Protocols For Health Insurance System

G. V. Ramesh Babu[1] ,Dr. M. Padmavathamma[2]
1. Assistant Professor,2.Research Supervisor and Head, Department of Computer Science
1,2 S.V.College of CM&CS,S.V.University,Tirupati

Abstract

Health insurance companies (HIC) should provide health services to their customers in an efficient and secure way. Insurance companies are using modern technologies of IT to provide service to customers through E-Health Insurance, which is an Internet-enabled health insurance applications involving management of Customers data electronically. Due to the ease of global access to the information systems, privacy and security is becoming a major concern in the e-health insurance systems. To achieve above criteria we have proposed protocols for Health Insurance System (HIS) which provides the services to Customers in Secure manner in two phases. In each phase we propose protocols for secure communication. Phase - I consists of a)Client Registration service i.e., between Client (C) and Insurance Company(IC) b) Insurance Company Verification (Client data) and Health Card Generation service . In Phase-II we propose protocols between Insurance Company and Client for verification of health records and between Hospital (H) and Insurance company to ensure payment securely by using Expert Security Service.

1. Introduction

Group practice prepaid health care plans have been shown to operate in a business like way and to deliver high quality health care at lower costs. The number of people in developing countries in India covered by such plans, however, is very small. A well-formulated and well-managed Health insurance services could provide a comprehensive financial assistance. Generally a) Insurance companies negotiate rates with health care providers to provide financial coverage to clients. b) It shields you from unexpected medical costs – Even if your health plan requires you to pay certain costs out of pocket, being covered can help, save you from bankruptcy in case of injury or hospitalization. c) It shields your business from personal medical costs – As a self-employed person or small business owner, unexpected personal medical expenses can cripple your business. By limiting your personal liability for medical costs, health insurance can help keep your business afloat.

Securing confidential patient data is more important than ever – and it requires more than good intentions. It demands a comprehensive security solution built around strong encryption, robust identity management, and policy-based data management. This is especially true as hospitals and healthcare providers, insurers, pharmaceutical companies and others grow their ranks of mobile workers who carry or remotely access personally identifiable health information and R&D data. Data centres should maintain Client's data at Insurance offices should follow HIPAA Privacy Rule and the HIPAA Security Rule.

According to HIPAA the Privacy Rule protects all individually identifiable protected health information (PHI) maintained by the Covered Entity. It is not specific to electronic information and applies equally to written records, telephone conversations, etc. According to the Department of Health and Human Services, PHI includes data that relates to:

- the individual's past, present or future physical or mental health or condition or
- the provision of health care to the individual or
- the past, present, or future payment for the provision of health care to the individual

According to HIPAA Security Rule the security of *electronic* protected health information (ePHI). It prescribes a number of required policies, procedures and reporting mechanisms that must be in place for all information systems that process ePHI within the Covered Entity. It also prescribes a number of required and addressable implementation specifications designed to protect the confidentiality, integrity and availability of ePHI within the enterprise. These specifications fall into five categories:

- Administrative Safeguards
- Physical Safeguards
- Technical Safeguards
- Organizational Requirements
- Policies and Procedures

Health Insurance System protocols should be well designed to meet requirements stated below to to provide security, to a)access PIN b) digital certificates c)read/write by smart card readers d)access to basic patient's data e)access to health insurance data f)submission of data g) exchange of data g)Payment Billing and insurance.

- Have strong measures protecting confidentiality of the medical information they contain. (*Requirement* I)[6-9]
- Prove the validity and accuracy of the HER so as to be able to protect the patient's rights. (*Requirement* II) [6-9]
- Contain measures for the selective protection of privacy that allow for consultations with a trusted third party (TTP) on related medical information inquiries[6-9].*Requirement* III.

For ensuring security for clients data in Health Insurance premises we formulated a model and set of protocols to exchange of data between client and Insurance agents/office servers. Hospitals and health systems like insurance companies take measures for protecting the security of patient health information; yet, data breaches remain common in the industry. Health insurance companies must take following steps make data security a priority. 1. Conduct a HIPAA risk analysis 2.Implement encryption for all data as recommended by the AMA.3). Choose the highest level of encryption without the lag.4)Secure laptop data with encrypted portable storage devices.5) Make sure you have disaster recovery and business continuity plan.

