https://doi.org/10.48009/2_iis_2015_168-175

A MULTIFACTOR RESEARCH MODEL OF ANTECEDENTS OF SECURITY AND PRIVACY IN HEALTHCARE SETTINGS

Sushma Mishra, Robert Morris University, mishra@rmu.edu
Peter Draus, Robert Morris University, draus@rmu.edu
Natalya Goreva, Robert Morris University, goreva@rmu.edu
Donald Caputo, Robert Morris University, caputo@rmu.edu

ABSTRACT

Security, privacy, accessibility, transparency, awareness and perception are the new initiatives in the health care forum promulgated by the HIPAA structural demands, and implemented more recently by the Affordable Care Act. Health care breaches, adverse medical events, hacking into hospital and health care corporation files have become common events. This research study concentrates primarily on the security, privacy, and awareness of the health care providers in their professional assignments and in their responses and perceptions of the solutions that are integrated into the fabric of their health care experience. The demographics, derived from a survey, examine the length of current employment, occupational spectrum, size of organization, level of computerization, and length of health care employment. Five hypotheses are detailed concerning training, user awareness, equity of security policies and perceptions based on management policies.

Keywords: Healthcare, security, privacy, HIPPA, training, communication, fairness, technical infrastructure

INTRODUCTION

The Healthcare industry, like any other vital computerized entity, has similar challenges in ensuring confidentiality, integrity and availability of all facets of healthcare data. Despite the growth in digitization of medical records and associated security risks, there are limited studies that have focused on security and privacy challenges in meeting HIPAA compliance requirements [8]. Due to the sensitive nature of health care data, its improper use or disclosure can cause serious negative implications for the patient, the caregiver and the facility, reflecting the areas of discrimination, stigmatization, loss of insurance or employment and financial outcomes [12].

The Health Insurance Portability and Accountability Act (HIPAA) was the first comprehensive federal legislation in the United States to address the need to protect individual health information and declare it "privileged". Regulations such as HIPAA make security and privacy controls mandatory. This law protects the privacy of patients by limiting the use of patient information disclosure and ensures security of this data in healthcare organizations through their databases, in rest as well as transit. The Security Rule of HIPAA works efficiently with the Privacy Rule to prescribe a number of administrative, physical, and technical safeguards, organizational requirements, and policies and procedures. Increased regulation as proscribed in the formulations of HIPAA has made security and privacy practices mandatory for all healthcare organizations. However, some surveys by both industry groups and the United States Department of Health and Human Services (HHS) noted wide disparity both in security practices and in perceived compliance with federal (HITECH/HIPAA) and state regulations [11]. It is not surprising that hospital health care practices vary, and so do security practices that achieve regulatory compliance. It is important to investigate the factors that would lead to better security compliance practices. Thus, the major thrust of this paper is to fully understand the practices that lead to better compliance of security policies that ultimately effect regulatory compliance.

With the changing nature of organizations today, security preparedness needs to be aligned with compliance requirements to keep the health data secure. Healthcare organizations in particular maintain complex environments where human capital (in the form of healthcare workers such as physicians, nurses, pharmacists and ancillary services staff etc.) and technological assets (in the form of electronic medical records, data transmission modalities etc.) have to be tightly integrated to foster a secure environment for privacy of privileged health records of patients. The breadth of health care services and the life cycle of health data ranging from clinics/hospitals, scanning, diagnosing, insurance, pharmacy and more, makes it difficult to define the boundaries of what the health care organization really controls as an entity [8]. Traditional ways of developing and instituting security controls and expecting complete compliance might not work in the modern healthcare organizations.

In order to ensure tight integration of people and technology for information security, it is imperative to understand the antecedents of effective security compliance activities and develop controls in alignment with the factors leading to the success or failures of such initiatives. This study postulates the underlying factors that lead to better compliance of HIPAA initiatives for security and privacy of electronic medical records. A research model is proposed based on current critical literature reviews. The relationships are hypothesized and statistically tested.

