THE UNIVERSITY OF ARIZONA | COLLEGE OF MEDICINE PHOENIX

Security and Privacy in Radiology

Betre Workie, Class of 2011

Background

The Health Insurance Portability and Accountability Act (HIPAA) of 1996 mandates privacy and security of Protected Health Data (PHI). Digitization of medical information including radiographic data improved efficiency and productivity, but presented new challenges for privacy and security

Research Question

The goal of this study is to evaluate how secure the current electronic radiology systems are and what individual and systemic factors affect the security and privacy of confidential patient data. We have focused on three aspects of security: physical security, computer systems security and training and prevention.

Research Method

- The research was conducted using an online survey.
  - 25 multiple choice questions: 3 on demographics, 4 on physical security, 9 on computer systems and network security, 5 on training and prevention, and 4 on overall security.
- 77 radiologists and radiology residents from teaching and non-teaching institutions in the Phoenix and Tucson area participated in the survey
  - 70% male and 29% female.
  - 38% in private/group practice, 61% in academic/research setting (31% residents)
- Response rate is unknown since we are able to determine how many radiologists received the invitation to fill out the survey
- The overall security grade given by survey takers to their institution is used as an outcome variable. The responses to the questions in the physical security, computer systems security and training and preventions sections are analyzed using multiple regression to determine how they relate to the overall security grade.

Research Method

The physical security section includes questions on instances where unauthorized person gained access to the facility, whether all entrances to the facility are secured, and whether everyone entering the facility is required to wear an identification badge.

The computer systems and network security section includes question on password usage, sharing and frequency of password reset, locking computer monitors while temporarily away from desk, data backup, and teleradiology.

Training and prevention section includes questions on HIPAA training and refresher courses to radiologist, other security awareness training, and whether the facility does analysis of potential security threats to patient data.

Results – Physical Security

variable	Coeffici ent	std. error	std. coeff	t-value	P-value
Intercept	6.27	1.11	0.27	5.63	<0.0001
Entrances secured	-0.37	0.25	-0.18	-1.45	0.153
Unauthorized entry	1.47	0.43	0.38	3.44	0.001
Id required	-0.24	0.22	-0.13	-1.07	0.29

Table 1: Regression analysis of overall security grade vs. physical security variables.

Count	R	R^2	ANOVA P-value
73	0.481	0.231	0.003

Table 2: Regression summary table for physical security section

Among the three questions included in the physical security section, only one, the question about unauthorized entry to the facility, predicted the overall security grade in a significant manner (p = 0.001).

The R^2 analysis shows that 23% of the variation in the overall security grade can be explained by the variations in the independent variables included in the analysis of physical security and this is significant (p = 0.003).

Results – Computer Systems Security

Variable	Coeffici ent	std. error	std. coeff	t-value	P-value
Intercept	14.16	2.96	14.16	4.79	<0.0001
Unique login password	-2.29	1.2	-0.23	-1.9	0.062
Reset login password	-0.36	0.25	-0.2	-1.43	0.158
Lock comp screen	1.17	0.37	0.42	3.19	0.002
Freq of data backup	0.04	0.09	0.06	0.47	0.642
Ever disable security feature	-0.5	0.86	-0.07	-0.58	0.563
Audit log generation	0.2	0.19	0.14	1.07	0.288
Work remotely	0.4	1.39	0.04	0.29	0.777
Use VPN	-0.18	0.87	-0.03	-0.21	0.836

Table 3: Regression analysis of overall security grade vs. computer systems and network security variables.

Count	R	R^2	ANOVA P-value
71	0.459	0.21	0.129

Table 4: Regression summary table for computer systems security section

Among the nine question included in the computer systems and network security section, only one, question asking about locking computer screens while temporarily away, predicted the outcome in a significant manner (p = 0.002).

The R^2 analysis shows that 21% of the variability in the outcome is predicted by variability in the variables analyzed in the computer systems and network security section and this is not significant (p = 0.129)

Results – Training and Prevention

Variable	Coeffici ent	Std. error	std. coeff	t-value	P-value
Intercept	6.78	1.18	6.78	5.73	<0.0001
Security Training	-0.29	0.28	-0.13	-1.02	0.311
Security threat analysis	0.07	0.15	0.06	0.48	0.634
HIPAA training	1.61	0.9	0.22	1.67	0.1
HIPAA refresher	-0.22	0.17	-0.18	-1.23	0.194

Table 5: Regression analysis of overall security grade vs. training and prevention variables.

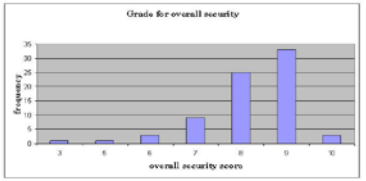
Count	R	R^2	ANOVA P-value
72	0.288	0.083	0.449

Table 6: Regression summary table and ANOVA P-value for training and prevention section

- None of the variables in the training and prevention section predicted the overall security grade in a significant manner.
- The R^2 and analysis of variance also show no significant relationship between the overall security grade and other independent variables.

Distribution of overall security grade of participating institutions as ranked by survey takers

(10 – completely secured, 0 – completely unsecured)



Conclusion

- Analysis of the answers to the individual survey questions suggest that the security threat level to current radiology systems is very low.
  - Only 18% of the participants reported that they have identified security gaps in their facility and almost all of them reported that those gaps have been fixed.
- The following data sets are of concern.
  - Only 8% of the respondents always lock their computer screens when temporarily away from their work station.
  - As many as 12% of the respondents reported that they do not anonymize patients' private information when sharing images with an unauthorized person.
  - When asked whether all individuals entering their facility are required to wear an ID badge, 34% answered no.
- This indicates that although the current security threat level is low, the preparedness of these institutions to defend future security attacks is not adequate and there is room for improvement.
- As far as maintaining sensitive patient information private, most of the institutions who took part in this study seem to be doing a good job.
  - 96% of the respondents have had HIPAA training and more than 90% of them get a HIPAA refresher course at least once every 5 years.

Future Direction

- Questions about type of antivirus software used, firewall, data encryption, data storage etc. were not included in this survey because these questions are best answered by chief information officers (CIO) and not by radiologists, future research in this area should include CIO's in the study.
- Other possible improvements to this study are:
  - Increasing the sample size
  - Comparing security technologies used by different facilities
  - Implementing one simple solution to existing security gap and measuring the outcome.
- The ultimate test to security of computer systems will be trying break or hack into the network by hiring a professional computer hacker.
  - This requires permission from appropriate authorities and approval from IRB committee.