2. Literature Survey

Insurance Companies must deliver cost effective, quality health care to its members as well as address the key administrative and clinical issues. To do this, Insurance and hospital managements relies heavily on its IS/IT (Information Systems/Information Technology), in particular. MARS (medical automated record system).Smart Cards are efficient for security for authentication [1]. In 1996, the Health Insurance Portability and Accountability Act (HIPAA) offered some general guidelines to enforce the protection of private medical information. One such guideline stated that patients must be able to view and obtain copies of their records, and request amendments to confirm they have the right of accessing their medical records to understand and monitor their health status and the process of diagnosis and therapy [2].

Bhatti et al. [3] proposed a policy-based system to address the following requirements: 1) the integration of privacy and disclosure policies with well-known healthcare standards used in the industry for the purpose of producing precise requirements of a practical healthcare system, and 2) the provision of ubiquitous healthcare services to patients using the same infrastructure that can enable federated healthcare management for organizations. More specifically, the disclosure and privacy policies have been designed by making use of requirements specification based on a set of use cases for the Clinical Document Architecture (CDA) standard. Also, a context-aware policy specification language has been proposed, which allows encoding CDA-based requirements use cases into privacy and disclosure policy rules. Unfortunately, the HIPAA security regulations are not covered in this framework.

Consequently, Health Insurance System should use modern technologies and must ensure quality information via Internet[5]:
1) *Cost savings*: the provision of detailed, structured and extensive information to the insurant aims at avoiding costs for highly individual, time-consuming consultation. Therefore providing information by websites is cheaper than providing telephone-based customer services or individual services in a local agency.

(2) *Competitiveness*: as the fee for health insurances in Germany was harmonized to a uniform level, sickness funds need other major differentiating factors from their competitors than costs. One possibility that can also be found as a major differentiating factor in other industries is “quality of services”. Consequently, information services provided by electronic means with a wide availability and a certain quality level could be a factor that distinguishes high-quality from low-quality from the point of view of insurant.

The private insurance system is based on an individual agreement between the insurance company and the customer. The fee depends on a range of individual characteristics, for example, the percentage of coverage, the amount of chosen services, the individual risk or the entrance age into the private system, and so forth.

3. Proposed Health Insurance System (HIS)

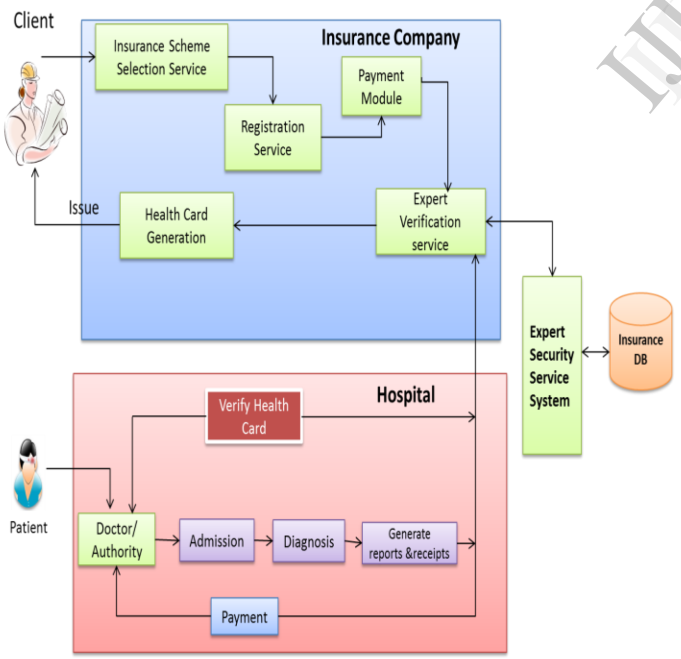

Figure-1 Health Insurance System

To address the above issues we are proposing new Health Insurance System(HIS) model shown in figure-1 which allows to store clients data in Smart E-Health-Insurance Card (SEHIC) which is given to clients by Health Insurance companies in turn used by hospital to access patients data. HIS provides Expert services to advice clients regarding insurance schemes selection (Decision Support system),verify and secure patients data. In this model SEHIC contains clients data like finger prints, photo and personnel data is encrypted by using PKI, Digital Image encryption techniques. SEHIS model verifies counterfeit documents, if any of the client to use insurance facility, or an insured person and a physician may deviate from insurance company rules to get benefits illegally etc. In our proposed model SEHIS will benefit insurance companies, patients and works accordance with HIPPA requirements.

