Securing Health Care: Assessing Factors that Affect HIPAA Security Compliance in Academic Medical Centers

James W. Brady, PhD
Nova Southeastern University
bradjame@nova.edu

Abstract

HIPAA security compliance in academic medical centers is a central concern of researchers, academicians, and practitioners. Despite increasing accounts of data security breaches, greater numbers of information technology implementations, and new HIPAA Security Rule requirements and audits, academic medical centers have shown limited HIPAA security compliance. Based on a literature review of technology acceptance and security effectiveness, this study investigated the factors that affect HIPAA security compliance. A theoretical model using management support, security awareness, security culture, and computer self-efficacy to predict security behavior and security effectiveness was proposed. Multiple linear regression and correlation analysis demonstrated that security awareness, management support, and security culture were significant predictors of security effectiveness and security behavior, with security awareness being the most significant predictor. The results of this research provide guidance to those involved with HIPAA security compliance initiatives in health care.

1. Introduction

Academic medical centers (AMCs) and other covered entities in the U.S. are not fully complying with the Health Insurance Portability and Accountability Act (HIPAA) of 1996 [26]. Based on the results of the 2008 Centers for Medicare & Medicaid Services (CMS) HIPAA security compliance reviews, covered entities have struggled to comply with the Security Rule [11]. Concerns about security of patient health information (PHI) therefore remain more than a decade after the passage of HIPAA.

According to Herold, data security breaches in health care organizations continue to increase [24]. Numerous AMCs reported data security breaches in 2009 and 2010 [15]. The slow adoption of information technology (IT) has been reported as an internal weakness within health care organizations [22]. As a result, the health care industry has been viewed as a laggard in terms of technology adoption.

As stated by Nash, health care organizations typically address security requirements reactively [39]. Logan and Noles noted that such organizations do not always consider security when implementing new products and services [35]. Further, computer security has often been implemented as an afterthought [36]. Additionally, shortcomings in the HIPAA Security Rule relating to business associates, breach notifications, data transmission standards, investigation of complaints, and penalties and enforcement have created liabilities for health care organizations [5].

Literature on HIPAA and information security has identified a number of factors that contribute to security behavior and security effectiveness. These factors include management support [35], security awareness [32, 38], security culture [36], and computer self-efficacy [7, 32, 53]. Additionally, security effectiveness [14, 21] and security behavior [37, 43] were found to be valid predictors of each other as well as of HIPAA security compliance [29, 45].

2. Literature review

2.1. HIPAA security rule

Information security and privacy are major concerns in the health care domain [27]. According to the 2009 HIMSS Security Survey, one-third of the 196 respondents reported that their organization had at least one known case of medical identity theft, with only one-half having a plan in place for responding to security breach threats or incidents [18]. The 2009 Ernst & Young Business Risk Report identified regulation and compliance as the only critical risk in the Life Sciences area [17]. Based on the 2009 Computer Security Institute (CSI) Computer Crime and Security Survey of 443 information security and information technology professionals in the U.S., Peters reported that theft of PHI through all causes other than mobile device theft was the second most expensive security incident, with losses reported at $710,000 [44]. Therefore, in addition to complying with HIPAA regulatory requirements, health care organizations must prioritize data security breach prevention to reduce damage to their reputation.

As a result of the rapid adoption of health information technology and an increasing dependency on electronic medical records, Li and Shaw indicated...
that a wide range of security concerns must be addressed [33]. As a consequence, health care leaders are under continued pressure to ensure compliance with the HIPAA Security Rule. Additionally, the federal government recently initiated a comprehensive HIPAA Security Rule audit of covered entities, with stringent financial penalties issued for noncompliance [26].

New federal regulations and state laws have significantly increased the requirements of the HIPAA Security Rule and the consequences for noncompliance [3]. 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 [3]. Consequently, there is a need to investigate HIPAA security compliance in health care organizations, specifically in AMCs that represent the leading U.S. medical schools, teaching hospitals and health systems, and academic societies.

