A Study Of The Security Of Electronic Medical Records Utilizing Six Knowledge Categories And Subjects Demographics

Natalya Goreva, Robert Morris University, USA
Sushma Mishra, Robert Morris University, USA
Peter Draus, Robert Morris University, USA
George Bromall, Point Park University, USA
Don Caputo, Robert Morris University, USA

ABSTRACT

Healthcare employees with their motivation to comply with security policies play an extremely important role in protecting patients' privacy. In this research we attempt to survey the attitude of healthcare employees towards security of Electronic Medical Records. We further review what factors impact their perception of the medical data security and determine how well they understand policies, procedures, organization structures, and other aspects related to EMR protection.

Keywords: Electronic Medical Records (EMR); Security; Healthcare Information Systems

INTRODUCTION

The information security process in healthcare starts not only with the effective leadership and the effective distribution of security policies among all healthcare workers (Love, 2011). It also assumes employees' motivation and effort to comply with the policies (Bulgurcu et al, 2010). While many organizations have material assets to protect, the number one asset of healthcare organizations is highly confidential patients' information stored in Electronic Medical Records (EMR). The question of EMR safety has been raised since the very first instances of computerization in healthcare. According to HIPPA Regulatory Alert of 2011, 70% of healthcare organizations admitted that EMR protection was not a top priority four years in the past. Although this number substantially decreased in the past year, there are still many cases of EMR security breaches, which cost over $6 billion to healthcare organizations (HIPPA Regulatory Alert, 2011). The ubiquitous presence of IT and increasing mobile technologies make the task of protecting EMR extremely challenging (Glaser & Aske, 2010). In many cases the organizations do not realize the cost of data breaches until the loss of information occurs or the vulnerabilities are exploited.

There are strict government regulations that enforce the protection of healthcare records. In addition to HIPPA, there is the 2009 Stimulus Act that requires every heath privacy breach with more than 500 patients involved to be reported to the Secretary of Health and Human Services and become public knowledge. In spite of that, data breaches occur in healthcare on a regular basis. In the Anthem data security breach of 2014 (Hiltzik, 2015) the hackers stole patients' names, social security numbers and dates of birth from Anthem health insurance. Not all attacks are technology-driven: sometimes negligence and failure to comply with security policies can lead to serious security threats, such as the AHMC healthcare data breach in Anaheim, CA, where the attackers stole two laptops with unencrypted data from 729,000 patients (McCann, 2013). Overall, more than 32 million Americans became victims of healthcare data breaches due to thieves, hackers, and employees' negligence (Campbell & Schoch, 2014).

Researchers admit that EMR breaches in healthcare are no longer just an issue of someone hacking into the hospitals' computer system, but also an issue of negligence and non-compliance with security policies (Strauss, 2015), e.g. leaving an unattended laptop or iPad with unencrypted patient data or sending patient's records to a

wrong address. Employee training, communication, and motivation are key factors in preventing data breaches due to non-compliance. When employees receive training and communication, they are more likely to believe that Information Assurance policies are beneficial to all parties involved (Cannoy & Salam, 2010). They improve healthcare employees' beliefs in the importance of EMR security. The research mentioned above leads us to identifying the following three categories of the survey questions:

- Category 3, *Training*.
- Category 4, *Team Work*. We broadened the Communication category and decided to look at team work, which includes communication and the effectiveness of performing the security-related tasks by employees as part of the team.
- Category 2, *Sense of Responsibility*. This category is closely related to the definition of successful training and communication of policies, which should lead not only to employees' understanding that they must comply with the policy, but also their motivation and voluntary compliance described by Bulgurcu et al, 2010 and by Cannoy & Salam, 2010.

