ISSN - 2250-1991 | IF : 5.761 | IC Value : 79.96

Original Research Paper Management

INFORMATION SECURITY MANAGEMENT (ISM) IN ACCORDANCE TO HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT (HIPAA) IN HEALTHCARE INDUSTRY

Mr. Anupam — Assistant Professor, HMR Institute of Technology & Management, Hamidpur, New Delhi – 110036

Dr. Himanshu Sharma — Medical Officer Incharge, South Delhi Municipal Corporation, Ayuvedic dispensary, basai darapur, New Delhi – 110088

ABSTRACT

Inspite of advancement in research studies about Information Security Management (ISM), very limited studies focused on importance of Information Security Management (ISM) in the healthcare Industry, which is in actual a highly regulated business models according to Health Insurance Portability and Accountability Act (HIPAA). Information security and privacy both are upcoming issues in the healthcare Industry. The advancement in patient records storage, regulatory acts, service provider details and the increasing demands for sharing detailed information among patients and service providers with secrecy maintenance of Patients data, demands for better information security management. On surveying the literature on information security and privacy available in books, information published in journals as well as interdisciplinary subjects like health informatics, public health & administration, Regulatory laws, medicine and industry reports. We will discuss about recent advancement and upgradation of new areas of interest to the information systems management (ISM).

KEYWORDS: Information Security Management (ISM), Healthcare Industry, Health Insurance Portability and Accountability Act (HIPAA).

Introduction

Information system management (ISM) is most important components in Healthcare Industry for improving quality of services, online portal and maintenance of patient data security. Recently Government has taken initiatives for wide-scale adoption for online transaction in Healthcare Industry. Although, advancement in Information Technology in Healthcare Industry affects many other industries or components like 3–5% of revenue, unlike to previous financial services which were closer to 10% is the business[1]. Agencies suggests that today 75% of patients are aware about their health compared to earlier and sharing information over health websites without proper caution[2]. Possibly, this patient perception is fueled by the fact that medical data disclosures are the second highest reported breach[3]. In response to these increasing threats to health information and privacy, new regulations at both the state and the federal level have been proposed in the USA, e.g., Health Insurance Portability and Accountability Act (HIPAA).

INFORMATION SECURITY AND PRIVACY

Here, we discuss about a comprehensive management of the information security and privacy in healthcare Industry. Fig 1 clearly demonstrated various research domains of an interdisciplinary survey in various publications and fields including information system and privacy. There are majorly four research domains available in information security and privacy which correlated with corresponding four domains of information-systems-related research areas in Healthcare Industry.

1. Researches related health consumers like personal record management and website based systems, have framed variety of security-related topics including privacy and security concerns among consumers, economic impact of privacy and security breaches to consumers, medical identity theft on consumers.
2. Research related to service providers like drivers of Information Technology companies, impact of Information Technology on medical account, telemedicine and pervasive computing along with interaction for emerging security issues i.e. layout and development of control systems, sustainability of information integrity, network security, privacy policy and risk management.
3. Research focusing towards internal organizational issues like health services subcontracting, network and upgradation of organizational health coordination.
4. Research deals with several information security and privacy research directions (For example development of data interoperability standards, regulatory guidelines of Information security and privacy in healthcare and secured data mechanisms).

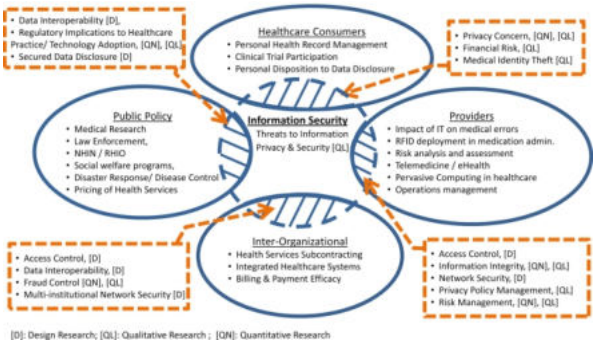

Fig 1. Research domains in Information security and privacy

PRIVACY CONCERN AMONG HEALTHCARE CONSUMERS

The perception of security and privacy concerns deeply from feedback of a special class of patients, including mental health patients, seekers of HIV testing and adolescents. In a recent survey data of research on healthcare confidentiality, make four overarching conclusions as follows[4]: -

