Issues in Information Systems

Volume XII, No. 1, pp. 224-236, 2011

SECURITY AWARENESS FOR HEALTH CARE INFORMATION SYSTEMS: A HIPAA COMPLIANCE PERSPECTIVE

Sushma Mishra, Robert Morris University, mishra@rmu.edu
Gregory J. Leone, Robert Morris University, leone@rmu.edu
Donald J. Caputo, Robert Morris University, captuo@rmu.edu
Robert R. Calabrisi, Robert Morris University, calabrisi@rmu.edu

ABSTRACT

The purpose of this paper is to understand the state of security awareness and preparedness for health care organization with regards to compliance with HIPAA security rule. A survey instrument was developed pertaining to strategic, managerial, training, awareness and communication issues in security management. A total of 64 usable responses were received and analysis was performed. The results show an overall agreement of the population with security measures. There are certain areas of concern identified that need to be further studied. Contributions are listed and future research directions identified.

Keywords: health care information systems, security, privacy, HIPAA, electronic medical records, compliance

INTRODUCTION

The advancements in electronic health could impose several challenges in terms of patient privacy and security of information in the healthcare systems. An electronic health record is a collection of medical information about individual patients and populations stored in an electronic format. It may contain personally identifiable information about a patient such as social security number, home address and also health related details [6]. There have been several medical security breaches reports in the news and implications of such damages for patient vulnerability are unprecedented. The Privacy Rights Clearinghouse [15] in California maintains a database of reports on breaches culled from the media and websites. One of the most widely reported security breaches occurred in 2006, when records of 2.65 million veterans were stolen from a Veterans Administration employee working from his home. It listed 184 medical data incidents in 2009 and 2010 involving the records of 5.2 million people. As personal medical information is being entered, processed, stored and transmitted electronically, new threats to the protection of individuals' rights to privacy are becoming evident [6]. There are several benefits associated with shifting to electronic records from paper based systems but it is important that measures be instituted to ensure privacy and confidentiality of medical records. The introduction of the Privacy and Security Rules of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 is a giant step by Federal Government to establish some guidelines for patient privacy and security of medical records.

This study is intended to determine the level of HIPAA related security established by medical personnel.

In order to achieve the results five research questions were developed and analyzed. The research questions were the following:

RQ1: Does your organization have a strategy related to HIPAA compliance?

RQ2: Is your organization proactive in its efforts to maintain information security?

RQ3: Are there training procedures for proper computer use relating to information security?

RQ4: Is the awareness of information security established through proper procedures?

RQ5: Does the organization communicate the need for information security adequately?

Considering the HIPAA compliance requirements for health care organizations, a survey was prepared to study and compare awareness about security and privacy issues across four separate, distinct groups of stakeholders: 1) student trainees 2) administrators 3) ancillary service providers and 4) direct care providers. The intent was to gain quantitative data and analyze the results concerning the awareness of these groups on different aspects of security issues for electronic health records. For the purpose of this study, the data discussed was drawn from a sample taken from students from three different universities pursuing different health care degrees.

LITERATURE REVIEW AND RESEARCH METHODOLOGY

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandates that the privacy, security and electronic transaction standards for maintaining the patient information for all healthcare providers. HIPAA basically targets two goals [6]: insurance flexibility (electronic record can be easily accessed and transferred and thus would prevent refusal of coverage due to change of jobs) and administrative ease (reducing healthcare cost due to standardizing the transactions.) Hence electronic data interchange is an important element in assisting the organizations to meet with high patient load and enhance business partner relationships in healthcare organizations. HIPAA seeks to validate and assist with the inevitability of electronic data transactions, while also addressing privacy and security issues that may stem from converting to the use of vulnerable electronic transactions [6].

HIPAA safeguards the privacy of medical records of patients by preventing unauthorized disclosure and improper use of patients' Protected Health Information (PHI). With a significant emphasis and monetary investment in the 1990s on the computerization of health services operations, the possibility of data manipulation and nonconsensual secondary use of personally identifiable records has tremendously increased [3]. HIPAA declares PHI "privileged," protecting individuals from losses resulting from the fabrication of their personal data. Businesses subjected to HIPAA are directed to protect the integrity, confidentiality, and availability of the electronic PHI they collect, maintain, use, and transmit.

