On the Security Policy and Privacy Protection in Electronic Health Information System

Hsuan-Yu Chen[1], Yao-Min Huang[2], Zhen-Yu Wu[3(✉)], and Yin-Tzu Huang[4]

[1] Department of Radiology, Tri-Service General Hospital, National Defense Medical Center, Taipei, Taiwan
[2] Department of Management Sciences, National Chiao Tung University, Hsinchu, Taiwan
[3] Department of Information Management, National Penghu University of Science and Technology, Penghu, Taiwan
zywu@gms.npu.edu.tw
[4] Department of Electrical Engineering, National Taiwan University, Taipei, Taiwan

Abstract. The integration of information technology and medical techniques could benefit expanding the time and location for medical services as well as provide better medical quality that it has become a trend in medical domain. For this reason, this study proposes to develop an integrated healthcare information system. Furthermore, based on user privacy and system information security, the key in a smart national health insurance card or a patient's fingerprint together with a doctor's group signature and public key are utilized for retrieving electronic medical records from the system so as to protect the confidential information in the system and guarantee patients' privacy. This system covers other relevant functions of medical record mobility, data link, information security protection, and drug conflict avoidance. In the integrated healthcare information system, a patient's privacy could be protected through hiding. The retrieval location of medical records is always the same that doctors from different hospitals could access to the medical records through authorization. When dealing with an urgent case, the real-time medical record retrieval could effectively enhance the recovery rate. The information in the system procedure broadly covers diagnoses of patients, insurance claims, and drug collection in order to prevent doctors from prescribing wrong medicine, avoid the troublesome of insurance claim application, and reduce patients' problem about collecting receipts.

Keywords: Healthcare information system · Group signature · Electronic medical records · Privacy · Protection

1 Introduction

For several years of network development, the application has become complicated and the relevant technology is getting diversified. Digitalization in daily life has become a major trend in modern technology development. Common e-commerce, e-medical treatment, e-banking, g-government, and online community application are the applications of network.

X. Wang et al. (Eds.): 6GN 2020, LNICST 337, pp. 439–444, 2020.
https://doi.org/10.1007/978-3-030-63941-9_34

Relative to medical application, the meaning of information technology lies in expanding the clinical facilitating function of medical information. The technology covers health insurance IC card device, digital certificate and signature, electronic medical records, and electronic prescriptions [1, 5]. The introduction of information technology to medical systems presents obvious performance on medical management. However, the development and maintenance costs for medical information systems is large that it is simply tried in large medical centers, e.g. National Taiwan University Hospital, Veterans General Hospital, and Chang Guang Medical Foundation, in the beginning of the development. Besides, it is merely one-way information feed-in, rather than interactive information feedback, such as assisting medical personnel in teaching, inquiry, aid, and alert with built-in professional medical knowledge. After the practice of national health insurance in 1995, novel and mature system development technology has been emerging to cope with frequently changing health insurance payment reporting and accelerate the application of medical information to small and medium medical institutions. With the application of new technology, the development of programs becomes faster, more flexible, and more easily maintained. After the provision with direct operation and application for doctors, medical information systems are developed the comprehensive function to avoid the delivery of manual document, acquire real-time revision of users' feed-in information, maintain the timeliness of information in database, and get rid of the time difference in information update in traditional batch processing. It therefore could reduce and even avoid possible human errors of nurses, pharmacists, and technicians. An information system is also an inevitable infrastructure in medical management for the improvement of medical quality.

Research on the data structure of health insurance IC cards and digital certificates, electronic medical records, and the data format of electronic prescriptions is mature. However, the integration of cross-medical institution electronic medical record format, cross-department secure patient record information exchange agreement [2], telemedicine, and caregiver authentication mechanisms still require improvement. These are research on cross-medical institution electronic medical record format exchange agreement and medical information system transfer format.

The reinforcement and integration of medical information systems could assist in the promotion of medical quality and efficiency, where the integration of function and technology is the key to implement medical informatization.

First, reinforce the function of health insurance IC cards and the compatibility with integrated medical information systems. The generally used health insurance IC cards are wafer cards with small memory capacity, bad computing function, and not being able to support digital signature or encryption/decryption requirements in actual applications that it is not convenient for the verification and acquisition of electronic medical records, prescriptions, and examination forms. The selection of the saving medium of a health insurance IC card and the wafer material, e.g. ROM, RAM, or EPROM, should be carefully considered and matched the system according to the characteristics. Furthermore, the built-in data could be graded according to the importance of data or segmented the necessity according to emergency use. The reading and security mechanism of built-in data should be well planned and designed in advance.

Second, establish electronic prescription system with complete functions and the integration with medical information systems. As the rapid development of electronic medical records, prescriptions are inclining to electronic [3]. In terms of current medical systems and health insurance systems, the assistance of digital signature allows pharmacies and patients verifying the correctness, integrity, and non-repudiation of electronic prescriptions; meanwhile, pharmacies could complete the health insurance payment reporting through online verification mechanisms. It could enhance the integrity of medical information networks and is worth of development in the future.