The remainder of this paper is organized in the following manner. A critical review of the research literature in the area of healthcare security in the context of EMR is presented. The review leads to the next section of research model development and hypothesis. The model is followed by presentation of data collection, analysis and results of the survey. The discussions are provided with implications, constraints and limitations.

LITERTAURE REVIEW AND PROPOSED MODEL

Within a short period of time information technology progressed relentlessly in the healthcare domain, from an occasional use in a few hospitals, to playing a vital part in managing almost all salient patient information. As it became ubiquitous within the healthcare community, the protection of Electronic Medical Records (EMR) has become a vital task that cannot be neglected. On average, EMR security breaches cost the healthcare organizations $6 billion a year [10], and more than 32 million Americans became victims of healthcare data breaches due to thieves, hackers, and employees' negligence [3]. Mobility and the presence of mobile technologies (such as smartphones and tablets that are widely used by doctors, nurses and other healthcare employees) add a new dimension to the challenge of protecting patients' privacy [4].

Many healthcare organizations follow a reactive path of implementing technical stopgaps because information security has been perceived to be largely a technical issue—independent from the business of providing care [11]. This attitude needs to shift towards a comprehensive focus on security in a proactive manner that would entail emphasizing the importance of integrating technical solutions with organizational security culture, policies, and education [18]. A holistic perspective relies on many of the same underlying mechanisms as societal laws: providing knowledge (through education) of what constitutes acceptable and unacceptable conduct to increase the efficiency of an organization's security activities [1].

Employees in healthcare organizations are the main asset and the driving force in security compliance. All employees can be divided into the group that is willing to comply, and the other that is not willing to comply with security policies. The non-complying group can be further divided into those employees who have malicious intentions and those who choose not to comply for non-malicious reasons (lack of time, lack of motivation, conflicting interests etc.). The malicious non-complying group is less researched and less predictable that the non-malicious group [20]. The non-malicious non-complying group is far larger in size, more predictable, and thus permeates the focus of this paper. Researchers believe that the most data breaches occur due to the non-malicious non-complying group, as the result of negligence: unattended devices with patients' information, unencrypted data, mistakenly sent information, etc. We believe that by changing the employee perception of security and its importance, it is possible to improve their compliance. As Sipponen and Vance (2010) admit, the way employees rationalize their behavior may impact their compliance with security policies.

Effective distribution of security policies among healthcare workers became an important task of the management [14]. However, managing security policies becomes effective only if the healthcare employees are willing to comply with the security standards [2]. Many researchers and healthcare professionals admit that the key to preventing EMR breaches is employee training, communication, and increased motivation. Glaser and Aske, 2010 recommend establishing an IT steering committee in all medium to large size health organizations. The committee should include representatives from different layers of the organization, from management to doctors, nurses, and IT personnel. This kind of engagement should increase the compliance with security policies. This employee engagement in developing and implementing security policies can be named as a key factor in increasing security compliance. Besides engagement, three factors emerged from the review of literature as possibly increasing employee motivation to comply with security. These factors are training, awareness, and effectiveness of technical infrastructure. However, no significant quantitative results were found to support this statement in its entirety. In conclusion, it is important to lead employees to believe that Information Assurance policies are beneficial and vital, and training and communication is the way to develop such assurances [4]. In this paper we attempt to outline the factors that impact employees' motivation to comply with the security policies and regulations.

Healthcare organizations are likely to place the highest priority on adopting technical solutions (i.e., firewalls, encrypted e-mails, network monitoring, intrusion detection etc.) rather than security management processes [11]. Even with the high adoption levels of technical solutions, health care organizations reported that compliance levels remained varied. This compliance variation seems to be associated with the adoption levels of policies and procedures suggesting better initiatives for understanding and compliance of such policies. These studies argue that increased security awareness of employees and educational programs leads to better compliance with information security rules [18]. Based on the review of literature, the following research model is proposed and relationships are hypothesized:

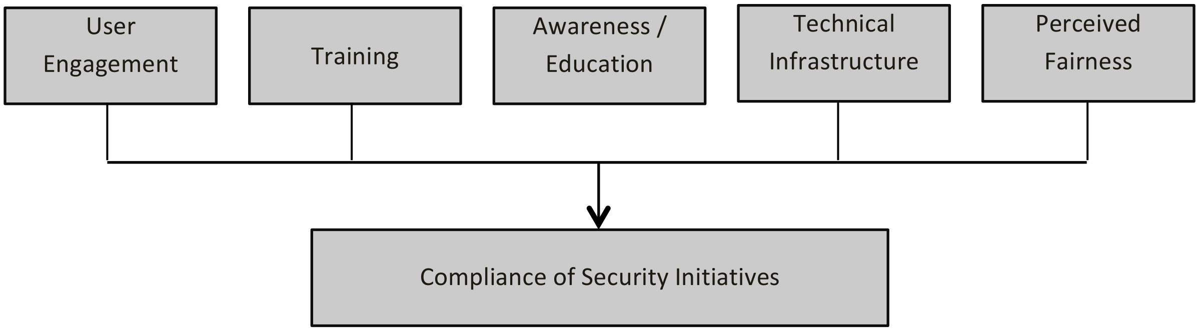


Figure 1. Antecedents of Security Compliance Initiatives Research Model

H1: User engagement in developing and implementing security policies and procedures increases the compliance of security initiatives in an organization.

H2: Adequate training for users while implementing security policies and procedures increases the compliance of security initiatives in an organization.

H3: Increasing the awareness of users' about security policies and procedures increases the compliance of security initiatives in an organization.

H4: Perceived fairness of security policies and procedures increases the compliance of security initiatives in an organization.

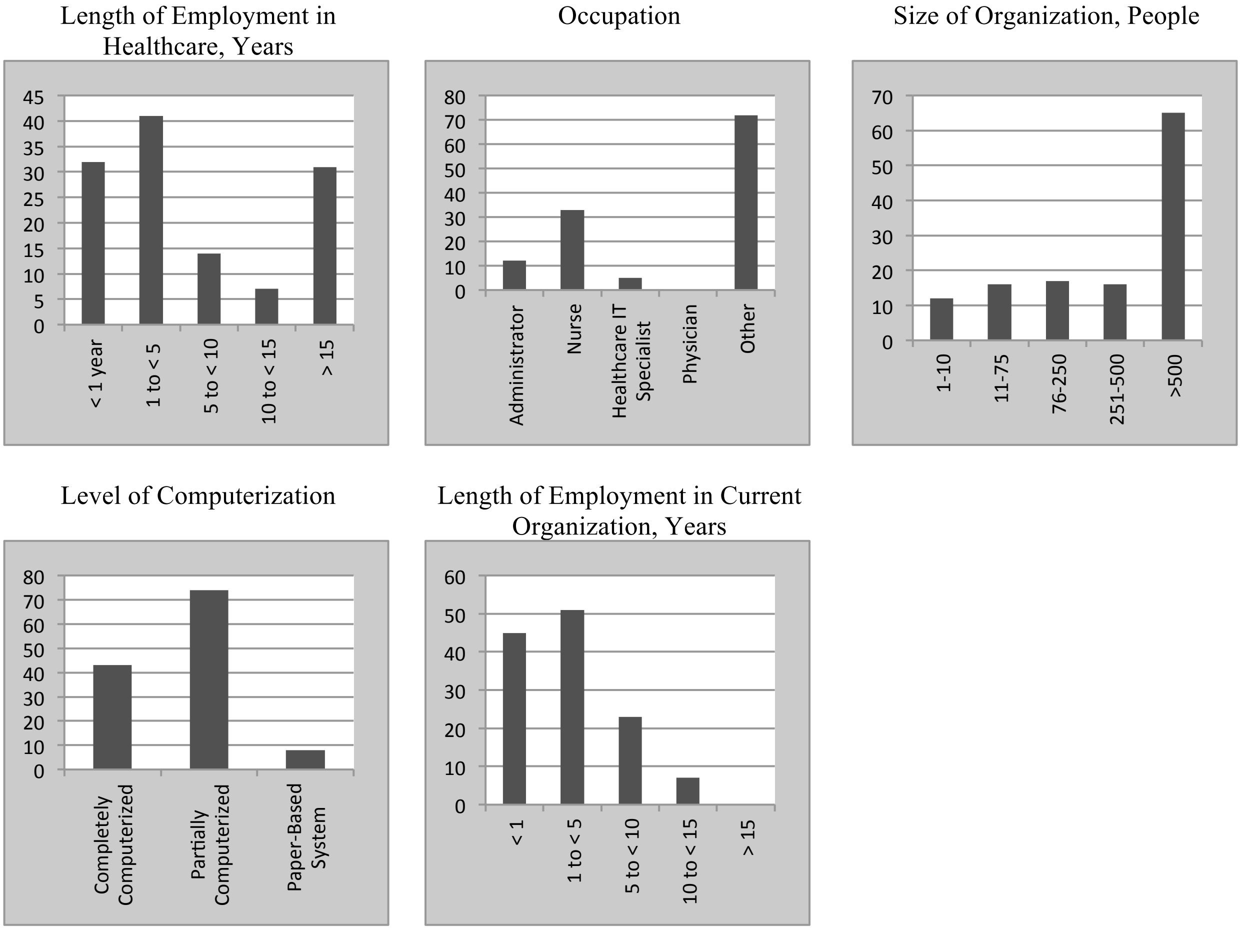
H5: Effective technical infrastructure available to the users' increases the compliance of security initiatives in an organization.

