To Report or Not Report Health Care Data Breaches

Amanda Walden, PhD, RHIA, CHDA; Kendall Cortelyou-Ward, PhD; Meghan Hufstader Gabriel, PhD; and Alice Noblin, PhD, RHIA, CCS, PMP

ABSTRACT

OBJECTIVES: The study's objectives were to explore the impact of personal/organizational knowledge, prior breach status of organizations, and framed scenarios on the choices made by privacy officers regarding the decision to report a breach.

STUDY DESIGN: A survey was completed of 123 privacy officers who are members of the American Health Information Management Association (AHIMA).

METHODS: The study used primary data collection through a survey. Individuals listed as privacy officers within the AHIMA were the target audience for the survey. Descriptive statistics, logistic regression, and predicted probabilities were used to analyze the data collected.

RESULTS: The percentage of privacy officers who chose to report a breach to the Office for Civil Rights varied by scenario: scenario 1 (general with little information), 39%; scenario 2 (4-factor risk assessment, paper records), 73.2%; scenario 3 (4-factor risk assessment, ransomware case), 91.9%. Several factors affected the response to each scenario. In scenario 1, privacy officers with a Certified in Healthcare Privacy and Security (CHPS) credential were less likely to report; those who previously reported a prior breach were more likely to report. In scenario 2, privacy officers with a bachelor's degree or graduate education were less likely to report; those who held the CHPS or coding credential were less likely to report.

CONCLUSIONS: Study findings show there are gray areas where privacy officers make their own decisions, and there is a difference in the types of decisions they are making on a day-to-day basis. Future guidance and policies need to address these gaps and can use the insight provided by the results of this study.

Am J Manag Care. 2020;26(12):e395-e402. doi:10.37765/ajmc.2020.88546

The Health Information Technology for Economic and Clinical Health Act strengthened Health Insurance Portability and Accountability Act (HIPAA) laws, including those surrounding enforcement, penalties, and breach notification.[1] Under these guidelines, a health care organization must notify patients and the Office for Civil Rights (OCR) of instances of breached protected health information (PHI) as defined by "acquisition, access, use, or disclosure of [PHI] in a manner not permitted by the HIPAA Privacy Rule which compromises the security or privacy of the [PHI]."[2]

When a breach occurs, a facility must assume that there is harm to the patient unless, after completion of a 4-factor risk assessment, they can prove that there was sufficient low probability of compromise to the information.[3-5] The 4-factor risk assessment must address the (1) nature and extent of the breach, (2) the individual who accessed or was disclosed the information, (3) whether the information was acquired/viewed, and (4) the extent to which the risk was mitigated.[5] Although the guidelines are in place, interpretation of them can be subjective. Therefore, some issues may influence decisions outside of the 4-factor risk assessment. These issues may include past history with breaches (prior reporting experience), current trends (as identified by OCR with guidance), and financial liability (cost to organization of reporting vs not reporting). This means that there are gaps in the policy where individuals and organizations are making decisions about patient privacy concerns.

Federal policy instituted that all covered entities are required to have a designated privacy official to develop and implement the facility's privacy/security policies and procedures.[6,7] Many facilities have termed this position as a privacy officer. Although there are guidelines in the case of HIPAA and breach notifications, the organization and its privacy officer(s) are responsible for determining an individual organization's breach reportability status. Matters related to patients and their privacy are now subject to internal determinations made by health care organizations, which could cause significant harm if not handled appropriately.

Reporting to OCR and/or the patient can open an organization to risk of financial and possible criminal penalties. There is a

TAKEAWAY POINTS

This study presents information regarding the decisions that health care privacy officers make about reporting a data breach, including factors that can affect the decision process, such as personal/organizational knowledge, prior breach status, and framed scenarios.

- The percentage of privacy officers who chose to report a breach varied by scenario. Credentials, prior breach reporting, and education level had significant effects on the decision to report depending on the scenario.
- Study findings show that there is a gray area where privacy officers have to make their own decisions, and there is a difference in the types of decisions they are making on a day-to-day basis.
- The findings from this study, including the results showing the impact of education, credentials, and prior experience on the decision to report a breach, can provide insight to address gray areas in future guidance and legislation.

risk of harm to the organization's reputation, which could affect patient visits and market share, thereby negatively affecting future revenue. There are high costs associated with maintaining patient privacy, as well as high costs when patient privacy is breached, which may be taken into account when deciding whether to report a breach.[8-19] Therefore, privacy officers might view risk differently and their processes may vary dependent on their knowledge of the policy, the status of previous reported breaches, and their framing of an incident.

This is the first study to focus on the decisions that health care privacy officers are making in regard to patient data breaches. Privacy officers may be weighing the implications of reporting, and that knowledge may affect their choice to report breaches that do occur to the OCR. This study aims to explore how personal and organizational knowledge, prior breach status, and scenario framing influence how a privacy officer makes determinations about reporting a data breach.