The Security Rule requires compliance actions in the following categories:

(1) Administrative safeguards— this requires formal practices to manage security and personnel from the healthcare service provider side. Ensuring right administrative safeguards entails a right approach to governing the information security of the organizations, putting right controls in place and frequently monitoring and upgrading such controls.

(2) Physical safeguards—an important piece of the security solution of an organization lies in physical protection of the data including the computers in which it resides and the premises where it resides. This would entail creating right physical security controls in the form of authorizations for physically accessing the computers and premises and taking care of the data in form of trash from printed documents with requisite importance.

(3) Technical safeguards—securing the information technically requires creating detailed access control mechanisms to monitor information access. It is also important to make sure that the data in transit (moving from one point to another in the healthcare circle) is secure.

(4) Organizational requirement—formal management of security needs at an enterprise level makes sure that the employees understand the implications of the seriousness of the data that they deal with on a daily basis. It implies that employees should have explicit business associate contracts to agree upon the role that is required for them.

(5) Policies and procedures and documentation requirements—right security policy and procedure are in place to protect the data.

Meeting the security rule requirements entails coming up with a comprehensive security plan that has detailed procedures for addressing risks at several levels in the organization and proactively deals with those risks. Examples of steps in the plan include establishing security certification processes for employees and contractors, updating employee records to indicate the level of security appropriate to each job position, assessing the compliance of the Management Information Systems (MIS) department with the Security Rule standards, and explicitly stating consequences for noncompliance with new security rules [6].

Transaction: various participants in the healthcare industries must effectively and electronically communicate patient information. Successfully meeting this requirement necessitates the privacy and security covenants also be met.

There has not been considerable research in understanding the security requirements for healthcare information systems. Heath care organizations are not proactive in adopting security requirements [24]. Research literature in information security identifies several factors instrumental in overall providing of security to organizations: awareness [19, 23], effectiveness [18], culture [20], behavior [5, 21], deterrence [8, 27], training [22], communication [22], and compliance [8, 27].

HIPPAA compliance allows organizations to prioritize security preparedness to prevent damage to reputation. Also, the federal government has initiated a comprehensive HIPAA security rule audit of covered entities with penalties in case of non-compliance. There is increasing pressure for health service providers to ensure compliance with security rules. The passage of the Health Information Technology for Economic and Clinical Health (HITECH) Act on February 17, 2009, as part of the American Recovery and Reinvestment Act (ARRA) of 2009, has substantially altered and extended the HIPAA Security Rule compliance requirements [6]. Brady (2011) argues that security awareness, security behavior and management support influences security effectiveness and culture leading to better HIPAA compliance. In a study, the author finds empirical support to claim the relationship between security culture and effectiveness to compliance initiatives.

The impetus from federal and state government towards digitization of patient health records is aimed at avoiding errors in medical judgments from heath care providers, reducing cost of the healthcare delivery and improving overall care for the patient [17]. Increasing popularity and adoption of Electronic medical records (EMR) is geared towards improving quality of healthcare provided in the country through better patient communication, integration of disparate records and accessibility and aggregation of records to provide holistic health profile for a patient [17]. Such benefits are not without associated risk of exposure of personally identifiable information and compromise in digital health data resulting in patient anguish and provider embarrassment. It is crucial that provider utilizing EMRs must address the challenges to security and privacy issues of EHR. The anecdotal evidences about medical security breaches suggest a rather weak preparedness on the part of the heath service providers in governing security of health data. Based on research on HIPAA compliance requirements for health care service providers, a questionnaire was developed.

Respondent Groups

Major Medical Centers across the Unites States offer a wide variety of services for inpatients and/or outpatients to the population served. Services include but are not limited to Nuclear Medicine, Inpatients and/ or Outpatients, Pharmacy Services, Surgical Services Sub-Specialty Services, receptionist, greeters, and insurance staff for billings, Administrative Leadership, and more. To organize these services, the medical centers further group those areas into categories. The categories are: Direct Patient Care, Ancillary Support Services, Administrative and Student Training programs.

