician, the physician and the medical institute, the medical institute and the pharmacy, and the pharmacy with the IR.

Registration phase

For protecting the privacy, the patient has to register with the IR for a healthcare card with anonymity function (i.e., being issued under a pseudonym other than the patient's true identity). Therefore, the patient makes a request R_P to the IR that includes details *Con*, and the public key PPK_P under which the pseudonym is used when making visits. Using the private key SK_P made under his real name, *Con* and PPK_P is signed on, and together with the key's certificate $Cert_P$, transmitted to the IR via a secure network channel. When the IR receives the R_P, it will use the patient's public key of real name PK_P involved in *Cert* to authenticate the correctness of the signature$Sig_{SK_P}(Con,\ PPK_P)$. If all is correct, a random pseudonym PID_P is chosen, with which the PPK_P sent by the patient, a signature of PPK_P signed by the IR, and the basic personal information *Infor*, forming the pseudonymous public key certificate $PCert_P$ for the patient, and is sent back to him along with the information *IR.Infor* related to the IR with its signature $Sig_{SK_I}(IR.Infor)$, thereby completing the process as shown by Eqs. 1 and 2.

$$\text{Patient (P)} \rightarrow \text{IR} \quad R_P = \{Con,\ PPK_P,\ Sig_{SK_P}(Con,\ PPK_P),\ Cert_P\} \tag{1}$$

$$\text{IR} \rightarrow \text{P} \quad PCert_P = \{PID_P,\ Infor,\ PPK_P,\ Sig_{SK_I}(PPK_P)\},\ IR.Infor,\ Sig_{SK_I}(IR.Infor) \tag{2}$$

In regard to protecting the privacy of physicians, the physicians need to register with the MA to obtain a personal group signature private key for signing. With the characteristics of group signature, other than the MA who can verify from the records with the signature to know which physician signed on the records, the rest can only use the group signature public key to verify its correctness and completeness, without knowing who signed on the record, fulfilling the anonymity need and protecting privacy. Thus, after the physician has signed with the private key SK_D made under his real name on his identity ID_D, the application request R_D is formed and sent via a secure network channel to the MA including the SK_D's certificate $Cert_D$. After the MA verifies the correctness of the signature, it will use the Master Key *MK* of the group signature to generate the physician's group signature private key K_D through the function F_{GK} by combining *MK* with ID_D and return the K_D back to the physician, completing the process for generating the signature key as shown by Eqs. 3 and 4.

$$\text{Physician (PC)} \rightarrow \text{MA} \quad R_D = \{ID_D,\ Sig_{SK_D}(ID_D),\ Cert_D\} \tag{3}$$

$$\text{MA} \rightarrow \text{PC} \quad F_{GK}(MK,\ ID_D) = K_D \tag{4}$$

Besides, because the IMIS posses the function of assisting in proxy prescription collections, when necessary, after the IR has verified the legality of the agent, between the patient and the agent, the patient's pseudonymous private key PSK_P and the agent's pseudonym PID_A can be used to generate the agent's signature private key PSK_A through the function F_A as demonstrated by Eq. 5. The Agent's primarily function is to provide patients with a convenient signature for use in the system environment, through which a patient's identity can be verified and their rights of access subsequently authorized. In Eq. 5, the PSK_A obtained through PSK_P and PID_A is one such signature that is used to execute the agent's role.

$$\text{P} \leftrightarrow \text{Agent (A)} \quad F_A(PSK_P,\ PID_A) = PSK_A \tag{5}$$

Diagnosis phase

In this phase, the patient will carry his owned healthcare card to make a visit to the hospital. The process will run as follows:

First, the patient registers with the front desk by using his PSK_P and signs on the stamp of the current time on computer *TS*. Following, he waits for his turn to see the physician. During the process, through the $PCert_P$ in the patient's card, physicians can verify the correctness of the signature $Sig_{PSK_P}(TS)$. Once the verification comes clean, and the identity of the patient is also verified, the patient's basic information, medical records with the institute, and recent medical records RC_S will be shown on the physician's monitor, making it easier for the physician to follow the patient's recent health condition. If there are additional needs, the physician can upon verification, access information $OtherRC_S$ of (as shown by the green line in Fig. 1) other institutes from the MA as shown by Eqs. 6 and 7.