DATA COLLECTION AND ANALYSIS

A survey with 20 items for all the dependent and independent variables and 9 items for demographic information of the sample was developed. Data was collected in heath informatics courses taught at a University in Northeastern United States. The survey was distributed in undergraduate, masters and doctoral level courses.

The sample consisted of 80 subjects currently working in a Health Care environment. More than 55% of the subjects had more than 5 years of professional experience and only 9 subjects had less than 1 year experience in the field. Additionally, 9 subjects reported having a high school or trade school degrees, with the rest reporting advanced degrees. While the age range skewed younger with 47% reporting being between 20 and 29 years old, the spread of ages was broad with over 26% reporting being over 50 years old. 82% were female. Almost 75% of the subjects worked in larger institutions employing more than 250 health care providers.

The survey was designed to gather general information on security awareness and environments in a health care setting. The questions were grouped into six areas of interest: Engagement, Training, awareness, Fairness, Technology, and Compliance. To analyze the data, indexes were developed for each one of these areas by summing the subjects' responses to specific questions on the survey that had been keyed to each area. The number of items in each index was not equal.


Length of Employment in Healthcare, Years

Occupation

Size of Organization, People

Level of Computerization

Length of Employment in Current Organization, Years

Figure 2. Demographics of the Sample

One of the demographic questions, "Are you aware of any reported security breach in your organization in the recent past?" shows about 57% respondent were not aware if any such incident occurred or was reported.

RESULTS AND DISCUSSIONS

H1: User engagement in developing and implementing security policies and procedures increases the compliance of security initiatives in an organization.

The above hypothesis was accepted. A Pearson correlation was performed between the User Engagement Index and the Security Compliance Index, resulting in a coefficient of .724. The two indexes were highly correlated. This clearly indicates that user engagement is important in ensuring compliance of HIPAA initiatives in an organization. The users are invested from the initial phase of development of security controls, and the application and acceptance of such initiatives increase.

Research in this domain suggests that changes in working conditions of employees, in the form of complex controls, could relate to IT espionage and sabotage incidents [17]. Developing controls that can create problems in daily work conditions, without explaining the intent and necessity of such controls, leads to employees feeling pressured to perform at the same operational level as prior to their implementation, and employees will hence see these increased controls as constraining, inconvenient, and difficult to understand [17]. It is important to engage the end users of the systems about the importance of security controls, formally and informally, and communicate the concerns of acceptable security behaviors. Clarity in intent of controls leads to better acceptance of these measures leading to effective compliance actions.