Third, protect patients' and doctors' privacy. Confidentiality in medical practice is the basic element to establish good doctor-patient relationship. Patients have the right to request the confidentiality of personal medical information and doctors have the obligation to respect patients' medical privacy. In the essence of law, privacy is a limited right which is passively restricted to balancing the conflict among public health benefits, third party benefits, and personal privacy benefits [4]. Moreover, under current medical system with referral, consultation, and health insurance IC cards, medical division and medical teams are the trend as well as the major challenge to maintain patients' privacy. In this case, authorized access of patients' medical records could implement the protection of both doctors' and patients' privacy.

An integrated medical information system should be a secure, convenient, and complete system with following characteristics.

1.1 Portability of Recent Medical Records

A patient's recent medical records are logged in the health insurance IC card. With authentication, a doctor could read the patients' medical information in other medical institutions and rapidly access the patient's medical history to promptly make correct diagnoses. It would enhance doctors' diagnosis correctness and efficiency.

1.2 Medicine Collection Function

The function stresses on the convenience for patients collecting medicine. An agent's identity and authentication information are integrated with the medical information system and registered in the patient's health insurance IC card. When the patient is not able or busy to collect medicine by himself/herself, especially the one with physical & mental disabilities or with difficulty in moving, could entrust a legal agent, through authority mechanism, to collect medicine.

1.3 Linkability and Privacy Protection

In the digital medical system, patients' and doctors' medical privacy is extremely emphasized. In the beginning of the system development, the following points should be drawn.

Anonymity: Patients and doctors use pseudonyms in an integrated medical information system.

Patient identity linkability: Merely the health insurance reporting unit could access a patient's real identity. Pharmacies' linkability to patient identity is simply the holder of electronic prescriptions, but not the real identity.

Doctor identity linkability: Merely specific just medical associations could grasp a doctor's real identity. The linkability of Bureau of National Health Insurance to doctor identity is simply the prescription writer, but not the real identity.

Non-linkability of doctor identity: Pharmacies could not link a doctor's identity from electronic prescriptions.

1.4 Avoiding Patients' Repeated Medicine Collection

After the comprehensively electronic health science and technology, the access to electronic prescriptions might be easier than to written prescriptions. To avoid a patient repeatedly collecting medicine in different pharmacies with the copy of electronic prescriptions to result in medical resource waste, a healthy integrated medical information system should present the function to prevent such similar behaviors.

2 Research Method

The proposed Integrated Medical Information System (IMIS), including the architecture, physical mechanism, and execution process, are introduced in this section. IMIS integrates e-patient records and e-prescriptions to simplify the originally complicated and time-consuming medical process, e.g. diagnosis, inspection, medicine collection, emergency, and insurance payment. It even applies cryptography, e.g. encryption/decryption and digital signatures, to protect patients' and doctors' privacy, and prevent illegal benefit acquisition. Besides, when there are medical malpractice claims, the just third party in the system would inspect the message and signature to calm the dispute.

The architecture and operation process of IMIS are shown in Fig. 1. The entire mechanism could be divided into registration phase, diagnosis phase, collecting medicine phase, and subvention phase. The physical mechanism contains insurers, Bureau of National Health Insurance, pharmacies, patients, doctors, and agents. Bureau of National Health Insurance is responsible for national medical businesses, covering from doctors to patients' medicine collection. A patient is first offered a national health insurance IC card used for medical institutions; doctors and pharmacies are provided consultation and medicine authentication, including collecting, storing, and updating patients' electronic medical records and prescriptions; and, an agent is verified the qualification to collect medicine. What is more, it is also responsible for subsidizing medical expenses and partial or full diagnosis and treatment expenses of patients, issuing group signature and certificate for doctors diagnosing and treating patients, as well as assisting in possible medical malpractice claims among pharmacies, insurer, doctors, and patients. A pharmacy is responsible for verifying prescriptions and the correctness of signature in prescriptions as well as provides medicine for patients or agents. Patients, doctors, and agents play primary roles in IMIS.

Based on protecting patients' and doctors' privacy, a patient, at registration phase, should apply for an anonymous national health insurance IC card from Bureau of