The goal of this research is not only to study the opinion of healthcare employees on EMR security, but also to see how their perception varies by their job classification (administrative vs. non-administrative, technical vs. non-technical, etc.). A well-defined organizational structure is extremely important in understanding the roles of healthcare employees. Different groups of healthcare workers occupy different levels of the structure. For example, it is believed that the CIO should be in charge of operations and not security. Nanji (2010) states that operations should be separated from integrity monitoring. Every organization dealing with EMR needs a CIO reporting to CSO and COO (De Haes & Van Grembergen, 2008). Because the CIO is primarily in charge of operations, an additional position of Chief Information Security Officer (CISO) needs to be established for the sole purpose of managing organizational IT security (Nanji, 2010). Based on these findings, we derive the following two categories of the survey questions:

- Category 1, *Reporting Structure*.
- Category 6, *Organizational Control*.

The level of employees' understanding of organizational structure is crucial, and it is one of our research questions. Medium to large size organizations should establish an IT steering committee that includes representatives from different layers of the organization, from management to doctors, nurses, and IT personnel (Glaser & Aske, 2010). The more effective the communication between the organizational layers, the less chance that sensitive data will be compromised. This leads to identifying the 5th Category of the survey questions:

- Category 5, *Knowledge and Understanding* of Security Policies.

HIPPA Regulatory Alerts identifies three main causes of EMR breaches: (1) unintentional employee actions, (2) lost or stolen computer devices, or (3) third party mistakes. These causes are all non-technical and can be prevented by sufficient employee training and their compliance with security policies. While employees are "the greatest assets in the effort to reduce the risk to information security" (Bulgurcu et al, 2010), they need training and motivation to comply with security policies. In conclusion, healthcare employees play a crucial role in IT security and protection of EMR.

RESEARCH QUESTIONS

One of the goals of the study is to review the general attitude of healthcare employees to EMR security and to see how well, in their opinion, the security policies are designed and implemented in their organizations. The following specific research questions emerged in the course of study.

RQ1: *Does the perception of EMR security change with the number of years of employment in healthcare organizations?* Our expectation is, the longer one is employed in healthcare, the more understanding of policies and procedures he or she has, and the more motivation to comply.

RQ2: *Does perception of EMR security depend on the characteristics of a healthcare worker's*

organization, such as the size of the organization and the degree of computerization. The assumption is that the larger the organization, the more structured it is, and the more seriously EMR protection is taken. We also assumed that the higher the degree of computerization, the more attention is paid to security policies.

RQ3: *Is there a difference between various groups of employees' perception of EMR security?* We did not predict any specific answer to this question.

METHODS, DATA COLLECTION AND ANALYSIS

The link to the survey was distributed through Question Pro among 164 healthcare professionals with different levels of experience, from different organizations and occupations in the field. We recruited the sample from the students enrolled in the Graduate and Undergraduate programs in nursing at Robert Morris University. Of all the students that were asked to complete the survey, 126 responded and gave valid answers to the survey questions. The survey included demographic questions and questions related to the respondents' perceptions of EMR security in their organizations. For the purpose of the study we broke the questions into six categories, which emerged from the review of literature as explained in the Introduction:

1. Reporting structure
2. Sense of responsibility
3. Training
4. Team work
5. Knowledge and Understanding
6. Organizational control

Table 1. Employment & organizational details (demographics) of respondents

Number of Years of Employment in Healthcare	
<1	32
1 to <5	41
5 to <10	14
10 to <15	7
15 or more	31
Number of Years in Current Organization	
<1 year	45
1 to <5 years	51
5 to <15 years	23
15 or more years	7
Level of Computerization	
Paper-Based Only	8
Partially Computerized	43
Completely Computerized	74
Role in Organization	
Administrator	12
Nurse	33
Healthcare IT Specialist	5
Physician	0
Other	72
Size of Organization, people	
1-10	12
11-75	16
76-250	17
251-500	16
>500	65