H2: Adequate training for users while implementing security policies and procedures increases the compliance of security initiatives in an organization.

The above hypothesis was accepted. A Pearson correlation was performed between the User training Index and the security compliance Index, resulting in a coefficient of .750. The two indexes were highly correlated. This is not surprising at all considering there is a large support contingent in research literature for training users adequately for compliance purposes. Training multiple times with work related examples increases the understanding of the business process and the systems that reduced the occurrence of mistakes.

Employees can err often in ignorance and misunderstanding, and sometimes (despite a strong determination to avoid them), these errors may enter the system. Errors may arise from processes within an actor or from processes external to the actor. Incorrect input, insufficient knowledge, or wrong action are all causes of error [13]. The disparate and fragmented nature of the healthcare delivery system and organizational issues such as staffing, procedures, and work environment are considered major contributing factors [19] to the occurrence of errors. Training individuals with work related examples would help in reducing the errors caused by ignorance, lack of clarity and lack of understanding of the context of the security control.

A recent study [15] concerning critical factors for successfully reducing the likelihood of medical errors and minimizing their effects identifies education and training as one of the critical factors that reduce errors leading to undesired consequences.

Barlaow el al (2013) argue that improved training techniques and other communications that focus on reducing rationalization behaviors may be the key in helping employees understand that policy-breaking is unacceptable. Properly structured communication may ultimately lead to fewer violations of IT security policies.

Management along with formal training of employees concerning security controls should also encourage informal discussion among all employees in communications and awareness raising initiatives. An ideal security communication program should include training on both deterrence and neutralization techniques which means that organizations need to include consequences for violating policies in their training, as well as focus on how behavior should be justified [1]. Focused discussion on those types of neutralization points that are most salient to the organization's policies are warranted.

H3: Increasing the awareness of users about security policies and procedures increases the compliance of security initiatives in an organization.

The above hypothesis was accepted. A Pearson correlation was performed between the user awareness index and the security compliance index, resulting in a coefficient of .764. The two indexes were highly correlated. Raising the awareness of security policies and procedures provides a reference framework to the users and bounds the behavior of these users around the security control instituted in the organization. Security policies provide a blueprint of all security initiatives that are currently executed in an organization. Users of the systems in healthcare settings are required to know these policies not only for securing the informational assets at the work place but also for protecting their positions in case of an unexpected event.

The Health and Human Services (HHS) security guidance (U.S. Department of Health & Human Services, 2006) suggests security awareness and training as the key to successful compliance of regulations.

H4: Perceived fairness of security policies and procedures increases the compliance of security initiatives in an organization.

The above hypothesis was accepted A Pearson correlation was performed between the perceived fairness index and the security compliance Index, resulting in a coefficient of .770. The two indexes were highly correlated. The perceptions about security policies do have an impact on actual compliance of these policies. Security policies define the acceptable and unacceptable behavior of users around informational assets and lists the penalties in case of non-compliance. It is essential that employees perceive these controls and associated penalties as fair practices to assure the success of the security efforts.

Employees should sense fairness in terms of clear disciplinary actions in case of non-compliance with controls. The perceived fairness goes a long way in developing an attitude of being a part of the solution of a potential security problem in the organization ([7], [17]).

The clinical staff, compared with the administrative staff or third parties, is generally the most difficult to work with and to educate in terms of privacy compliance enforcement. The clinical staff also tends to commit errors more frequently [13]. Due to the nature of the work experience, where rules are frequently broken or overridden to provide the best service to the patient, the clinical staff is often seen as one that bypasses privacy and security restrictions related to the use or disclosure of PHI [13]. Managing the clinical staff needs to be a high priority in gaining compliance with HIPAA and this can be achieved through clearly establishing the fairness of policies and procedures around security controls. If the understanding of the requirements of the controls is high and consequences of non-compliance are clear, the likelihood is that such violations of controls will not occur.