METHODS

Data Sources

This study utilized primary data through a research survey conducted over a single-year time period. The collection of primary data was necessary due to a lack of prior research of this format and subject. A subject matter expert provided guidance on the scenarios. A pilot test was conducted to counteract any bias and to provide feedback on ease of use. The University of Central Florida Institutional Review Board completed a review of the study and questionnaire.

The population targeted for this study were members of the American Health Information Management Association (AHIMA) who were designated as privacy officers. AHIMA has taken the lead in the United States regarding HIPAA and privacy. AHIMA offers educational program-credentialing exams, including a specialized credential, Certified in Healthcare Privacy and Security (CHPS).[20] Privacy officers are likely to be AHIMA members due to the nature of the regulations ensuring access, privacy, and security of patient records. Survey questionnaires included demographic and personal information questions, prior breach reporting details, and hypothetical scenarios that had several outcomes regarding data breach reporting.

Variables to Characterize Privacy Officers and Breaches

Variables used to characterize privacy officers include (1) age,[11] (2) gender, (3) education level, (4) credentials, (5) department of employment, (6) number of years worked in health care, (7) number of years worked in health care privacy, (8) percentage of years worked in health care privacy out of health care career years, (9) knowledge level, (10) facility classification, (11) state privacy laws, (12) organization's profit status, and (13) if the respondent has previously reported a breach to the OCR. Credentials included Registered Health Information Administrator or Registered Health Information Technician, CHPS, and coding credential (including all coding-based credentials). The department in which the privacy officer worked was captured into the following categories: executive, health information management/information technology/other, and compliance. Participants were asked if they were in a state with additional health care privacy laws, and a list was provided identifying these states. Facilities in which the privacy officer worked were categorized as acute care hospital, integrated health delivery system, and other.

Dependent Variables

The dependent variables are the privacy officers' responses to whether they would report a breach in response to 3 scenarios provided through the survey. The response options for the outcome variable in each scenario were yes or no.

1. Breach scenario 1 asked if the respondent would report or not report in an instance where the breach was not clearly identified as reportable (question #19).
2. Breach scenario 2 was a paper health record scenario in which a facility had a break-in. Although no PHI was stolen from the facility, the individual who broke in had access to 450 paper medical records in the office. The 4-factor risk assessment was provided and included areas of concern. The choices to report or not report highlighted the benefits of reporting (question #20).
3. Breach scenario 3 was a ransomware scenario that involved a phishing email. Access was restored, but the attacker potentially had access to 750 unsecured (unencrypted) patient records. The 4-factor risk assessment was provided and included areas of concern. The decisions to report or not report highlighted the potential issues with reporting (question #21).

The first scenario was a simple statement whereas the second and third were more complex. The primary distinctions between the second and third scenarios are the method (paper vs electronic) and the factors that come with those methods (amount of records potentially breached). The scenarios were designed with a level

of real-world ambiguity to allow respondents the opportunity to make either choice, report or not report. The scenarios are listed at the end of the survey in the **eAppendix** (available at **ajmc.com**).

Data Analysis

AHIMA membership included 5293 individuals who held the director/officer classification. Of these individuals, 479 were identified with privacy in their title and were contacted to participate in the study. Using a margin of error of 8%, a significance (α) level of 0.05, and a population of 479, the minimum sample size required was 115 individual responses.[21] There were 123 completed surveys from respondents, resulting in an appropriate sample size for robust analyses.[22]

Descriptive statistics, logistic regression, and predicted probabilities were used to characterize the data. For all regression models, the predictor variables included age, gender, department, state laws, facility classification, profit status, years in health care, years of experience in health care privacy, education level, health care credentials, knowledge level, prior breach status, breach number, and breach effects. The 3 dependent variables are breach scenario 1, breach scenario 2, and breach scenario 3.

RESULTS

For breach scenario 1, 39% of respondents chose to report. For breach scenario 2, 73.2% of respondents chose to report. For breach scenario 3, 91.9% of respondents chose to report (**Table 1**).

TABLE 1. Dependent Variable Responses

Variable	Response	n	%
Breach scenario 1	Not report	75	61.0
	Report	48	39.0
Breach scenario 2	Not report	33	26.8
	Report	90	73.2
Breach scenario 3	Not report	10	8.1
	Report	113	91.9

Predicting Factors for Breach Scenario 1

The CHPS credential (odds ratio [OR], 0.144; $P = .018$) was significantly associated with reporting a breach in scenario 1 (**Table 2**). Prior breach status (OR, 4.422; $P = .010$) was also significant. Due to the high OR of the prior breach variable, a univariate model was attempted to understand the impact that particular variable had on the model; however, the numbers were not sufficient to run the logistic regression models.