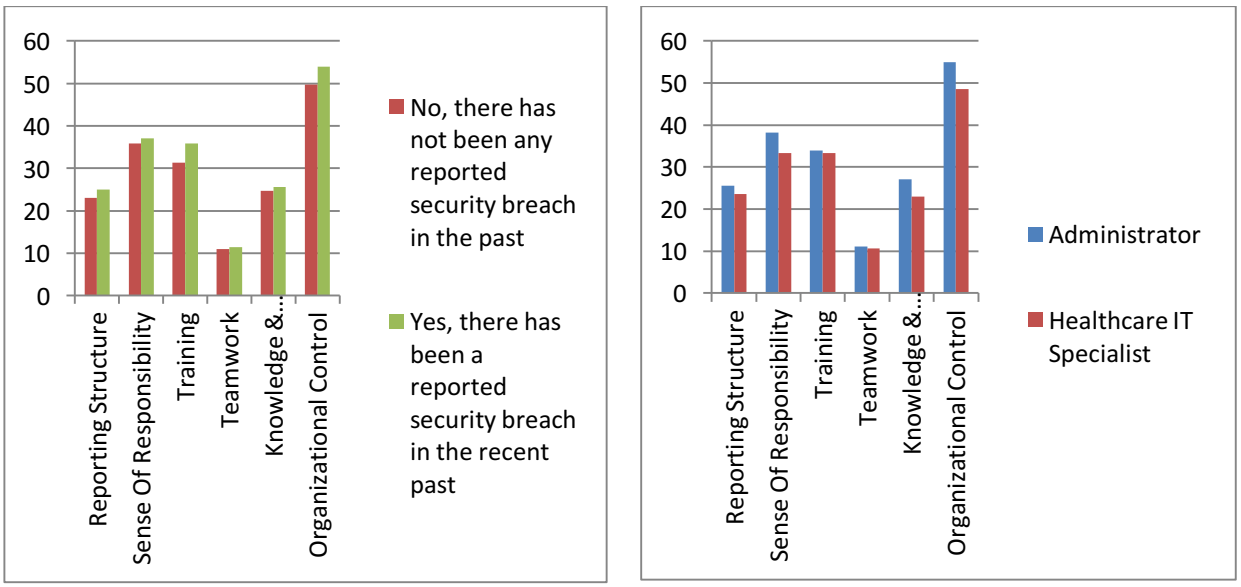
The survey respondents varied in their professional experience in healthcare, from being a new employee to those with 15 or more years of experience in the field. Positions varied from nursing (or a nursing student) to administration. The demographic data about the respondents is shown in Table 1. We used Spearman's Rho to find

out if there is significant correlation between the measurable demographic values (such as duration of employment or degree of computerization) and the answers to the security-related questions. A simple mean comparison and ANOVA were used to determine if the responses were different between the different groups of respondents (e.g. administrators vs. IT technicians). When interpreting ANOVA results we took into account the fact that the dependent variables were measured not by a continuous, but rather on a discrete scale (from 1=Strongly Disagree to 5=Strongly Agree).

FINDINGS

The first group of respondents received the survey in fall 2014 and the second group later in spring 2015. No significant differences were found between the respondents from the two groups, although the first group did include more highly experienced healthcare professionals as compared to the second. We found a difference in perception of EMR security between the respondents who reported that there has been a security breach in their organization, and the group that reported no security breach in their organization. The group that reported a breach ranked all organizational security higher than the other group (Figure 1). There is a possibility that the organizations that have been subjected to cyber-attacks have increased their security measures. When we looked at the security perception scores between the different groups of employees, the highest gap in ranking the security categories was between administrators and the IT specialists, with administrators ranking their organization security noticeably higher than the IT specialists (Figure 1).

Figure 1. Mean comparison between specific groups of employees and organizations



As we used ANOVA to compare the means, the only statistically significant difference between the means in the first case was in training, meaning that the organizations that experienced data breaches in the past provide a more extensive employee training. Knowledge and understanding was the only category with statistically significant differences between Administrative and IT groups' rating, meaning that the IT personnel group admitted having less knowledge and understanding of the security policies. We found a significant difference in the sense of responsibility and the knowledge of security policies among the employees of organizations with different levels of computerization. Those employees who work in highly computerized environments admitted better understanding of security policies and sense of responsibility.