$$\text{P} \rightarrow \text{PC} \quad TS,\ Sig_{PSK_P}(TS),\ PCert_P;\ RC_S \tag{6}$$

$$\text{MA} \rightarrow \text{PC} \quad OtherRC_S \tag{7}$$

After the physician has diagnosed the patient, the details of the diagnosis $NewRC_S$ will be added to the patient's medical

record, at the same time, used to update the patient's records stored with the institute and finally, together with the physician's group signature $Sig_{K_D}(NewRC_S)$, uploaded to the MA for integration with the patient's comprehensive medical records. In another matter, the physician fills out the e-prescription R_X to be followed for this visit, including the serial number R_X_ID and medication details MR_S. Similarly, the physician will sign with his K_D signifying his taking responsibility. All the information, together with the patient's $PCert_P$ will be sent to the pharmacy specified by the patient through encryption (E) by the PH's public key PK_{PH}. The patient's healthcare card is also updated to include the most recent diagnosis and treatment records with the corresponding R_X_ID to be used in prescription collection phase. Equations 8-10 demonstrates these steps.

$$\text{PC} \rightarrow \text{MA} \qquad NewRC_S,\ Sig_{K_D}(NewRC_S) \tag{8}$$

$$\text{PC} \rightarrow \text{PH} \qquad E_{PK_{PH}}(R_X,\ R_X\_ID, MR_S, Sig_{K_D}(R_X,\ R_X\_ID, MR_S),\ PCert_P) \tag{9}$$

$$\text{PC} \rightarrow \text{P} \qquad NewRC_S,\ R_X\_ID \tag{10}$$

Prescription collection phase

In this phase, the PH decrypts (D) using his personal private key SK_{PH} to obtain the patient's R_X, the serial number R_X_ID, the medication details MR_S, and their group signature $Sig_{K_D}(R_X,\ R_X\_ID, MR_S)$ signed by the physician. The correctness of them is thus verified (V) through the public key of the group signature PK_{GK} announced by the MA. The verification results will be saved to assist the MA in off-line mode should medical or financial disputes arise.

Next, the patient goes to the pharmacy with his owned healthcare card for collecting his medication. With the verification of the R_X_ID stored in the patient's card against the serial number sent by the physician, the PH can identify if it is the right person collecting the medication. If no error arises, the PH asks the patient to sign against the serial number, in turn becomes evidence for the pharmacy to make claims from the IR. Finally, the pharmacy dispenses the medication to the patient, and marks the R_X_ID as "collected," thus ending the whole process as demonstrated by Eqs. 11 and 12.

Furthermore, should the patient be physically disabled or cannot make it in person, an agent can collect the medication on his behalf as per regulations. From the above explanations, it is known that the agent can obtain the PSK_A for proxy prescription collections in the registration phase. Therefore, when the agent uses the PSK_A to sign $Sig_{PSK_A}(R_X\_ID)$ on to the R_X_ID, the medications can be collected from the pharmacy. The PH will use the PPK_P and PPK_{AoP} to restore the agent's PPK_A through function F_A to verify the correctness of signature signed on the R_X_ID. If no discrepancies arise, the signature will be retained as evidence against claims from the IR. The process is similar to the scenario where the patient collects the medication personally, as demonstrated by Eqs. 13 and 14.