Direct Patient Care Providers (hereby referred as group 60) are those who **have "**Hands-on or face-to-face contact with patients"[14]. There are many staff members who are involved with this level of care. These persons are mostly comprised of medical doctors, professional nursing staff, paramedics and even those in an emergency department that are able to triage patients. "It also might include police or other persons, such as volunteers, who routinely

work in health-care settings and have hands-on or face-to-face contact with patients." This should not be confused with those providers that are staff who work in an office setting "even if the office is located in a hospital or clinic."

Additionally, located in clinics and or hospital settings are those professional staff who perform support to the patient but are not categorized as "Direct Patient Care Providers". The section of professional staff is grouped in a category called the Ancillary Support Services (hereby referred to as group 70). Services that fit into this category do not include room and board, and the medical and services that are provided by nursing during while the course of care [15].

The administrative areas within the medical centers are those that include the executive leadership. It is often stated that "The administrative service (hereby referred to as group 80) remains behind the scenes, and makes it possible for health care organizations to operate." This also entail the business section of the medical center. "According to the Princeton Review, administration is responsible for overseeing health care regulations and compliance; evaluating the need for personnel, equipment and office space; setting budgets; and allocating money. Health care administrators make major decisions about the direction of their health care organizations [16].

Some medical centers are used for training student nurses and or other healthcare providers (normally the residents and interns are at the Direct Care Level) and are part of a 4th category. This category (hereby referred to as group 90) can also be considered as an entery level or apprentice level. It can include any persons that may require training for any supportive position as stated above such as nursing, etc.

DATA COLLECTION AND CONTEXT

The target population of this study was Master's and Doctoral students in the school of nursing of three universities in the northeast region of USA. A paper based survey was conducted. There were 64 responses for the survey. The respondent profile could be described as: all the respondents have work experience in health care industry and a majority (>60%) of them had more than one year relevant experience (see table 1).

Table 1: Respondent Profile: years of service

Years of service in the healthcare industry		
	Total Responses	Percentages
Less than 1 year	24	38.71
1-5 Years	15	24.19
6-10 Years	9	14.51
11-15 years	5	8.06
16 or > years	9	14.51

A majority of the respondents are working in computerized (partially or fully) health care facilities (see table 2).

Table 2: Respondent Profile: computerization

Computerization of Patient Records		
	Total Responses	Percentages
Completely computerized	26	43.33
Partially computerized	32	53.33
Paper based system	2	.033

A majority of the respondents have an undergraduate degree (50%) followed by Masters degree (41.93 %). About 5 % of the respondents hold a doctoral or equivalent degree (see table 3) and work primarily in administrative roles in health care organizations. This suggests a mature and educated set of respondents.

Table 3: Respondent profile: Education

Current Education Status		
	Total Responses	Percentages
High School	2	3.22
Undergraduate Degree	31	50.00
Master's Degree	26	41.93
Doctorate or Equivalent	3	4.83

For gender composition, 62.5 % of the respondents were female and 37.5% were male. Majority of the respondents (52.45%) belonged to the age group of 20-30 years followed by (16.39%) each for the age group 31-40 and 41-50 (see table 4). The remaining respondents belonged to an age group of 50-60 years.

Table 4: Respondent profile: Age

Age		
	Total Responses	Percentages
20-30 Years	32	52.45
31-40 Years	10	16.39
41-50 Years	10	16.39
50 Years or greater	9	14.75

The data from the survey were imported in SPSS for analysis.

DATA ANALYSIS AND DISCUSSION

RQ1: Does your organization have a strategy related to HIPAA compliance?

A Likert scale from 1 strongly agree, 2 agree, 3 tend to agree, 4 disagree, 5 strongly disagree for each survey question was analyzed. The following analysis determined the findings of the study. Arithmetic means were developed to determine results for each research question. Any mean with 2 or greater indicated a significant response of negativity to the question, indicating that several respondents indicated that they disagree or strongly disagree regarding the survey question. In addition to the entire population, medical personnel were aligned into four groups that represented their occupational specialty (see table 5).