1. Patients who strongly emphasize that their personal information should be shared only with service providers / staff, involved in their medical care.
2. Patients who claims for the need of information sharing among physicians / service providers, though HIV patients are generally less interested to approve share of their health information.
3. Patients who agree to inform sharing among physicians / service providers, reject the notion of releasing information to third parties, including employers and family members.
4. Patients who have undergone genetic investigation believe that Hospital / laboratory should bear the responsibility of revealing test results to other at-risk family members.

REGULATORY COMPLIANCE

Health Insurance Portability and Accountability Act (HIPAA) compliance has become a basic requirement in Healthcare Industries / Organization. Recently, a study Warkentin et al. (2006) has been conducted to characterize the compliance behaviour among administrative staff and medical staff of government and private sector Healthcare Industries. It has been observed that healthcare professionals of government hospitals have higher self-efficacy (i.e., belief in their capability to protect patient's information and privacy) as compared with their counterparts in private hospitals. Furthermore, on average the administrative staff exhibits higher self-efficacy than medical / paramedical staff across both Government and private hospitals. Moreover, the behavioural compliance of medical, paramedical and administrative staff, was positively concerned to self-efficacy and perceived in purview of organizational support.

DATA INTEROPERABILITY AND INFORMATION SECURITY

Most of the healthcare information systems currently in use, store patients information in various proprietary formats. This diversity of various data formats invites a great hurdle in sharing patients information data among industries / organizations. In a recent studies, empirically forced that investing in ISM interoperability and establishing a health information exchange module could save billions of money to the industry annually[5]. Whereas without interoperability, continued adoption of current ISM technologies, will encourage information kiosk which already exist in paper based patients information records leading improper management. Moreover, privacy and information security in maintaining an interoperable health information exchange remain one of the dominant issues.

INFORMATION SECURITY ISSUES OF E-HEALTH SYSTEM

The development of internet advancement has transformed the business module for customer-oriented industries such as retail, wholesale and related financial services completely. The healthcare sector is also experiencing an upgradation in installation of healthcare services through internet services and mobile serivices like online consultation, e-prescription, online reporting of pathological investigations, e-clinical trials and patient information system[6]. Recent advancement in web services have opened new approaches to patient information management such as 'Banking on Health' or 'Health Bank'[7]. The detailed information about health bank, was first conceptualized in 2000. It is basically a platform for storage and exchange of patient health records synchronized after banking system where patient / consumers could submit and withdraw information about himself. Recently launched programs of Microsoft's 'Health Vault' and 'Google Health' are presentable examples of health banking systems.

INFORMATION SECURITY RISKS IN AUTHORISED DATA DISCLOSURE

Among healthcare industry, it is much needed to share patients information across organizational boundaries to maintain the deep interest of multiple stakeholders as well as bodies / agencies involved with public health interest. Although, the release of patient information could appear as identifying information as well sensitive information which may violate privacy as well cause socio-economic repercussions for patients. Still such information, when transferred for identifying and sensitive information, must exhibit the analytic properties to assure statistical inferences, particularly when it was released for the epidemiological research[8]. Advances in technology have enabled the consolidation of health records from multiple sources to a single research database, which supports researchers engaged in public health, clinical methods and health services in general.

INFORMATION INTEGRITY IN HEALTHCARE INDUSTRY

Information security and privacy risks are often referred by terms like 'data breach', 'hackers attack' and 'data theft' in the social-media. Although the key aspects of information security and privacy is maintaining data integrity of patients information in addition to confidentiality and availability. In the healthcare industry, mis-management in system services could invite primary internal threat for patients information security. For example, the integrity of patients records may be compromised by faulty alert design. Recent research has mentioned that even excessive alert design may cause 'alert fatigue' resulting physicians to receive override alerts and finally impacting patient safety and privacy[9]. An esteemed organization of research has starting working on alert overriding patterns among physicians using both quantitative and qualitative research approach.