$$\text{PH} \leftrightarrow \text{MA} \qquad D_{SK_{PH}}(E_{PK_{PH}}(Sig_{K_D}(R_X,\ R_X\_ID, MR_S))),\ V_{PK_{GK}}(Sig_{K_D}(R_X,\ R_X\_ID, MR_S)) \stackrel{?}{=} R_X,\ R_X\_ID, MR_S \tag{11}$$

$$\text{P} \rightarrow \text{PH} \qquad Card(R_X\_ID) \stackrel{?}{=} R_X\_ID,\ Sig_{PSK_P}(R_X\_ID) \tag{12}$$

$$\text{A} \rightarrow \text{PH} \qquad Sig_{PSK_A}(R_X\_ID) \tag{13}$$

$$\text{A} \leftrightarrow \text{PH} \qquad PPK_A = F_A(PPK_P, PPK_{AoP}),\ V_{PPK_A}(Sig_{PSK_A}(R_X\_ID)) \stackrel{?}{=} R_X\_ID \tag{14}$$

Subvention phase

When the PH makes claims from the IR for the subsidies made, two signatures have to be provided. The first being the physician's group signature $Sig_{K_D}(R_X,\ R_X\_ID, MR_S)$, the second being the patient's or his agent's signature on the e-prescription number $Sig_{PSK_P}(R_X\_ID)$ or $Sig_{PSK_A}(R_X\_ID)$. This way, it can be proved that the patient's treatment was administered by a certain physician, and the medication had also been collected. With these two signatures and the PPK_P or PPK_{AoP} and other supporting documents, using the IR's public key PK_I, the claims and the supporting documents are encrypted and sent to the IR.

When the IR receives the package, it is decrypted with the IR's private key SK_I and the contents are verified against the signatures obtained to verify for correctness and completeness. If all goes correct, an electronic payment receipt EP is issued with its signature $Sig_{SK_I}(EP)$ to the PH to collect the claims, as demonstrated by Eqs. 15 and 16.

$$\text{PH} \rightarrow \text{IR} \qquad E_{PK_I}(R_X, R_X\_ID, MR_S, Sig_{K_D}(R_X, R_X\_ID, MR_S), Sig_{PPK_P}(R_X\_ID), PPK_P) \text{ or } E_{PK_I}(R_X, R_X\_ID, MR_S, Sig_{K_D}(R_X, R_X\_ID, MR_S), Sig_{PPK_A}(R_X\_ID), PPK_P, PPK_{AoP}) \tag{15}$$

$$\text{IR} \rightarrow \text{PH} \qquad EP,\ Sig_{SK_I}(EP) \tag{16}$$

Security analysis

To confirm that the proposed IMIS is complete, convenient and secure, it shall be demonstrated to achieve the following properties: mobility of medical records, function of proxy prescription collection, protection of linkability and privacy, and avoidance of dispensing and prescribing wrong medication, profiteering, and conspiracy problems. We will analyze each in detail and show how the proposed system satisfies them as follows.

Mobility of medicine records

As development of mobile devices for the use of medicine, such as smart cards, cell phones, and PDA continues to advance, under the constant advancements in storage space, computational ability, or memory size, it is only a matter of time before medical records achieves mobility. Assume that healthcare cards are designed according to the details mentioned in Smart card section, it will not only have the ability to sign, encrypt and decrypt, but also enable the storage of related medical records safely in the card, and with the portability of the card, exhibit mobility of information. Even though the present healthcare systems have yet to adopt such healthcare cards, under the present systems, complex authentication procedures have to be passed in order to obtain medical records. However, when e-medicine, including e-medical system, EPRs, and e-prescriptions, become increasingly common, healthcare cards similar to what we proposed will undoubtedly be used to enable medical information mobility.

Since wireless transmission takes place in a public network, it is not possible to predict attacks. However, as the proposed architecture is to be used in the premises of a hospital, all wireless base stations are equipped with encryption function, such as: the WPA. The proposed method can also be integrated with the user's ID and the signature given by the MA to authorize use of the wireless equipment. This also helps the management to monitor the network, such that unauthorized users are barred from access to confidential data, preventing further rise in medical costs and other legal problems.