Table 5: Research question 1 with all items

Research Question 1	All	Means by Group			
		60	70	80	90
1) In my organization, there is a predefined agreed upon plan for security and privacy compliance efforts	1.41	1.53	1.50	**1.32**	1.43
2) There is a prevalent security culture where individuals look out for each other in my organization	2.06	2.24	2.25	**1.87**	2.33
3) Creating security awareness is an ongoing process in my organization	1.88	2.00	2.38	**1.67**	2.00
4) There is visible leadership about seriousness of security assurance efforts in my organization	1.85	2.06	2.00	**1.65**	2.17
5) In my organization, there are adequate internal controls (policies, procedures, training, encryption, access restrictions) to provide security and privacy of health records	1.69	1.71	2.13	**1.50**	1.69
6) Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	1.91	1.88	1.83	**1.83**	2.43

The survey results for the first 6 questions indicated a positive response among the entire population. Any mean with less than 2 indicates positive agreement. The question 2 relating to a security culture had the highest negative score indicating respondents negative feelings. This could be due to lack of understanding of the concept of security culture or the absence of it. Answers to question 1 indicated that virtually all respondents felt there is a predefined plan for security and privacy. Group 80, administrators, scored the lowest means compared to an overall score of the population. This finding is consistent with the role of administrators in ensuring a strategic plan for compliance. Group 90, student trainees, had the highest mean in all the four groups indicating lack of involvement and awareness of trainees in strategic planning for security. Research in this area suggests the importance of strategic planning for compliance [9]. Auditing has been emphasized in security literature as an important step in planning for security [10].

RQ2: Is your organization proactive in its efforts to maintain information security?

The specific issues related to this question include security policies and procedures in place and their accessibility to all the employees. Are their auditing policies in place and is the process understood and well communicated? Are violations to the security policies clearly established? These policies should include employee violations that could result in suspension and loss of information technology privileges. Worst cases could result in civil or criminal procedures.

The survey questions used to answer RQ2 follows:

Table 6: Research question 2 with all items

Research Question 2	All	Mean for groups			
		60	70	80	90
7) Security policies and procedures are easily accessible and comprehendible in my organization	1.95	2.17	1.63	1.81	2.43
8) In my organization, there is an emphasis on establishing open communication channels about security issues without the fear of reprisal.	2.06	2.12	1.88	2.00	2.43
9) We emphasize having informal meetings and discussions about importance of managing security and privacy of the records in my organization	2.49	2.67	3.00	2.34	2.00
10) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as a necessary component for security	1.44	1.28	1.86	1.32	2.00
11) Access to the system is based on the role that I play in the organization	1.68	1.59	1.75	1.55	2.43
12) Training about security measures is provided regularly to the staff/personnel in my organization	2.03	2.18	1.88	1.81	3.00
13) In my organization, security policies and procedures are periodically reviewed to assess if the policies meet the changing organizational needs	2.15	2.18	2.14	2.03	2.67
14) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	1.72	1.59	1.63	1.73	2.14

Even though the means continued to indicate a positive agreement among the respondents, there definitely was an indication about some dissatisfaction regarding the organizations commitment to information security (see table 6). Question 12 and 13 and 14 had several respondents indicating a negative response. There is strong indication that there are some failures relating to information security policies and how they are communicated among the general employee population. Question 9 has the highest overall mean in this group of questions, suggesting lack of informal communication with employees about security requirements. In the long run, such delineation of employees from security efforts could hurt the organizations assurance for security information. Robeznieks (2005) claims that one of the biggest problem with non compliance with HIPAA is "no anticipated legal consequences to noncompliance". The main problem of non compliance with security rule is lack of proactive behavior on the part of health care organizations [26]. In a survey in 2005, 43% of service providers were compliant with security rules of HIPAA [26].

RQ3: Are there training procedures for proper computer use relating to information security?

This question examines the training initiatives established at the medical organizations. Are the controls established by management thoroughly communicated and understood by all personnel?