INFORMATION SECURITY AND PRIVACY RISK MANAGEMENT

Management of information security and privacy risks is very comprehensive procedure and demands huge investments in organizational resources and multidisciplinary approaches like OCTAVE which usually implies for investment - based information security assessment[10], Bayesian network analysis[11], elicitation of user's privacy valuation using experimental economics[12], and information security insurance contracts. The OCTAVE approach was developed at the Software Engineering Institute (SEI) at Carnegie Mellon University and was first launched at hospital indutry for public use in 2001. Furthermore, The approach was designed on the basic of three pillar principles

- **Security methods -** self-direction, adaptable procedures with well-defined process having scope for continuous improvement.
- **Risk management -** forward looking system to manage uncertainty, focus on critical assets and integrated management of information security and privacy with precise business strategies and goals.
- **Organizational culture -** open discussion of current security issues, identifying security and privacy risks at route level with analyzing them globally using an interdisciplinary approach with team members from both of the specialty management and technology.

CONCLUSION

We have discussed in detail the complete body of latest information on information security and privacy among healthcare industry with the help of several research domains including privacy concerns among healthcare patients / consumers and providers of regulatory compliance. Our review about the subject indicates that research scholars from health informatics, legal and information technology with software have invented a magnitude of methodologies including research domain, qualitative and quantitative research methods to completely perfecting each and every aspect of security and privacy in the healthcare Industry. Information security management (ISM) has emerged as significant tool among mainstream information system research scholars, yet there has been only few publication concerning the unique security and privacy challenges found in healthcare industry.

References

1. Baker, D.B. (2006) 'Privacy and security in public health: maintaining the delicate balance between personal privacy and population safety', Proceedings of 22nd Annual Computer Security Applications Conference, Miami, FL, pp.3–22.
2. Raman, A. (2007) 'Enforcing privacy through security in remote patient monitoring ecosystems', 6th International Special Topic Conference on Information Technology Applications in Biomedicine, Tokyo, Japan, pp.298–301.
3. Hasan, R. and Yurcik, W. (2006) 'A statistical analysis of disclosed storage security breaches', Proceedings of 2nd ACM Workshop on Storage Security and Survivability, Alexandria, VA, pp.1–8.
4. Sankar, P., Moran, S., Merz, J.F. and Jones, N.L. (2003) 'Patient perspectives on medical confidentiality: a review of the literature', Journal of General Internal Medicine, Vol. 18, pp.659–669.
5. Walker, J., Pan, E., Johnston, D., Adler-Milstein, J., Bates, D.W. and Middleton, B. (2005) 'The value of health care information exchange and interoperability', Health Affairs, Vol. 19, No. 1, pp. W5.10–W5.18.
6. Kalorama Information (2007) Wireless Opportunities in Healthcare, www.MarketResearch.com.
7. Ramsaroop, P. and Ball, M.J. (2000) 'A model for more useful patient health records', MD Computing, Vol. 17, No. 4, pp.45–48.
8. Truta, T.M. and Vinay, B. (2006) 'Privacy protection: p-sensitive k-anonymity property', Paper presented at the 2nd International Workshop on Privacy Data Management, 8 April, Atlanta, GA.
9. Sijs, H.V.D., Aarts, J., Vulto, A. and Berg, M. (2006) 'Overriding of drug safety alerts in computerized physician order entry', Journal of Medical Informatics Association, Vol. 13, pp.138–147.
10. Alberts, C.J. and Dorofee, A. (2002) Managing Information Security Risks: An OCTAVE Approach, Addison Wesley Publications, Boston.

11. Maglogiannis, I. and Zafiropoulos, E. (2006) 'Modeling risk in distributed healthcare information systems', Proceedings of the 28th Annual International Conference of the IEEE Engineering in Medicine and Biology Society, New York City, NY, pp.5447–5450.
12. Poindexter, J.C., Earp, J.B. and Baumer, D.L. (2006) 'An experimental economics approach toward quantifying online privacy choices', Information Systems Frontier, Vol. 8, pp.363–374.