Function of proxy prescription collection

This function bestows to patients greater convenience in collecting medications, especially to those physically disabled, by allowing them to authorize agents to collect them on their behalf, ensuring that the medications are not lost or fraudulently collected by malicious parties. Completely digitized medical systems in the future will not permit the current method of proxy collections, simply by obtaining the e-prescription prescribed by the physicians and handing them over the pharmacy's counter. In order to prevent malicious parties from hacking and stealing or modifying the e-prescriptions from the network environment, providing a safe method for proxy prescription collection is an important issue. In the proposed IMIS, the proxy signature is employed to authorize agents and the TTP, so that agents enables to sign e-prescriptions, to collect medications, and to offer legal signatures with verifiability, integration, unforgeability, and undeniability, and the TTP can verify the legitimate of the collector. This function guarantees that patients and agents can collect the medications safely and surely, and bestows upon e-medicine systems the ability of permitting proxy prescription collections.

Protection of privacy

In terms of protection of privacy, the proposed IMIS uses pseudonym for patients and group signature for physicians against the linkability related to privacy, including anonymity, linkability of patients, linkability of physicians, and non-linkability of physicians.

For anonymity, the use of pseudonym provided by the IR would ensure that no patient's real name is revealed. This way, not only will the patient's privacy of medical data be safeguarded, but at the same time, it can unselfishly help contribute to science by offering the data for scientific research in the search for better treatment and medication.

For linkability of patients, since the pseudonym of patients are given by the IR, only the unit can recognize the relationship between patients' true identities and the pseudonyms issued. (Other than the physicians seeing the patient), no one can know of the patients' real identities. At the same time, the PHs can only distinguish e-prescriptions for the same patient. Therefore, the proposed IMIS satisfies the definition of linkability of patients.

For linkability of physicians, because the IMIS employs the use of group signature, allowing the fair MA to track down the real identity of physician from the physician' signature, other units can only verify if the signature is legal, but cannot know of the real identity of the signer. Under these circumstances, the PH will also be unable to know from the contents of e-prescriptions, of the physician who prescribed them, achieving the requirement of non-linkability of physicians.

Avoidance of making wrong prescriptions, profiteering, and conspiracy problems

To avoid these problems such as handing out wrong prescriptions, profiteering, and conspiracy problems that can occur between pharmacies, IRs, physicians, and

patients, our proposal would rely on the off-line MA to mediate these likely differences as follows:

(1) Assist in solving the problem of making wrong prescriptions:

For physicians, it is not unlikely to prescribe an inappropriate medication. If the patient takes the medication without knowledge, tragedies may occur. Therefore, to prevent such scenarios, when the pharmacist finds abnormality in the list of medicine prescribed, such as medication that are not appropriate to be taken, or should not be taken together, the pharmacist can contact the off-line MA for help as to why such medication were prescribed.

(2) Assist in solving the problem of expensive medication:

For physicians aiming to profit, prescribing series of expensive medication is not uncommon. For IRs, this means covering substantial amount of medication expenses. Therefore, when the IRs are unsure about the claims made by certain hospitals and clinics, they can raise reasonable doubts with the off-line MA and request for investigations on the series of expensive prescriptions.

(3) Assist in investigating frequency of visits made by patients:

Physicians and patients may conspire to profit illegally. For example, if a patient who is not sick nonetheless visits the hospitals, on one hand he can collect the medication that have been subsidized, and on the other, the physicians can earn fees for the diagnoses made. Thus, if the IRs find that a patient's visits for medical care is too frequent, they can request the off-line MA for investigation to see if the patient really needed medical care, or is bent on wasting medical resource.

The above-mentioned problems are connected with the physician. Therefore, the off-line MA can trace the physician responsible simply by looking up the group signature signed. Using function F_{GK_T}, and Trace Key TK, the MA can trace the group signature $Sig_{K_D}(\cdot)$signed by the physician and match the data with the stored information in the database containing list of physicians' key and their real identities. From this, the physician who signed the prescription will be made known, and the MA can arrange the physician for questioning by the pharmacy or IRs, thus assisting in solving possible disputes. This is demonstrated by Eq. 17.

$$\text{MA} \quad F_{GK\_T}(Sig_{K_D}(\cdot),\ TK) = K_D \qquad K_D \leftrightarrow ID_D \tag{17}$$