Upon the general review of the scores that the respondents gave to EMR security in all six categories, we observed very high and statistically significant correlation among all categories. In other words, an organization that had a well ordered reporting structure also paid serious attention to training, team work, organizational controls, and other

areas. There were no examples where one aspect of security was valued highly, while some other aspects were ignored. The correlations between the categories varied from 0.6** to 0.907** in Spearman Rho model.

As we predicted at the beginning of the study, the demographic variables such as the number of years of experience in the healthcare field, the size of the organization and the level of computerization should correlate with the respondents' perception of security in the six given categories. Some correlation was found, although not as strong as we expected (Table 2).

Table 2. Correlation with six categories of organizational security

	Time in healthcare	Size of organization	Computerization level	Time with current employer
Reporting_Structure	.139	.170	.222*	.014
Sense_Responsibility	.168	.203*	.121	.086
Training	.109	.182*	.218*	-.024
Teamwork	-.010	.067	.093	-.054
Knowledge_Understanding	.221*	.166	.132	.112
Organizational_Control	.164	.234**	.170	.081

p=0.05 was used in this test

We found the least correlation with the number of years of employment in the healthcare and employment in the current organization. There was only a weak correlation between time employed in healthcare and the knowledge and understanding of the security policies and procedures. This fact is understandable, assuming that the time of employment should not correlate with reporting structure, team work, or organizational control. The new employees or the employees with newly defined responsibilities may anticipate more training, but in general the amount of training remains the same. The sense of responsibility may increase or decrease during employment, but we did not find any particular variations from group to group. We found out that larger organizations pay more attention to developing the sense of responsibility among the employees, provide more training and more organizational controls over security. Highly computerized companies were found to have better reporting and structure and provide better training to their employees. These results are summed up in Table 3.

Table 3. Correlations with specific questions

	Years in healthcare	Size of organization	Computerization level	Years with current employer
Frequently receive security communication	.076	.225*	.118	-.104
Feel accountable to secure data	.158	**.290****	.081	.111
Feel encouraged to work as a team	.078	.183*	.056	.036
Security training is provided regularly	.102	.228*	.213*	-.071
Ongoing security awareness	.130	.195*	.160	.018
Required encryption, access controls etc.	.075	.219*	**.250****	-.010
Required to read security policies	.211*	.143	.135	.061
Required to report information misuse	.145	**.247****	.021	.069
Communicate without fear of reprisal	.045	.189*	.185*	-.066
Clear structure of disciplinary actions	.011	**.241****	.198*	-.097
Understand consequences of inappropriate act	.090	**.236****	.129	.038
Adequate internal controls	.029	.202*	.182*	-.006
Role-based access to the system	.185*	.221*	-.022	.148
Access only through approved devices	.146	**.273****	.064	.117
There is a Compliance Plan	.203*	**.247****	.088	.076
Clear structure in place	.058	.220*	**.347****	-.101
Top management committed to security success	.181*	.096	.151	.062
Clearly understand organizational structure	.216*	.104	.052	.117
Periodic review of security policies	.102	.187*	**.258****	.028
Know what to do with "sensitive" trash	**.310****	**.260****	.059	.215*
Visible leadership in security	.129	.106	.226*	.055
Ongoing training for employees	.178*	**.246****	**.240****	.081

p=0.05 was used in this test

We predicted that the duration of employment will affect the respondents' views on how well EMR security is implemented in their organization. While we found some correlation in this area, it was not as strong as we expected. The correlation with the number of years of employment in the current organization was particularly weak. We found a substantially higher correlation between the organizational size and the employees' ranking of security. The level of computerization, as expected, requires adding some specific regulations, such as encryption and system access control. In addition, we found that the organizations with higher levels of computerization have more clear structure, better training for employees and review of security policies.