The survey questions used to answer RQ3 follows:

Table 7: Research question 3 with all items

Research Question Three	All	Mean of Groups			
		60	70	80	90
15) Auditing is viewed as a necessary complimentary action to improve the security initiatives in my organization.	1.84	1.94	2.00	1.58	2.57
17) In my organization, there is an emphasis on establishing open communication channel about security issues without the fear of reprisal	1.61	1.61	1.63	1.41	2.43
19) In my organization, security controls (encryption, access control, password policy, segregation of duty) are viewed as a necessary component for security	1.54	1.78	1.63	1.32	1.86
25) I am required to read the security policies frequently (Quarterly, bi-anually, annually) in my organization	2.23	2.44	2.63	1.90	2.83
32) In my organization, I have frequent communication about social engineering issues and am aware of how such tactics can create vulnerability for our system.	1.34	1.28	1.38	1.27	1.83

Most respondents agreed that training procedures were well established. The high mean score of 2.238 for question 25 indicated the possible failure or reluctance to read the security procedures (see table 7). An organization's security policies are the guide to their security program. Employees need to be encouraged to be aware of such policies and should be in a way encouraged and rewarded for reading such policies.

Having and Davis (2005) in an survey found that 54% of respondents felt that the most effective strategy for limiting threats to security of health records in their facility to be education and support staff. Two main themes consistent in several health care provider surveys about security concerns have been education and adherence issues [13].

RQ4: Is the awareness of information security established through proper procedures?

Are training sessions established and mandated periodically for all personnel. Are training manuals established for information security purposes? Do all personnel readily accept the mandate for continuing education of the security policies?

The survey questions used to answer RQ4 follows:

Table 8: Research question 4 with all items

Research Question Four	All	Mean of Groups			
		60	70	80	90
16) Security policies and procedures are easily accessible and comprehendible in my organization	2.26	2.12	3.13	1.80	3.83
18) We emphasize having informal meetings and discussions about importance of managing security and privacy of the records in my organization	1.59	1.67	1.38	1.50	2.17
21) Training about security measures is provided regularly to the staff/personnel in my organization	2.98	3.39	3.50	2.52	3.43
22) In my organization, security policies and procedures are periodically reviewed	2.81	2.59	2.00	2.97	3.71
24) In my organization, I understand what information I have access to and why?	2.57	2.83	2.88	2.19	3.33
26) I am required to access health information only through approved devices and software in the organization.	2.04	2.00	1.75	2.00	2.71
30) I am allowed to use removable storage media from outside on my machine in the organization.	1.79	1.61	1.75	2.00	1.43
31) In my organization, I am required to take permission to use social networking sites	1.50	1.61	1.38	1.66	1.43
33) I am aware of the procedure about what to do when my system has malware in my organization	1.43	1.41	1.50	1.47	1.86

Questions 16, 21, 22 and 24 had the highest negative score among all respondents (see table 8). Training appears to be inadequate for many employees. There is some indication that training reaches most proficient levels at the start of new regulations but spirals downward after time. Research literature in information systems has consistently identified training as one of the most important ingredient in the success of security programs. Ongoing employee training and education are essential in achieving and sustaining HIPAA compliance. Possible training and awareness methods include computerized training modules, automated training programs, frequent communication and employee recognition for good compliant behaviour [13].

RQ5: Does the organization communicate the need for information security adequately? Organizations need to monitor whether too small or too large a certain percentage of employees never get the message. Communications in most organizations is a problem area. With the tremendous technological capabilities available communication problems should decline significantly.

