A Cryptographic Alternative for Preserving PHI in Compliance with HIPAA Privacy/Security Regulations

Bo Li¹ and Jung-San Lee²,*

¹Department of Information Security,
Tongji University,
NO.1239, Siping Road, Shanghai, China
lxbosky@live.cn
²Department of Information Engineering and Computer Science,
Feng Chia University,
Taichung 40724, Taiwan, ROC
leejs@fcu.edu.tw

Received 4 March 2010; Revised 15 August 2010; Accepted 15 September 2010

Abstract. The privacy/security regulation of HIPAA has addressed many of the rights and obligations of both the patient and the health information system. Emergency treatment, however, still presents problems as we do not have an exact definition to apply. Employing cryptographic techniques, we provide a novel model which can confirm essentials in HIPAA. In particular, we have discussed how the new model can appropriately handle emergency cases. This is useful for engineers to design a better HIPAA system. Furthermore, the correctness of authentication is confirmed under the BAN logic model.

Keywords: HIPAA, privacy, security, PHI, EMR, BAN logic

References


* Correspondence author