Perceived justice in punishment of non-compliant actions is a predictor of insider and employee violations [21]. Research suggests several other techniques for deterrence to reduce policy violations such as formal and informal organizational sanctions [6]. This is accomplished through neutralization and rationalization of deviant behavior and formal techniques among employees [1].

The results are summarized in the table below.

		Engagement	**Training**	**Awareness**	**Fairness**	**Techno**
Compliance	Pearson Correlation	.724**	.760**	.821**	.713**	.739**
	Sig. (2-tailed)	.000	.000	.000	.000	.000
	N	79	79	79	79	79

H5: Effective technical infrastructure available to the users' increases the compliance of security initiatives in an organization.

This hypothesis was accepted. A Pearson correlation was performed between the effective technical infrastructure index and the security compliance index, resulting in a coefficient of .739. The two indexes were highly correlated.

Lignilal et al (2012) analyzed 237 security incidents in the health care industry to understand the cause of such breaches. These researchers determined that only 12% of the 237 incidents involved malicious acts; human error accounted for the remainder (approximately 88%). Further analysis of the human error category suggested about 53% of these incidents were related to stolen or missing media containing confidential patient information [13]. These losses can be attributed to poor policy formulation and enforcement in healthcare organizations. Additionally, the lack of a second level of control such as data encryption on those lost or stolen media further aggravated the losses. These events clearly suggest that technical infrastructure such as use of encryption, and policies regarding stolen or lost records need to be addressed and controls built into and around these areas would result in an increasingly more effective security compliance model.

Technical infrastructure within organizations is essential in ensuring security compliance efforts. Security behavior can be enforced using technical controls such as reminders when sensitive documents are printed, and alerts when clinical staff or anyone else is accessing records of patients who are not directly under their care.

The architecture of the technical infrastructure could potentially prevent and deter non-compliance of security controls. For example automatically disabling lost devices, monitoring system log files for suspicious behavior or traffic on a regular basis can significantly reduce the issues of failing to meet control standards.

It is pertinent that technology can help implement a defense-in-depth strategy founded on error avoidance, error interception, and error correction [13]. Situation dynamics and policies and processes play an equally important role.

In summary, management commitment and attitude play a critical role in the success of security compliance initiatives. Employees, who perceive uncertainty in management style, strongly sense that managements' future actions will be unpredictable, surprising, and filled with ambiguity, exhibit less identification with controls and practices [17].

IMPLICATIONS AND LIMITATIONS

There are several implications of this study. First, the results suggest that having security policies and procedures is not enough to ensure compliance with policies and regulations. It is essential that antecedents to compliance of policies need to be developed, fostered and sustained. Thus, it plays a part in ensuring training, adequate IT infrastructure, effective communication, awareness and perceived fairness of such security policies and rules. Second, practitioners can design tasks and activities around the antecedents identified in this study to increase the effectiveness of security controls and increase the availability better compliance policies and procedures. Finally, this study contributes to research literature in this area by suggesting a statistically significant relationship between compliance initiatives and its antecedents.

This study is not free of limitations. The data statistics were collected through a survey instrument, which has elements of self-report bias. Additionally, all the participants were in some guise of a nursing role within healthcare organizations, which could shape the perception of the participants in a skewed boundary. A survey for all stakeholders in healthcare organizations might provide a more holistic and accurate perspective.

CONCLUSIONS

The intent of this study was to examine the antecedents and present practices of the security and privacy dimensions in health care environments in order to understand the nature and parameters of involvement, as well as the effectiveness of management as perceived by the caregiver. It was based on a survey-driven tool that captured relevant experiential data in five interest categories, defined as engagement, training, awareness, equity (fairness), and technology/ compliance. Weaved throughout the discussion was the subject perception of variances in the primary categories in order to compare the intent of the action to the perception of the relevance and management of the action, which could preface the success of their involvement.

The most persuasive general results of the research, supported by significant correlation indices, were that (1) user engagement is vital in ensuring compliance results, that (2) specialized training increases compliance of security initiatives, that (3) raising the awareness level of users heightens the compliance factor in all categories, that (4) perceived fairness (equity) largely dictates the involvement of the care giver and instills confidence in the management of health care resources, that (5) technology within the infrastructure that is made available, intuitive and understandable to health care providers measurably ensures and protects the effectiveness of security compliance and efficiency.