The survey questions used to answer RQ5 follows:

Table 9: Research question 5 with all items

Research Question Five	All	Mean of groups			
		60	70	80	90
20) Access to the system is based on the role that I play in the organization.	2.14	2.18	2.50	1.82	3.20
23) There exists a clear structure for disciplinary action in case of noncompliance with policies and procedures in my organization.	2.61	2.78	3.00	2.30	3.17
27) I am required to report any misuse of information (that I am in-charge of) or its inappropriate access	1.98	1.89	1.63	2.07	2.89
28) I am aware of the password policy that I have to comply with, in my organization	3.54	3.22	3.50	3.53	4.45
29) I frequently receive communication about acceptable security behavior in my organization	1.93	2.00	2.17	1.76	2.33
34) In my organization, there is an ongoing effort on training and education of employees about security issues.	1.60	1.61	1.75	1.60	1.71

Question 28 had the highest negative score of any question (see table 9). In order to have computer access, individuals must know their password and the procedures relating to password use. Password creation and change policies have been more complex and frequently required. The conclusion from these results infer a dislike of the procedures rather than an understanding and awareness of the policy. It is obvious that anyone using the computer systems must know and understand how to create and use passwords. Rules mandating password creation and use are often disregarded unless software is in place that requires time limits and password creation rules. Da Veiga and Eloff stated that user awareness, education, and training are critical information security components [9]. Medlin suggest more employee training is required for improving employee password selection [23].

Communication and training for employees would be the key in this process of assuring consumers about safety of their information. The most common training methods used by HIPAA employed by respondents are pamphlets, formal classes and informal training and the not-so-common method is computer based training [12]. However this data is from 2002 and much has changed since then including a major rise in electronic medical records. It requires further investigation to see how much computer based training is provided currently.

Organizations have rewritten policies and procedures (74%) for their HIPAA compliance program in light of HITECH [25]. Training for compliance increased in 65% of respondent organizations with internal auditing increased by 36%. Resources have often been cited as most important barrier for full HIPAA compliance [2]. Consumer awareness has also been regarded as a significant step to achieve compliance.

HIPAA compliance and creating a safe IT infrastructure is not a result, it is an ongoing process. Even if an organization is compliant at a given point in time, the challenge lies in establishing a protocol for maintenance and reinforcement of security standards [13]. The importance of internal auditing must be stressed to ensure continued compliance. The Healthcare industry has much to learn from HIPAA as it moves towards integrated electronic health record nationwide. There is considerable debate over whether the security and privacy issues with national integrated health records are a bigger problem currently [2].

Group wise analysis

Table 10: Research questions data- group wise

Means of all Research Questions by Groups					
RQs	All	Groups			
		60	70	80	90
RQ1	1.80	1.73	2.01	1.64	2.01
RQ2	1.94	1.97	1.97	1.82	2.39
RQ3	1.71	1.81	1.85	1.56	2.30
RQ4	2.11	2.14	2.14	2.01	2.66
RQ5	2.30	2.28	2.43	2.18	2.96

For research question 1, which alludes to a strategic plan for security compliance, the overall agreement in entire respondent population was high. This suggests that healthcare organizations do plan for compliance and take this preparedness seriously. Group 80, which comprises for administrators, did the best on this question (see table 10). Research question 2 refers to proactive preparedness of organizations for security, capture of information about security policies, procedures, auditing and culture. The overall mean was low indicating an agreement with the items on this question. Group 90, student trainees, did not have an overall significant score on this question indicating a lack of understanding of this group about proactive measures of the organization. This could be due to lack of proper understanding of processes and procedures due to the nature of their job. Trainees by definition are starters in the organization inexperienced and lack institutional knowledge. For research question 3, training and education, there is an overall agreement about the use of such effort of security management. Group 90 again reached the highest score suggesting lack of training for entry level personnel in such organizations. This might be a problematic area because starters should have more opportunities about training and education than people who have been in organization for years. Research question 4 is about security awareness through various mechanisms in the organization. The overall population has a disagreement with this question with the highest score again by group 90. This is not surprising because a lack of training and education would definitely lead to lack of awareness of about security issues. Finally research question 5 is about communication with employees in health care organization, about security related issues. Again there is a general disagreement in the entire group with group 90 scoring the highest mean. This suggests a serious issue that needs to be looked into immediately. Health care organization should be open about communicating with its employees and explaining the need for various security initiatives. Lack in communication often leads to misunderstanding and creating vulnerability [13].