2.2. Security behavior

More attention needs to be given to the social and behavioral aspects of information security among AMCs. Numerous user acceptance models have been identified in the literature, including the Technology Acceptance Model (TAM) and TAM2 [50]. However, further research on the generalizability of factors associated with technology acceptance (TA) and user behavioral studies is needed particularly in the domain of information security [21, 41]. Many information security breaches in the workplace have been attributed to the failure of employees to comply with organizational security policies [7]. As a result, more attention was reported as needed to learn why noncompliant behavior takes place so that appropriate measures for curbing the occurrence of such behavior can be found.

Security behavior has been determined to be a key factor affecting health care organizations’ security effectiveness and HIPAA security compliance. A study of 104 employees from two IT intensive organizations in the logistics and petrochemical industries found that breaches in security generally result from noncompliant employee behavior [7]. Johnston and Warkentin reported that perceived organizational support and self-efficacy exerted a positive influence on HIPAA compliance behavioral intent [29].

2.3. Security effectiveness

A better understanding of information security effectiveness among AMCs is needed. Understanding the factors affecting the effectiveness of security countermeasures has been a consistent theme in the literature [9, 31]. Information security effectiveness has been seriously questioned due to the continued high volume of security-related incidents and subsequent financial losses [8]. Therefore, health care management needs to give more attention to developing effective security policies to address HIPAA Security Rule compliance.

Security effectiveness has been frequently reviewed in the IS security literature. Straub referred to IS security effectiveness as the ability of IS security measures to protect against the unauthorized and deliberate misuse of assets of the local organizational information system by individuals, including violations against hardware, programs, data, and computer service [48]. The theory of IS security effectiveness was advanced by developing and testing an integrative model of IS security effectiveness [30]. Chang and Lin found that organizational culture and management support had a positive influence on security effectiveness [9]. Further, Chang and Lin determined that effectiveness was significantly correlated to confidentiality, integrity, and availability. The HIPAA Security Rule specifies that each covered entity must ensure the confidentiality, integrity, and availability of ePHI that it creates, receives, maintains, or transmits.

2.4. Management support

Better understanding of management support for information security among AMCs is needed. The roles and responsibilities of board members and senior executives for information security have received little attention in the academic literature to date [37]. Many of the existing studies on the influence of top management support on technology adoption suffer from diverse and inconsistent conceptual definitions, weak measures, and insufficient theorization [40].

Management support is a major factor affecting secure compliance [16]. Da Veiga and Eloff identified executive level sponsorship of information security and commitment from the board and management to protect information assets as critical information security components. Top management support was found to be crucial in supporting security legislation such as the HIPAA Security Rule [36]. Poor implementations of information security resulted from a lack of authority, lack of executive support, and lack of understanding the importance of information security. Nevertheless, it was found that executive level management increasingly recognizes the value that information security brings to the organization.

Management support is important to achieving security effectiveness [8]. Top management support
was shown to positively influence four variables of security effectiveness: user training, security culture, policy relevance, and policy enforcement [31]. Top management should act as a champion of change in creating an organizational environment conducive to security goals. Smith and Jamieson investigated the key drivers and inhibitors affecting IS security success and security compliance [46].

2.5. Security awareness

Despite the recent increased attention afforded to security incursions, there is a lack of user awareness and understanding of information security reported in the literature. According to Pattinson and Anderson, instead of addressing only the technical aspects of network security issues, attention needs to be paid to user awareness and behavior as a central focus of an information security strategy [43]. As indicated by Williams, a more comprehensive and encompassing approach to security that includes awareness is required [51].

Security awareness is a key factor in attaining HIPAA security compliance. In an exploratory study of 80 students in a nursing school located in Central New York State, researchers found that better delineation of training requirements by policy makers and the inclusion of clinical caregivers in developing the training materials and processes were needed [28]. A study of 90 employees in a single health care agency determined that more employee security training was needed to improve employee password selection procedures [38].

Da Veiga and Eloff stated that user awareness, education, and training are critical information security components [16]. Hale and Brusil reported that, because a large part of security management must consider human vulnerability, enterprises must not overlook the importance of educating people about their personal role in providing and maintaining security [20]. Additionally, Chang and Yeh noted that effective information security should consider both technical and non-technical security threats [8]. Security awareness, therefore, is an important determinant in achieving security effectiveness.

2.6. Security culture

More attention needs to be paid to the information security culture. Additional research on the social and cultural aspects of employees’ workplace interactions with each other and with technology was reported as an issue [19]. The study reported that organizational subcultures caused conflict and affected compliance behavior within different departments.

