International Journal of Innovative Computing, Information and Control
Volume **5**, Number **11(A)**, November **2009**

ICIC International ©2009 ISSN 1349-4198
pp. 3923–3931

A NEW DESIGN OF CRYPTOGRAPHIC KEY MANAGEMENT FOR HIPAA PRIVACY AND SECURITY REGULATIONS

Hui-Feng Huang[1], Kuo-Ching Liu[2] and Hsin-Wei Wang[1]

[1]Graduate School of Computer Science and Information Technology
National Taichung Institute of Technology
Taichung 404, Taiwan
{ phoenix; s18953106 }@ntit.edu.tw

[2]School of Medical Laboratory Science and Biotechnology
China Medical University
Taichung 404, Taiwan
kchliu@mail.cmu.edu.tw

Received June 2008; revised November 2008

Abstract. *The protection of patients' health information is a very important concern today. Health Insurance portability and Accountability Act (HIPAA) privacy and security regulations are two crucial provisions in the protection of healthcare privacy, especially electronic medical information. To comply with HIPAA regulations, this article presents a smart card-based key management to facilitate inter-operations among the applied cryptographic mechanisms. Compared with Lee's smart card-based scheme, our scheme achieves more efficiency and functionality. The important merits include: (1) a dictionary of key tables is not required for users and other units; (2) users can choose their password freely; (3) the computational cost are very low for users; (4) users can freely update their own passwords after registration phase; (5) users are able to access their individual medical information through the authorization process; (6) case of consent exceptions intended to facilitate emergency applications or other possible exceptions can also be dealt with easier.*

Keywords: HIPAA, Privacy, Security, Protected health information, Cryptography

1. **Introduction.** The protection of patients' health information is a very important concern today. All sorts of bills regarding electronic medical data protection have been proposed around the world including the Health Insurance Portability and Accountability Act (HIPAA) of the U. S [1,2]. The trend of a centralized bill that focuses on managing computerized health information is an area that requires further attention. For improving healthcare quality and efficiency, HIPAA provides a conceptual guideline that must be strictly observed by all followed organizations. HIPAA specifically indicates that patients' privacy should be emphasized, and this belief can be applied to the entire health industry throughout the world. In fact, HIPAA is not only a national law of the U. S., but also applies to other countries which stipulate relevant domestic laws. HIPAA has a centralized framework, the integrated guideline learned from HIPAA could facilitate people comprehensively understanding health information issues. HIPAA is well-known. This prominence increases popular confidence in the confidentiality of health information, thus it can be simplifying the advancement of healthcare policies and procedures. In addition, internationalization is a tendency for all countries, and a guideline based on HIPAA would be beneficial for future international cooperation. Therefore, based on the HIPAA [4], Taiwan's Department of Health (DOH) has recently been creating a framework of the domestic health information regulations "Medical Information Security and