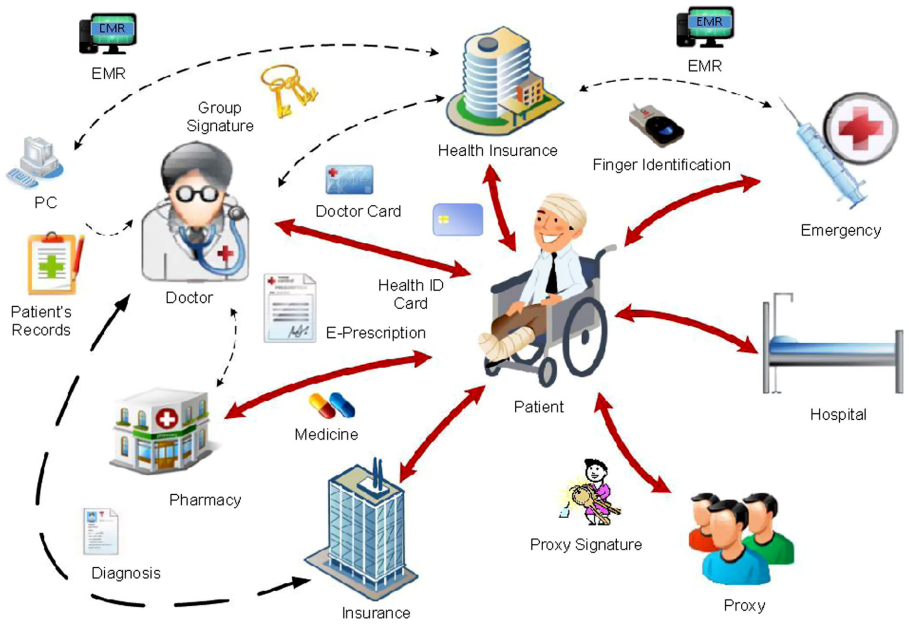

Fig. 1. IMIS process

National Health Insurance (NHI), while a doctor needs to apply for personal group signature secret key and doctor card. The characteristic of group signature could satisfy the requirement for anonymity. Besides, there is the function in IMIS of an agent collecting medicine for patients; the proxy signature secret key would be saved in the card.

At diagnosis phase, when a patient sees a doctor with the national health insurance IC card, the doctor would first insert the doctor card and the national health insurance IC card to the machine and transmit the patient data to Bureau of National Health Insurance for authenticating the patient's signature. When the patient is confirmed as the card holder, the patient's basic data, medical records, and recent diagnosis records would be displayed on the doctor's computer screen to help the doctor understand the patient's physical conditions and outpatient situations.

After the outpatient, the doctor would update the patient's medical record data and fill in prescriptions for the patient collecting medicine in a pharmacy. Such motions require the doctor using the personal group secret key for the signature to be responsible for the diagnosis. Moreover, the doctor would write the diagnosis records and prescription data in the patient's national health insurance IC card.

When a patient needs to apply for insurance, he/she could simply asks the doctor transferring the diagnosis content into a diagnosis certificate with the doctor's group secret key signature. The certificate is then transmitted to the insurer to complete the integration of insurance and medical treatment.

When an unconscious patient is delivered to the emergency, the patient's fingerprint is first collected in order not to postpone the treatment because of collecting or understanding the patient's physical conditions. The doctor then transmits the doctor card and the patient's fingerprint data to Bureau of National Health Insurance to acquire the patient's medical record data. After Bureau of National Health Insurance confirms the patient with the fingerprint data, the patient's basic data, recent diagnosis records, and medical records would be displayed on the doctor's computer screen. After the patient is out of danger, he/she would be transferred to other department and sickroom, and the rest process is the same as the outpatient clinic.

In the medicine collection phase, a patient would pick up medicine in a pharmacy (PH) with the national health insurance IC card. The pharmacist would first compared the data with the data transmitted from the doctor to authenticate the patient's identity. Without any mistakes, the medicine is given to the patient and the card is marked medicine collected. When a patient is not convenient or free to collect medicine, an authorized agent could collect the medicine.

After completing medicine collection and signature recognition, a pharmacy could apply for medicine subvention from Bureau of National Health Insurance with the patient's or the agent's signature. According to the insurance conditions, a patient could apply for claims from the insurer to complete the medical process composed of patients and doctors, doctors and hospitals, hospitals and pharmacies, as well as insurance companies and patients.

3 Conclusion

A integrated medical information system with security policy and privacy protection, which combines e-patient records, e-prescriptions, modified smart cards, and fingerprint identification systems and applies proxy signature and group signature, is proposed in this study.

References

1. Dai, C.-y.: Secure Access Control of Personal Health Records in Cloud Computing Using Attribute-Based Encryption. Department of Information Science and Engineering, National Chiao Tung University, Hsinchu City (2013)
2. Huang, K.-H., Hsieh, S.-H., Chang, Y.-J., Lai, F., Hsieh, S.-L., Lee, H.-H.: Application of portable CDA for secure clinical-document exchange. J. Med. Syst. **34**(4), 531–539 (2010)
3. Yang, Y., Han, X., Bao, F., Deng, R.H.: A Smart-card-enabled privacy preserving E-prescription system. IEEE Trans. Inf. Technol. Biomed. **8**(1), 47–58 (2004)
4. Stallings, W.: Cryptography and Network Security: Principal and Practices, 7th edn. Prentice Hall, Boston (2016)
5. Takeda, H., Matsumura, Y., Kuwata, S.: Architecture for networked electronic medical record systems. Int. J. Med. Inform. **60**(2), 161–167 (2000)