Security culture has been found to play a significant role in information security compliance [36]. Winkel defined security culture as the system of collective moral concepts, mindsets and behavior patterns anchored in the self-conception of a social unit and instructing its members in dealing with security threats [52]. Rotvold reported that security culture was determined to exert a positive influence on security compliance [45].

Chang and Lin examined the influence of organizational culture on the implementation of information security management [9]. The authors concluded that an appropriate and effective information security management implementation requires a combination of favorable organizational culture. Further, competent information security technology and management’s supportive attitude toward information security were noted as important.

2.7. Computer self-efficacy

Research on the factors associated with self-efficacy in AMCs is warranted. According to Lending and Dillon self-efficacy refers to a user’s confidence that he or she has the ability to use an information system [32]. Womble concluded that the literature has shown that users with high information and self-efficacy will perceive IT as a useful and resourceful tool and will, therefore, remain compliant with federal and state requirements [53].

Self-efficacy is a valid predictor of information security behavior. Self-efficacy was reported to positively influence employees’ compliant behavior and depend on a combination of organizational and personal factors [7]. The study found that compliant behavior was promoted by increasing employees' self-efficacy and enhancing perception of information security climate. According to Compeau and Higgins, researchers generally agreed that a positive relationship existed between CSE and IS use, and that understanding CSE was important to the successful implementation of systems in organizations [13].

D’Arcy and Hovav noted that research on computer self-efficacy suggests that there is a significant relationship between perceptions of self-efficacy and risk-taking behavior [14]. The authors found that computer self-efficacy negatively influenced the relationship between user awareness of security countermeasures and IS misuse intention. According to the authors, security education and training programs should take into consideration employees’ level of computer understanding.
3. Research model and research questions

The main goal in conducting this research investigation was to develop and empirically validate a model for predicting the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness and thus HIPAA security compliance in AMCs. The conceptual model derived from the findings of this investigation was used to predict intention to comply with the HIPAA Security Rule in lieu of actual HIPAA security compliance. The main research question that this study addressed was: What is the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs? Figure 1 presents the conceptual model for this study.

The main research question can be understood as being comprised of four specific research questions:

RQ1 What is the effect of management support on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs?
RQ2 What is the effect of security awareness on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs?
RQ3 What is the effect of security culture on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs?
RQ4 What is the effect of computer self-efficacy on security behavior and security effectiveness, and thus HIPAA security compliance in AMCs?

Figure 1. The conceptual model of the relevant factors and their effects on HIPAA security compliance in AMCs

4. Methodology

4.1. Instrument development

The author conducted a predictive study that used survey methodology to collect data and develop a model of factors that affect HIPAA security compliance in AMCs. In constructing the survey for this study, the author adapted clearly defined constructs and previously validated items to empirically assess the effect of management support, security awareness, security culture, and computer self-efficacy on security behavior and security effectiveness. The survey that was used in this investigation was a multi-item instrument, whose items were answered by a 5-point Likert-type scale. In the completed analysis, the author used MS to represent management support items, SA to represent security awareness items, SC to represent security culture items, CSE to represent computer self-efficacy items, SB to represent security behavior items, and SE to represent security effectiveness items. A total of 61 items for MS [31, 34], SA [14, 29, 31], SC [7, 31], CSE [2], SB [6, 7, 21, 29], and SE [9, 31] in the instrument were adapted from the survey items developed and validated in the literature. The Cronbach’s α measures for internal consistency reliability exceeded .70 for the items included in the survey instrument.

4.2. Sample and data collection

The target population of this study was health care professionals who are associated with the AAMC. The target sample of this study consisted of 590 health care professionals who are members of the Group on Information Resources (GIR) within the AAMC. An e-mail with the Web-based survey and instructions, along with an explanation of the purpose and relevance of the study, was distributed to the survey participants. A total of 76 AAMC GIR members completed the survey, yielding a response rate of approximately 12.9%. A post-hoc power analysis validated that responses from 76 GIR members adequately ensured that the sample was representative of the population and therefore ensured the generalizability of the study’s findings [12]. When the Web-based survey was completed, the data from the surveys were imported into Statistical Package for Social Science (SPSS) Statistics 18.0 for statistical data analysis.