Overall performance result

In this case, based on SOA and web services, this study utilizes HL7 as the exchange platform for heterogeneous systems. For solving the issues in medical information systems, the characteristics of service are defined as (1) connection and communication among heterogeneous systems, (2) applicability and scalability, and (3) fault tolerance. According to these characteristics, the service groups under the structure of SOA HIS are designed to achieve the characteristics. In addition to HL7-based SOA HIS structure, Taiwan University Hospital, which faces the same issue as above, is introduced in this study for the empirical research. It aims to prove the feasibility and the application value of the proposed system. Moreover, the efficacy of the SOA HIS structure is computed so that the HL7Central service groups can largely enhance the weekly reaction time in outpatient, inpatient, and emergency. The design and the development of the integrated medical information system are regarded as the major contributions, as it could solve the problems in academic research on medical information systems and actual applications as well as reach the objectives. What is more, electronic patient records can also be introduced to the structure. The proposed integrated medical information system should offer the reference for future development of medical information systems.

Conclusions

With the combination of hardware and software devices, the proposed IMIS realizes the following aims, making the EPRs exchangeable between medical departments and institutions, integrating the e-prescriptions with the medical system, and well protecting physicians' and patients' privacy. These hardware devices consist of the EPRs, e-prescriptions, healthcare cards, and the software technologies includes proxy signatures and group signatures. Not only are the originally complex and time-consuming administrative procedures simplified, but it also satisfies the mobility of medical records, provides the function of proxy prescription collection, protection of privacy, and the avoidance of making wrong prescriptions, profiteering, and conspiracy problems. In the current trend where e-medicine is receiving attention by the day, we believe this system is secure, efficient, and worth implementing in medical application environments.

Acknowledgement This work was supported partially by National Science Council of Republic of China under Grants NSC 100-2410-H-029-007.

