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

Bo Li[1] and Jung-San Lee [2,*]

[1]Department of Information Security,
Tongji University,
NO.1239, Siping Road, Shanghai, China
lxbosky@live.cn

[2]Department 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

[1] "Health Insurance Portability and Accountability Act of 1996," 104th Congress, Public Law 104-191, 1996.

[2] G. M. Stevens, "A Brief Summary of the Medical Privacy Rule," CRS Report for Congress, 2003.

[3] "Privacy rules," U.S. Department of Health and Human Services, [Online]. Available:

[4] W. B. Lee and C. D. Lee, "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations," *IEEE Transactions on Information Technology in Biomedicine*, Vol. 12, No. 1, pp. 34-41, 2008.

[5] C. Lambrinoudakis and S. Gritzalis, "Managing Medical and Insurance Information through A smart-card-based Information System," *Journal of Medical Systems*, Vol. 24, No. 4, pp. 213-234, 2000.

[6] L. J. Damschroder, J. L. Prittsc, M. A. Neblo, R. J. Kalarickal, J. W. Creswell, R. A. Hayward, "Patients, Privacy and Trust: Patients' Willingness to Allow Researchers to Access Their Medical Records," *Social Science & Medicine,* Vol. 64, No. 1, pp. 223-235, 2007.

[7] A. L. Dunlop, T. Graham, Z. Leroy, K. Glanz, B. Dunlop, "The Impact of HIPAA Authorization on Willingness to Participate in Clinical Research," *Annals of Epidemiology,* Vol. 17, No. 11, pp. 899-905, 2007.

[8] "Security rules," U.S. Department of Health and Human Services, [Online]. Available: http://www.hhs.gov/ocr/hipaa/.

[9] "HIPAA Administrative Simplification Enforcement Final Rule," U.S. Department of Health and Human Services, [Online]. Available: http://www.hhs.gov/ocr/hipaa/.

[10] D. K. W. Chiu, P. C. K. Hung, V. S. Y. Cheng, E. Kafeza, "Protecting The Exchange of Medical Images in Healthcare Process Integration with Web Services," *Proceedings of the 40th Annual Hawaii International Conference on System*

* Correspondence author

Sciences, Big Island, Hawaii, USA, pp. 131-131, 2007.

[11] P. Ray and J. Wimalasiri, "The Need for Technical Solutions for Maintaining the Privacy of EHR," *Proceedings of the IEEE 2006 International Conference of the Engineering in Medicine and Biology Society*, New York City, New York, USA, pp. 4686-4689, 2006.

[12] W. D. Yu and M. A. Chekhanovskiy, "An Electronic Health Record Content Protection System Using Smart Card and PMR," *Proceedings of the Ninth International Conference on E-Health Networking, Application and Services*, Taipei, Taiwan, pp. 11-18, 2007.

[13] T. D. Breaux and A. I. Anton, "Analyzing Regulatory Rules for Privacy and Security Requirements," *IEEE Transactions on Software Engineering*, Vol. 34, No. 1, pp. 1-16, 2008.

[14] T. D. Breaux, M. W. Vail, A. I. Anton, "Towards Regulatory Compliance: Extracting Rights and Obligations to Align Requirements with Regulations," *Proceedings of the 14th IEEE International Requirements Engineering Conference*, St. Paul, Minnesota, USA, pp. 46-35, 2006.

[15] W. Stallings, Cryptography, *Network Security – Principles and Practices, Pearson Education Inc., Fourth Edition*, New Jersey, USA, 2006.

[16] M. Burrows, M. Abadi, R. Needham, "A Logic of Authentication," *ACM Transactions on Computer Systems*, Vol. 8, No. 1, pp. 18-36, 1990.

[17] W. Rankl and W. Effing, *Smart Card Handbook, John Wiley & Sons Ltd., Second Edition,* New York, USA, pp. 18-19, 2000.

[18] C. H. Fancher, "In Your Pocket: Smartcards", *Spectrum, IEEE,* Vol. 34, No. 2, pp. 47-53, 1997.

[19] D. Jones, "Smart Cards-the Key to Secure and Flexible Healthcare Provision," *Card Technology Today*, Vol. 15, No. 11, pp. 8, 2003.

[20] P. Breese and W. Burman, "Readability of Notice of Privacy Forms Used by Major Health Care Institutions," *Journal of American Medical Association*, Vol. 293, No. 13, pp. 1593-1594, 2005.