5. Analysis and results

5.1. Validity and reliability analysis

To ensure the validity of the survey responses, the author included pre-analysis data screening. Pre-analysis data screening addresses the areas of data collection accuracy, response-set, missing data, and multivariate outliers or cases with patterns of scores that are extreme or abnormal. In the study, data
accuracy was not an issue because the Web-based survey software used to collect the data did not require free text responses. Response-set was not an issue because no survey submissions included the same score for 100% of the survey items. Missing data were not a factor in the study because the respondents were required to answer all of the survey items to complete the survey. Mahalanobis Distance ($D^2$) values were calculated for each case and no multivariate outliers were found. All of the $p$ values for the computed Mahalanobis $D^2$ values exceeded .001, providing evidence that the variables included no multivariate outliers at the .001 level of significance. As a result, all 76 cases were be included in the data analysis.

The author examined three validity measures of the instrument: content validity, construct validity, and external validity. The author achieved content validity, construct validity, and external validity with the survey items by basing the survey items on previously validated scales drawn from the literature. Cronbach’s $\alpha$ reliability tests were computed to determine the internal consistency for the survey items MS, SA, SC, CSE, SE, and SB. All items were reviewed to ensure that all scales were keyed in the same direction. The final analysis resulted in high reliability scores for each variable, with Cronbach’s $\alpha$ well above the desired minimum of .70 [47]. MS and SA had the highest internal consistency reliability ($\alpha = .943$ and .941), whereas SB had the lowest reliability ($\alpha = .807$). The reliability analysis results for the survey items are presented in Table 1.

<table>
<thead>
<tr>
<th>Variable</th>
<th>Number of Cases</th>
<th>Number of Items</th>
<th>Cronbach’s $\alpha$</th>
</tr>
</thead>
<tbody>
<tr>
<td>MS</td>
<td>76</td>
<td>10</td>
<td>.943</td>
</tr>
<tr>
<td>SA</td>
<td>76</td>
<td>10</td>
<td>.941</td>
</tr>
<tr>
<td>SC</td>
<td>76</td>
<td>10</td>
<td>.920</td>
</tr>
<tr>
<td>CSE</td>
<td>76</td>
<td>10</td>
<td>.881</td>
</tr>
<tr>
<td>SE</td>
<td>76</td>
<td>11</td>
<td>.930</td>
</tr>
<tr>
<td>SB</td>
<td>76</td>
<td>10</td>
<td>.807</td>
</tr>
</tbody>
</table>

5.2. Data analysis

Following the pre-analysis data screening, as well as validity and reliability tests, the mean values for the multiple item scores that comprised MS, SA, SC, CSE, SE, and SB were calculated to create six composite variables. The mean values of the independent and dependent variables were between 3.2 and 4.2, indicating a general tendency for the numerically-coded responses to represent a value somewhere between neither disagreeing nor agreeing with the items (score = 3) and agreeing with the items (score = 4). The standard deviations of all of the variables ranged from .49 to .71, indicating a relatively wide variability in the responses. Kolmogorov-Smirnov $Z$ statistics were used to test the null hypotheses that the variables were normally distributed. Based on the results, which were non-significant, the null hypotheses were accepted.

This study examined four independent variables: MS, SA, SC, and CSE and their contribution to the dependent variables: SE and SB. The author initially reviewed two regression methods, MLR and OLR analyses, to measure the effect of the independent variables, MS, SA, SC, and CSE, on the dependent variables, SE and SB. MLR analysis is used predict the values of normally distributed dependent variables measured at the scale/interval level [10]. OLR analysis, in comparison, is used to predict the values of dependent variables that are classified into ordinal categories, measured using integers [25]. OLR analysis does not assume linear relationships or necessitate that the data be normally distributed. In this investigation, the dependent variables, SE and SB, were not measured as ordinal categories but were computed as mean values, measured at the scale/interval level. As a result, for the purposes of this study, MLR analysis was considered to be more appropriate than was OLR analysis.