References

1. Ateniese, G., Cutmola, R., de Meideiros, B., and Davis, D., *Medical Information Privacy Assurance: Cryptographic and System Aspects, Third Conference on Security in Communication Networks*. Amalfi, Italy, pp. 199–218, 2002.
2. Ball, E., Chadwick, D. W., and Mundy, D., Patient Privacy in Electronic Prescription Transfer. *IEEE Security & Privacy Magazine* 1(2):77–80, 2003.
3. Chaum, D., and Heyst, E. van, "Group signatures," *In proceedings of Advances in Cryptology - Eurocrypt 1991*, Vol. 547 of LNCS, pp. 257–265, Springer-Verlag, 1991.
4. Chan, A. T. S., Cao, J., Chan, H., and Young, G., A Web-Enabled Framework for Smart Card Application in Health Services. *Communications of the ACM* 44(9):77–82, 2001.
5. Chen, C.-L., Chen, Y.-Y., and Chen, Y.-H., "Group-based Authentication to Protect Digital Content for Business Applications", International Journal of Innovative Computing. *Information and Control* 5(5):1243–1251, 2009.
6. Cao, F., and Cao, Z., A secure identity-based proxy multi-signature scheme. *Information Sciences* 179(3):292–302, 2009.
7. Diffie, W., and Hellman, M., New directions in cryptology. *IEEE Transaction on Information Theory* 22(6):644–654, 1976.
8. Dolin, R. H., Rishel, W., Biron, P. V., Spinosa, J., and Mattison, J. E., "SGML and XML as Interchange Formats for HL7 Messages," *Journal of the American Medical Informatics Association*, 720–724, 1998.
9. Dolin, R. H., Alschuler, L., Beebe, C., Biron, P. V., Boyer, S. L., Essin, D., Kimber, E., Lincoln, T., and Mattison, J. E., "The HL7 Clinical Document Architecture," *Journal of the American Medical Informatics Association* 8(6):552–569, 2001.
10. ElGamal, T., A Public Key Cryptosystem and Signature Scheme based on Discrete Logarithms. *IEEE Transactions on Information* 31(4):469–472, 1985.
11. Guthery, S. B., and Jurgensen, T. M., "SmartCard Developer's Kit, Macmillan Technical Publishing," ISBN 1-57870-027-2, available at http://www.scdk.com, 1998.
12. Gritzalis, S., Lambrinoudakis, C., Lekkas, D., and Deftereos, S., Technicl Guidelines for Enhancing Privacy and Data Protection in Modern Electronic Medical Environments. *IEEE Transactions on Information Technology in Biomedicine* 9(3):413–423, 2005.
13. Huston, T., "Security Issues for Implementation of E-Medical Records," *Communications of the ACM* 44(9):89–94, 2001.
14. Hsu, C.-C., and Ho, C.-S., A new hybrid case-based architecture for medical diagnosis. *Information Sciences* 166(1–4):231–247, 2004.
15. Hong, X., Efficient threshold proxy signature protocol for mobile agents. *Information Sciences* 179(24):4243–4248, 2009.
16. Huang, K.-H., Hsieh, S.-H., Chang, Y.-J., Lai, F., Hsieh, S.-L., and Lee, H.-H., Application of portable CDA for secure clinical-document exchange. *Journal of Medical Systems* 34 (4):531–539, 2010.
17. Jones, D., "Smart cards for the people," *Card Technology Today* 15(3):16–16(1), 2003.
18. Le, X. H., Lee, S., Lee, Y.-K., Lee, H., Khalid, M., and Sankar, R., Activity-oriented access control to ubiquitous hospital information and services. *Information Sciences* 180(16):2979–2990, 2010.
19. Mambo, M., Usnda, K., and Okamoto, E., "Proxy signatures: Delegation of the power to sign message". *IEICE transactions on fundamentals of electronics, communications and computer sciences* E79-A(9):1338–1354, 1996.
20. National Institute of Standards and Technology, "Digital signature standard," Technical report, 1994.
21. Rivest, R. L., Shamir, A., and Adleman, L., A method for obtaining digital signatures and public-key cryptosystems. *Communications of the ACM* 21(2):120–126, 1978.
22. Rankl, W., and Effing, W., "Smart Card Handbook," John Wiley & Sons, ISBN 0-471-96720-3, 1997.
23. Rash, M.C., "Privacy Concerns Hinder Electronic Medical Records," *The Business Journal of the Greater Triad Area*, 2005.
24. Stallings, W., "Cryptography and network security: principal and practices," Prentice Hall, 4th Edition, 2005.
25. Takeda, H., Matsumura, Y., and Kuwata, S., Architecture for networked electronic patient record systems. *International Journal of Medical Informatics* 60(2):161–167, 2000.
26. Tsumoto, S., Mining diagnostic rules from clinical databases using routh sets and medical diagnostic model. *Information Sciences* 162(2):65–80, 2004.
27. Um, K. S., Kwak, Y. S., Cho, H., and Kim, I. K., Development of an HL7 interface engine, based on tree structure and streaming algorithm, for large-size messages which include image data. *Computer Methods and Programs in Biomedicine* 80:126–140, 2005.
28. Ulieru, M., Hadzic, M., and Chang, E., Soft computing agents for e-Health in application to the research and control of unknown diseases. *Information Sciences* 176(9):1190–1214, 2006.
29. Wang, D.W., Liu, D.R., and Chen, Y.C., "A Mechanism to Verify the Integrity of Computer-Based Patient Records," *The Journal of China Association for Medical Informatics* 10:71–84, 1999.
30. Yang, Y., Han, X., Bao, F., and Deng, R. H., A Smart-Card-Enabled Privacy Preserving E-Prescription System. *IEEE Transactions on Information Technology in Biomedicine* 8 (1):47–58, 2004.
31. Yee, G., Korba, L., and Song, R., "Ensuring Privacy for E-Health Services," *In Proceedings of the First International Conference on Availability, Reliability and Security*, pp. 20–22 Apr. 2006, Vienna University of Technology, Austria, 2006.