Contributions and Limitations

This study is a preliminary step towards assessing the preparedness of heath care organizations in meeting security requirements for being HIPAA compliant. This study contributes mainly in three ways. First, it provides a starting point for other studies investigating security HIPAA compliance needs. There are few studies done in security in healthcare context and insights from this study add to the body of knowledge in this area. Second, methodologically the survey instrument created in this study could be used by other researchers. Third, practitioners in the health care industry can use the survey to assess their security preparedness and can find avenues of improvement based on the organization's score on the survey. The study is not without limitations. The most common limitation for a survey based research is common method bias. Also, the respondents were limited to students enrolled in degree programs of the universities where data was collected. Further research could look at data collection from health care service providers.

CONCLUSIONS AND FUTURE RESEARCH

The purpose of this study was to examine security preparedness of health care organization in compliance with HIPAA security rules. The study analyzed survey data from individuals working in health care industry assessing the state of security awareness in such organizations. The respondents were categorized into four groups based on the job description they provided in the survey. The four groups identified were: administrators, direct care providers, ancillary support and student trainees. The data was analyzed to answer five research questions identified at the beginning of the study. For each research question, five or six items were identified. These questions were developed based on the security rule of HIPAA. For each question, the overall mean and group wise mean were calculated and compared. For the most part, the overall means of the items for the entire group seemed significant but there were interesting insights when we compared the means of different groups. Security culture building measures and relevant training seemed inadequate, as were communication and deterrence practices. The message is: there are certain key issues that are not being adequately addressed in health care organizations. The issues such as training, communication, culture and deterrence practices have been identified as important factors for overall effectiveness of security. Further, this preliminary analysis suggests some initial planning points for health care organizations to consider when developing security and assurance plans.

This study is a first step in assessing security awareness and preparedness of health care organizations. It requires significant further development. There are several research directions that stem from this work. First, we could further analyze the data and see if there is a significant difference between the groups of respondents identified here and its relationships with different aspects of security management. Second, more data would be required to study if there is any significant relationship between security awareness and gender, age, education status, or size of health care organization. Third, this study uses constructs of security that have been identified as important for other industries. Even though conceptually it makes sense that health care organizations would have similar security issues, it requires more study to search out specific security measures that are tailored more to health care organizations rather than just any type of organization. Even though the security requirements are the same, relatively little has been focused on the unique managerial, regulatory, and policy challenges found in healthcare [1]. Fourth, a structure equation modeling tool could be used to estimate the relationship between different dimensions of security being studied here and overall security preparedness of organizations.

REFERENCES

1. Appari, A., Johnson, E. and Anthony, D. (2009).HIPAA Compliance: An Institutional Theory Perspective, *Proceedings of the Fifteenth Americas Conference on Information Systems, San Francisco, California August 6th-9th 2009*
2. American Health Information Management Association (AHIMA) 2006. The State of HIPAA Privacy and Security Compliance, Retrieved on 05/11/11 http://library.ahima.org/xpedio/groups/public/documents/ahima/bok1_047499.pdf
3. Baumer, D. L., Earp, J. B., and Payton, F. C. (2000) "Privacy of medical records: IT implications of HIPAA", *ACMComputers and Society*, 30, 4, 40–47.
4. Brady, J. W. (2011) Securing Health Care: Assessing Factors that Affect HIPAA Security Compliance in Academic Medical Centers, In Proceedings of 44th Hawaii International Conference on System Sciences, January 04-07, Kauai, Hawaii USA
5. Choi, Y, Caption, K, Krause, J. and Streeper, M. (2006) Challenges Associated with Privacy in Health Care Industry: Implementation of HIPAA and the Security Rules, Journal of Medical Systems (2006) 30(1): 57-64
6. Dhillon, G. and Mishra, S. "The Impact of Sarbanes-Oxley (SOX) Act on Information Security Governance" In *Enterprise information security assurance and system security: Managerial and technical issues,* Warkentin, M & Vaughan, R. (Eds.), Hershey, PA: Idea Group Publishing, 2006, pp. 62-79
7. Dhillon, G., and Torkzadeh, G. "Value-focused Assessment of information systems security in organizations," Information Systems Journal (16:3) 2006, pp 293-314.
8. Da Veiga, A., and J. H. P. Eloff, "An Information Security Governance Framework", Information Systems Management, 24(4), 2007, pp. 361-372.