The MLR model used in this investigation was:

$$
SB = \beta_0 + \beta_{MS}MS + \beta_{SA}SA + \beta_{SC}SC + \beta_{CSE}CSE + e
$$

$$
SE = \beta_0 + \beta_{MS}MS + \beta_{SA}SA + \beta_{SC}SC + \beta_{CSE}CSE + e
$$

where $\beta_0$ represented the intercept or the theoretical predicted value of the dependent variable when all the independent variables were zero; and $\beta_{MS}, \beta_{SA}, \beta_{SC},$ and $\beta_{CSE}$ represented the standardized partial regression coefficients for the independent variables. The null hypotheses in the investigation were that the intercept and partial regression coefficients were zero and that the adjusted $R^2$ value did not explain a substantial proportion of the variance in the dependent variables. The adjusted $R^2$ was used to account for the number of independent variables in the model. The null hypotheses were tested using $t$ statistics for the regression coefficients and ANOVA $F$ statistics for the $R^2$ value [49].

MLR analysis assumes that the independent and dependent variables are normally distributed. The approximately bell-shaped frequency distribution histograms provided visual evidence to suggest that the variables MS, SA, SC, CSE, SE, and SB were normally distributed (Figure 2). The frequency
distributions for each variable are presented in Figure 2.

In addition, Kolmogorov-Smirnov Z statistics indicated that the variables were normally distributed. The author confirmed that the residuals were randomly and relatively evenly scattered on either side of their mean (zero) value with respect to the predicted values, reflecting homogeneity of variance of the dependent variable, by visually using a plot of the residuals versus the predicted values (Figure 3). The matrix of scatter plots between the variables is presented in Figure 3.

MLR analysis also assumes that the relationship between the independent and dependent variables is linear. The linear relationships between the MS, SA, SC, SB, and SE variables were confirmed by the calculated values of Pearson’s correlation coefficients between .381 and .776 significant at \( p < .01 \) and observed in the scatter plots. Pearson’s correlation coefficients between -.083 and -.044 demonstrated that the CSE variable was not linearly related to the other variables. Further, the Pearson correlation analysis results demonstrated that the independent variables MS, SA, and SC were collinear. When a correlation coefficient matrix includes correlations of approximately 0.7 or higher, excessive collinearity may exist [49]. In this study, the correlation coefficient of 0.776 between the MS and SC independent variables was an indication of excessive collinearity that could potentially compromise MLR analysis results. Excessive collinearity is also determined with \( VIF \) statistics over 2.5 [1, 42]. In this study, MS and SC \( VIF \) values of 2.763 and 2.592 indicated excessive collinearity.

5.3. Results of MLR analysis to predict security behavior

To correct the MLR model for the influence of excessive collinearity, a new composite variable, MS x SC, was created and replaced MS and SC in the MLR model. The revised MLR model to predict the dependent variable, SB, including MS x SC, using standardized coefficients was:

\[
SB = 3.311 + .265 \times SA - .122 \times CSE + .255 \times MS \times SC + 0
\]

The adjusted \( R^2 = .204 \) indicated that this model predicted a large proportion of the variance in SB. The value of \( p < .05 \) for the t statistics indicated that the intercept was not zero and that SB increased significantly with respect to both SA and MS x SC. The values of \( p > .05 \) for the t statistic indicated that the regression coefficients for CSE were not significantly different from zero, thus indicating that CSE was not a significant predictor of SB. Additionally, performing MLR analysis for the model with CSE removed produced the adjusted \( R^2 = .200 \), providing further evidence that CSE did not contribute to the explanation of the variance in the dependent variable. The revised MLR model to predict the dependent variable, SB, including MS x SC, did not violate the statistical assumptions of MLR with respect to excessive collinearity. The \( VIF \) statistics < 2.5 indicated that the independent variables, MS (1.516), SA (1.511), and CSE (1.005), were not collinear, thereby demonstrating that the MLR statistics were not biased. The adjusted \( R^2 \) and standard error results to predict SB, including MS x SC, are presented in Table 2; the MLR coefficients to predict SB, including MS x SC, are presented in Table 3; and the collinearity statistics to predict SB, including MS x SC, are presented in Table 4. Overall, Tables 2 through 4
summarize the MLR analysis results to predict SB, including MS x SC.