REFERENCES

1. Barlow, J., Warkentin, M., Ormond, D. and Dennis, A. (2013). Don't make excuses! Discouraging neutralization to reduce IT policy violation, Computers & Security, 28, l-15
2. Bulgurcu, B., Cavusoglu, H., and Benbasat, I. (September 2010). Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS Quarterly, 34(3), pp. 523-548.
3. Campbell, R. and Schoch, D. (7-Jul-2014). Millions of electronic medical records breached. Center for Healthcare Reporting, California Healthcare Foundation. Retrieved on 4/2/15 from http://centerforhealthreporting.org/article/millions-electronic-medical-records-breached

4. Cannoy, S. D. andcannoy Salam, A. F. (2010). A framework for healthcare information assurance policy and compliance. Communications of the ACM, 53(3), pp. 126-131.
5. Davis, Diane C. and Squibb, Jeff (2004) "Policies, Procedures, and Devices Used by U.S. Hospitals for HIPAA Privacy and Security Compliance," Communications of the IIMA: Vol. 4: Iss. 2, Article 7. Available at: http://scholarworks.lib.csusb.edu/ciima/vol4/iss2/7
6. D'Arcy J, Hovav A, Galletta D. User awareness of security countermeasures and its impact on information systems misuse: a deterrence approach. Information Systems Research 2009;20(1):79-98
7. Da Veiga A, Eloff }HP. A framework and assessment instrument for information security culture. Computers & Security 2010; 29:196-207
8. Deursen, N., Buchanan, W. and Duff, A. (2013).Monitoring information security risks within health care, Computers & Security, 37, pp 31-45
9. Furnell SM, Gennatou M, Dowland PS. A prototype tool for information security awareness and training. Logistics Information Management 2002;15:352-7
10. HIPPA Regulatory Alert (February 2011). Importance of security risk assessment and hospital access management. Healthcare risk management, pp. 1-3.
11. Juhee Kwon and M. Eric Johnson, "Security Practices and Regulatory Compliance in the Healthcare Industry" (July 29, 2012). AMCIS 2012 Proceedings. Paper 3. http://aisel.aisnet.org/amcis2012/proceedings/ISHealthcare/3
12. Kulynych J, Korn D. The effect of the new federal medical-Privacy Rule on research. New England Journal of Medicine 2002;346: 201-4.
13. Liginlal, D., Sim, I., Khansa, L. Paul, F. (2012). HIPAA Privacy Rule compliance: An interpretive study using Norman's action theory, Computers & Security, 2012; 30: 206-220
14. Love, V.D. (November-December 2011). IT security strategy: is your healthcare organization doing everything it can to protect patient information? Journal of Healthcare Compliance, pp. 21-64.
15. McFadden KL, Towell ER, Stock GN. Critical success factors for controlling and managing hospital errors. Quality Management Journal 2004;11(1):61-4.
16. Montanan, M., Chan, E., Larson, K., Yoo, W. and Campbell, R. (2013). Distributed security policy conformance, Computers &Security, 33(2013), 28-44
17. Posey, C., Bennett, R., and Roberts, T. (2011). Understanding the mindset of the abusive insider: An examination of insiders' causal reasoning following internal security changes, Computers & Security, 30, pp 486-497
18. Sipponen, M., Vance, A. (2010). Neutralization: new insights into the problem of employee information systems security policy violations. MIS Quarterly, 34(3), pp. 487-502
19. Weinstein A. The bandwagon is outside waiting. Health Management Technology 2001;22(5):50-2.
20. Willison, R., Warkentin, M. (2013). Beyond deterrence: an expanded view of employee computer abuse. MIS Quarterly, 37(1), pp. 1-20
21. Xue Y, Liang H, Wu L. Punishment, justice, and compliance in mandatory IT settings. Information Systems Research, 2011;22(2):400-14