4. Protocols for Health Insurance System

In the Proposed model above in figure-1 we are proposing protocols between Client and Insurance company and, between Hospital and Insurance company to facilitate payment. In our architecture we divide working model into two phases and in each phase we propose protocols for secure communication. Phase - I consists of a) Client Registration service i.e., between Client (C) and Insurance Company(IC) b) Insurance Company Verification (Client data) and Health Card Generation service . In Phase-II we propose protocols between Insurance Company and Client for verification of health records and between Hospital(H) and Insurance company to ensure payment securely by using Expert Security Service.

In Phase-I ,We propose Protocols for

1. Client and Insurance Company (IC)

(C → IC)

a) Secure decision making process for Client selecting Insurance Scheme

b)Registration Process (for Client Registration/Authentication)

Secure authentication algorithms and digital signatures are used in the proposed scheme at the time of client data registration for ensuring data integrity.

2. Insurance Company(IC) and Client (C)

(IC → *C)*

a) Secure Verification Process (For client Data Encryption and Decryption during storing)

b) Health Card Issuing Process(Combination of Image Encryption and PKI)

In Phase-II ,We propose Protocols for

3. Insurance Company and Hospital(IC →H)

a)Secure Verification Process (to verify client/Patients Diagnosis Reports)

b)Secure Payment Process (to release payment to hospital by Insurance Company)

5. Conclusions

In this paper, we have proposed protocols for Health Insurance System to address the HIPAA privacy and security regulations in e-health insurance systems. Instead of adopting conventional manual procedures we have designed a Health Insurance System which is secure based cryptographic key management and ensures cryptographic authentication, encryption and non-repudiation, etc., The delegation of client's data to the Insurance companies and Hospitals are done securely and has avoided the problem of requesting a physical presence of the client/patient for each such access. The proposed scheme can address the HIPAA privacy and security regulations.

6. References

[1].Nilmini Wickramasinghe1 Gail L. Mills, M.Ed.,"E-Knowledge In Health Care: A Strategic Imperative", Proceedings of the 35th Hawaii International Conference on System Sciences – 2002,IEEE Computer Society.

[2]. Code of Federal Regulations (US), Title 45, Part 164, 2002.

[3] W.D. Yu, P. Ray, T. Motoc, *"*A RFID technology based wireless mobile multimedia system in healthcare*"*, The 8th International Conference on e-Health Networking, Applications and Services, HEALTHCOM 2006, Aug 17–19 2006, pp. 1–8

[4]. Lu-Chou Huanga,b, Huei-ChungChub, Chung-YuehLiena, Chia-HungHsiaoc, TsairKao, "*Privacy preservation and information security protection for patients' portable electronic health records*", Computers in Biology and Medicine 39 (2009) 743 – 750

[5] Nadine Blinn Mirko Kühne Markus üttgens,"*Are public and private health insurance companies going Web 2.0?* ",Proceedings of the 43rd Hawaii International Conference on System Sciences – 2010

[6] R. Bhatti, A. Samuel, M.Y. Eltabakh, H. Amjad, A. Ghafoor, "*A Policy based system for federated healthcare databases"*, IEEE Transactions on Knowledge and Data Engineering 19 (3) (Sept. 2007) 1288–1304.

[7] T.T. May,Medical information security: the evolving challenge, IEEE,1998, pp. 85–92.

[8] W.B. lee, C.D. Lee, *A cryptographic key management solution for HIPAA privacy/ security regulations,* IEEE Transactions on Information Technology in Biomedicine 12 (1) (Jan. 2008) 34–41.

[9] Standards for privacy of individually identifiable health information, Federal Register 67 (2002) 53181–53273