### Table 2. Adjusted R² and Standard Error to Predict SB, Including MS x SC

<table>
<thead>
<tr>
<th>Adjusted R²</th>
<th>Standard Error of the Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>.204</td>
<td>.441</td>
</tr>
</tbody>
</table>

### Table 3. MLR Coefficients to Predict SB, Including MS x SC

<table>
<thead>
<tr>
<th>Variable</th>
<th>β</th>
<th>t</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercept</td>
<td>3.311</td>
<td>8.344</td>
<td>.000***</td>
</tr>
<tr>
<td>SA</td>
<td>.265</td>
<td>2.096</td>
<td>.040*</td>
</tr>
<tr>
<td>MS x SC</td>
<td>.255</td>
<td>2.010</td>
<td>.048*</td>
</tr>
<tr>
<td>CSE</td>
<td>-.122</td>
<td>-1.178</td>
<td>.243</td>
</tr>
</tbody>
</table>

* p < .05, *** p < .001

### Table 4. Collinearity Statistics to Predict SB, Including MS x SC

<table>
<thead>
<tr>
<th>Variable</th>
<th>VIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA</td>
<td>1.511</td>
</tr>
<tr>
<td>MS x SC</td>
<td>1.516</td>
</tr>
<tr>
<td>CSE</td>
<td>1.005</td>
</tr>
</tbody>
</table>

The approximately bell-shaped frequency distribution histogram visually validated that the residuals for the MLR model to predict SB including MS x SC were normally distributed. Residual normality was also confirmed by the recalculated Kolmogorov-Smirnov Z = .818, p = .515. The residuals were not evenly distributed around their mean (zero) value, reflecting heteroskedacity or differing variances. However, the residuals displayed a definitive wedge-shaped pattern, indicating that the variances evenly decreased with respect to an increase in the predicted values of SB. The revised MLR model was considered to be a good fit for the two independent variables SA and CSE, the composite independent variable, MS x SC, and the dependent variable SB. The author concluded that, by comparing the magnitudes of the revised MLR coefficients, SA (β = .265) was a more significant predictor of SB than was MS x SC (β = .255).

5.4. Results of MLR analysis to predict security effectiveness

The revised MLR model to address excessive collinearity and predict SE using standardized coefficients was:

\[ SE = .864 + .569*SA + .069*CSE + .320*MS \times SC + 0 \]

The adjusted \( R^2 = .622 \) indicated that this model predicted a high proportion of the variance in SE. The value of \( p < .05 \) for the \( t \) statistics indicated that the intercept was not zero and that SE increased significantly with respect to both SA and MS x SC. The \( p \) values > .05 for the \( t \) statistic indicated that the regression coefficients for CSE were not significantly different from zero, thus indicating that CSE was not a significant predictor of SE. Additionally, performing MLR analysis for the model with CSE removed produced the same adjusted \( R^2 = .622 \), providing further evidence that CSE did not contribute to the explanation of the variance in the dependent variable.

The revised MLR model to predict the dependent variable, SE, including MS x SC, did not violate the statistical assumptions of MLR with respect to excessive collinearity. The \( VIF \) statistics < 2.5 indicated that the independent variables MS (1.516), SA (1.511), and CSE (1.005) were not collinear, thereby demonstrating that the MLR statistics were not biased. The adjusted \( R^2 \) and standard error results to predict SE, including MS x SC, are presented in Table 5; the MLR coefficients to predict SE, including MS x SC, are presented in Table 6; and the collinearity statistics to predict SE, including MS x SC, are presented in Table 7. Overall, Tables 5 through 7 summarize the MLR analysis results to predict SE, including MS x SC.

### Table 5. Adjusted R² and Standard Error to Predict SE, Including MS x SC

<table>
<thead>
<tr>
<th>Adjusted R²</th>
<th>Standard Error of the Estimate</th>
</tr>
</thead>
<tbody>
<tr>
<td>.622</td>
<td>.401</td>
</tr>
</tbody>
</table>

### Table 6. MLR Coefficients to Predict SE, Including MS x SC

<table>
<thead>
<tr>
<th>Variable</th>
<th>β</th>
<th>t</th>
<th>p</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intercept</td>
<td>.864</td>
<td>2.394</td>
<td>.019*</td>
</tr>
<tr>
<td>SA</td>
<td>.569</td>
<td>6.524</td>
<td>.000***</td>
</tr>
<tr>
<td>MS x SC</td>
<td>.320</td>
<td>3.666</td>
<td>.000***</td>
</tr>
<tr>
<td>CSE</td>
<td>.069</td>
<td>.972</td>
<td>.334</td>
</tr>
</tbody>
</table>