	Explanation	Conclusion
RH1	A weak correlation (.221) was found between the duration of employment in healthcare and the understanding of security policies and procedure. There was no significant correlation between the duration of employment in healthcare and the degree of motivation to comply with security policies.	Partially supported
RH2	Organizational size correlates with only half of the six categories; therefore, we made a conclusion that larger size of organization does not necessarily mean increased perception of EMR security. However, employees of larger organization do have increased sense of responsibility and believe that their organization provides higher quality training and organizational control over the security. Similarly, employees in organizations with higher level or computerization believe that they have better reporting structure and better training, but no conclusions can be made about the rest of the six categories.	Partially supported
RH3	There is significant difference between some groups of employees in terms of their perception of EMR security. • IT personnel claimed significantly lower understanding of IT security policies than the Administrators' group. • The group of employees who work in a highly computerized environment admitted significantly better understanding of security policies and better sense or responsibility.	Supported

CONCLUSIONS AND DISCUSSION

In this study we found that the parameters of a healthcare organization correlate with the way EMR security is addressed. In general, large organizations and more computerized organizations are more strict in developing and enforcing security policies and training employees in the importance of compliance with these policies. Administrators admit a slightly higher level of security in organizations than the technical workers; they also admit better reporting structure, training, organizational policies and other categories of EMR security. While the duration (years) of employment and the organizational characteristics correlate with many categories of EMR security, the size of the organization seemed the most important factor in setting high security standards.

In this study we did not ask the respondents the names of the specific organizations where they worked. Knowing the organizations of employment, we can compare the responses of different groups of employees within the same organization; however, many respondents admitted they preferred to not disclose this information. Another concern that we had after analyzing data was that a large group of respondents identified "Other" as their job category. In further research, we intend to break down this group by reviewing the answers and adding more categories to the question. It would be ideal to increase the sample and to make sure that all categories of employees are well represented. For example, even though we had a group of IT Specialists, the size of this group was barely enough to run the tests.

REFERENCES

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly*, 34(3), 523-548.

Center for Healthcare Reporting, California Healthcare Foundation. (2014). Millions of electronic medical records breached. Retrieved from http://centerforhealthreporting.org/article/millions-electronic-medical-records-breached.

Cannoy, S. D. & Salam, A. F. (2010). A framework for healthcare information assurance policy and compliance. *Communications of the ACM*, 53(3), 126-131.

De Haes, S. & Van Grembergen, W. (2008). An exploratory study into the design of an IT governance minimum baseline through Delphi research. *Communications for the Association for Information Systems*, 22(1), 443-458.

Glasser, J. & Aske, J. (2010). Healthcare IT trends raise bar for information security. *Healthcare financial management*, 40-44.
LA Times. (2015). Anthem is warning consumers about its huge data breach. Here's a translation. Retrieved from http://www.latimes.com/business/hiltzik/la-fi-mh-anthem-is-warning-consumers-20150306-column.html#page=1.
HIPPA Regulatory Alert (2011). Importance of security risk assessment and hospital access management. *Healthcare risk management*, 1-3.
Liu, C.H., Chung, Y.F., Chen, T.S., & Wang, S.D. (2012). The enhancement of security in healthcare information systems. *Journal of Medical Systems*, 36, 1673-1688.
Love, V.D. (2011). IT security strategy: Is your healthcare organization doing everything it can to protect patient information? *Journal of Healthcare Compliance*, 21-64.
Healthcare IT News. (2013). HIPPA breach is bad news for 729,000. Retrieved from http://www.healthcareitnews.com/news/HIPAA-breach-brings-bad-news-for-729,000.
Nanji, F. (2010). The BP crisis and information security compliance in healthcare: Parallel disasters? *Journal of Healthcare Compliance*, 15-22.
Strauss, L.J. (2015). Electronic medical records – benefits and liabilities. *Journal of Health Care Compliance*, 17(2), 57-58.

NOTES