9. Drummond, H. "Did Nick Leeson have an accomplice ? The role of information technology in the collapse of Barings Bank," Journal of Information Technology (18) 2003, pp 93-101.
10. Retrieved on 05/12/11 ftp.cdc.gov/pub/avian_influenza1/Appendix%20section%20of%20notebook/influenza%20glossary%20terms.doc
11. Firouzan, P. and McKinnon, J. (2004).HIPAA Privacy Implementation Issues in Pennsylvania Healthcare Facilities, Perspectives in Health Information Management, v1, Retrieved on 05/11/11 http://perspectives.ahima.org/index.php?option=com_content&view=article&id=76:hipaa-privacy-implementation-issues-in-pennsylvania-healthcare-facilities-&catid=44:hipaa&Itemid=89
12. Having, K. and Davis, D. (2005).HIPAA Compliance in U.S. Hospitals: A Self-Report of Progress Toward the Security Rule, Perspectives in Health Information Management, Retrieved on 05/11/11 http://perspectives.ahima.org/index.php?option=com_content&view=article&id=88&Itemid=56
13. Retrieved on 05/12/11 http://www.mondofacto.com/facts/dictionary?ancillary+services%2C+hospital (12 Dec 1998)
14. Retrieved on 05/12/11 http://www.ehow.com/facts_6858560_define-healthcare-administration.html
15. Retrieved on 05/12/11 http://www.privacyrights.org/Identity-Theft-Data-Breaches
16. Jha, A.K., DesRoches, C.M., Campbell, E.G., Donelan, K., Rao, S.R., Ferris, T.G., Shields, A., Rosenbaum, S., & Blumenthal, D. (2009). Use of electronic health records in U.S. hospitals. *The New England Journal of Medicine, 360,* 1628-1638.
17. Kankanhallia, A., Teo, H., Tan, B., and Wei, K. "An Integrative Study of Information Systems Security Effectiveness," International Journal of Information Management (23) 2003, pp 139-154.
18. Lending, D., and T. W. Dillon, "The Effects of Confidentiality on Nursing Self-Efficacy with Information Systems", International Journal of Healthcare Information Systems and Informatics, 2(3), 2007, pp. 49-54, 56-64.
19. Logan, P. Y., and D. Noles, "Protecting Patient Information in Outsourced Telehealth Services: Bolting on Security When it Cannot be Baked in", International Journal of Information Security and Privacy, 2(3), 2008, pp. 55-70.
20. McFadzean, E., J. Ezingeard, and D. Birchall, "Perception of Risk and the Strategic Impact of Existing IT on Information Security Strategy at Board Level", Online Information Review, 31(5), 2007, p. 622.
21. Mishra, S. and Dhillon, G., (2008), "Defining Internal Control Objectives For Information Systems Security: A Value Focused Assessment", In Proceedings of 16th European Conference on Information Systems (ECIS) June 09-11, Galway, Ireland
22. Medlin, B. D., and J. A. Cazier, "An empirical investigation: Health Care Employee Passwords and their Crack Times in Relationship to HIPAA Security Standards", International Journal of Healthcare Information Systems and Informatics, 2(3), 2007, pp. 39-48.
23. Nash, K., "The Global State of Information Security 2008", CSO Magazine, 2008 October, Retrieved May 11, 2011, from http://www.csoonline.com/article/454939/the-global-state-of-information-security-2008
24. Nicastro, D. (2010) HITECH Survey: Providers Remain Concerned About HIPAA Breach Notifications, Media Health Leaders, Retrieved 05/11/11 http://www.healthleadersmedia.com/content/TEC-246771/HITECH-Survey-Providers-Remain-Concerned-About-HIPAA-Breach-Notifications.html##
25. Robeznieks, A. (2005). Noncompliant and unconcerned: survey finds many not meeting HIPAA security rules, Modern Healthcare, 35(32):33
26. Straub, D. "Coping with systems risk: security planning models for management decision making.," MIS Quarterly (22:8) 1998, pp 441-465.