*** p < .001
* p < .05

### Table 7. Collinearity Statistics to Predict SE, Including MS x SC

<table>
<thead>
<tr>
<th>Variable</th>
<th>VIF</th>
</tr>
</thead>
<tbody>
<tr>
<td>SA</td>
<td>1.511</td>
</tr>
<tr>
<td>MS x SC</td>
<td>1.516</td>
</tr>
<tr>
<td>CSE</td>
<td>1.005</td>
</tr>
</tbody>
</table>

The approximately bell-shaped frequency distribution histogram visually indicated that the residuals for the MLR model to predict SE, including
MS x SC, were normally distributed. The recalculated Kolmogorov Smirnov Z statistic = .903, p = .388 also confirmed residual normality. The residuals were somewhat evenly distributed around their mean (zero) value, reflecting heteroskedacity or differing variances. However, the residuals did not display a definitive wedge-shaped pattern, thus indicating that the variances did not evenly decrease with respect to an increase in the predicted values of SE. The revised MLR model was considered to be a good fit to the two independent variables SA and CSE, the composite independent variable MS x SC, and the dependent variable SE. The author concluded that, by comparing the magnitudes of the revised MLR coefficients, SA (β = .569) was a more significant predictor of SE than was MS x SC (β = .320).

5.5. Results of power analysis

To investigate the minimum sample size in the study as a means to adequately permit the rejection of the null hypothesis of MLR, where the adjusted $R^2$ did not explain a substantial proportion of the variance in the dependent variable, the author performed a post-hoc power analysis. Cohen calculated the minimum sample sizes necessary to attain the desired power = 0.8 to reject the null hypothesis of MLR analysis at two specified significance levels ($\alpha = .01$ or $\alpha = .05$) and three population effect sizes $ES = (R^2)/(1 - R^2)$ for $k = 2$ to 8 independent variables [12]. For the two MLR models developed in this investigation to predict SB and SE, including MS x SC as a composite independent variable, the significance criterion was $\alpha = .05$ for $k = 3$ independent variables. The adjusted $R^2$ value for the MLR model to predict SB, including MS x SC, = .204, indicating that the effect size, $ES = .256$ for $k = 3$ independent variables, was medium. Additionally, the adjusted $R^2$ value for the MLR model to predict SE, including MS x SC, = .633, indicating that the effect size $ES = 1.725$ for $k = 3$ independent variables, was large. When $\alpha = .05$ and $k = 3$, the minimum sample size should be $N = 76$, when the effect size is medium, and $N = 34$, when the effect size is large. Therefore, the sample size of 76 used in this investigation was adequate to reject the null hypothesis of MLR.

6. Future research

Several areas of future research were identified. The author did not restrict the current study to one AMC per respondent. Thus, future investigations could ensure that no more than one representative from each AAMC organization participates in the survey. Future studies could also explore whether HIPAA security compliance perceptions differ based on the AAMC GIR member role in their organization. In addition, researching the perceptions of HIPAA security compliance from a broader group of health care professions (e.g., executives, line management, financial, clinical, and technical) within a single AMC would provide a richer view of differences in security compliance within an organization.

Examining additional factors affecting HIPAA security compliance from the literature, such as security framework, perceived security, perceived usefulness of security, resistance to change, and trust, also could be considered in future research. Finally, actual HIPAA security compliance was not measured in this study. Future investigations could measure actual HIPAA security compliance in AMCs.

7. Conclusions

MLR analysis results demonstrated that the theoretical model of this investigation predicted security effectiveness 62.2% of the time. MLR analysis also showed that the model predicted security behavior 20.4% of the time. Pearson correlation analysis revealed that MS, SA, and SC were collinear. As a result, a new composite variable, MS x SC, was developed. Consequently, MLR analysis indicated that the independent variables SA and MS x SC had a significant effect on the dependent variables, SE and SB. CSE, however, did not have a significant effect on either dependent variable. The empirically-validated conceptual model of the relevant factors and their effects on HIPAA security compliance in AMCs is presented in Figure 4.

![Figure 4. The empirically-validated conceptual model of the relevant factors and their effects on HIPAA security compliance in AMCs.](image)

8. References