Predicting Factors for Breach Scenario 2

Having a bachelor's degree (OR, 0.036; $P = .026$) was significantly associated with reporting a breach in scenario 2 (**Table 3**). Graduate education (OR, 0.013; $P = .006$) was significant as well. The third variable that was significant was coding credential (OR, 0.026; $P = .004$).

Breach Scenario 3

Although the study met the overall assumptions for logistic regression, the data set was homogenous in the outcome and thus there was no need to run a model of predicting factors. This is shown in the **Figure**. The first 2 breach scenarios had variation in the response and breach scenario 3 had a vast majority, 91.9% (113/123 responses), who chose "yes" to indicate that they would report the breach.

Predicted Probabilities

After running the logistic regression models, adjusted predicted probabilities were calculated (**Table 4**). For breach scenario 1, privacy officers who hold the CHPS credential were significantly less likely to report a breach in scenario 1 (predicted probability of 12.7% vs 42.7% for those who do not have the credential). Privacy officers who have previously reported a prior breach were significantly more likely to report a breach in scenario 1 (predicted probability of 47.2% vs 20.9% among those with no prior reported breaches).

For breach scenario 2, privacy officers who have a bachelor's or graduate education were significantly less likely to report a breach in scenario 2 (predicted probability of 56.2% for those with a graduate education and 71.6% for those with a bachelor's degree vs 98.2% for those with a high school diploma or an associate's degree). Privacy officers who hold the CHPS credential were significantly less likely to report a breach in scenario 2 (predicted probability of 57.5% vs 76% for those who do not have the credential). Privacy officers who hold a coding credential were less likely to report a breach in scenario 2 (predicted probability of 26.1% vs 76.7% for those who do not have the credential).

Breach scenario 3 was not included in the predicted probability models due to the homogeneity of the data.

DISCUSSION

Overall, this study found that several variables affect the choice to report a breach for the scenarios. Those with higher levels of education, bachelor's and graduate degrees, are less likely than respondents with only a high school or associate's degree to report a breach in scenario 2. The CHPS credential was the strongest predictor, as we found that privacy officers who hold this credential are less likely to report a breach. Therefore, those with a higher level of demonstrated knowledge, through education and credentials, may be less likely to report a breach dependent on the scenario.

Privacy officers who had reported a prior breach were more likely to report an ambiguous breach in the future if they knew little about the incident. However, when participants were provided additional detail and presented with options, this likelihood was not present. Therefore, those who have dealt with the process previously may err on the side of caution with little information. However, they may become more discerning when presented with additional information.

It is vital that privacy officers understand their reference points and how their framing of an incident can affect their response.

TABLE 2. Logistic Regression: Breach Scenario 1 (N = 123)[a]

Privacy officer characteristics	β	Standard error	EXP(β)	95% CI for EXP(β)		Hypothesis test		
				Lower	Upper	Wald χ^2	*df*	*P*
Intercept	−1.174	2.122	0.309			0.306	1	.58
Age	−0.01	0.028	0.99	0.937	1.046	0.135	1	.713
Gender								
Male	Reference	–	–	–	–	–	–	–
Female	1.235	0.892	3.437	0.599	19.733	1.917	1	.166
Education level								
High school/associate's degree	Reference	–	–	–	–	–	–	–
Bachelor's degree	−0.193	0.598	0.825	0.255	2.664	0.104	1	.747
Graduate education	−1.042	0.724	0.353	0.085	1.456	2.076	1	.15
Credentials								
RHIA/RHIT credential (Y)	−0.017	0.441	0.983	0.414	2.332	0.002	1	.969
CHPS credential (Y)	−1.94	0.819	0.144	0.029	0.716	5.605	1	.018*
Coding credential (Y)	−1.798	1.177	0.166	0.016	1.663	2.334	1	.127
Department								
Executive	Reference	–	–	–	–	–	–	–
HIM/IT/joint/other	−0.483	0.613	0.617	0.186	2.05	0.621	1	.431
Compliance	0.267	0.759	1.306	0.295	5.785	0.123	1	.725
State privacy laws (Y)	−0.198	0.46	0.821	0.333	2.021	0.185	1	.667
Facility classification								
Acute care hospital	Reference	–	–	–	–	–	–	–
Integrated health care delivery system	0.182	0.589	1.199	0.378	3.802	0.095	1	.758
Other	0.611	0.569	1.842	0.604	5.612	1.154	1	.283
Profit status								
Not for profit	Reference	–	–	–	–	–	–	–
For profit	0.259	0.558	1.296	0.434	3.872	0.215	1	.643
Percentage of years worked in health care privacy	0.042	0.88	1.043	0.186	5.855	0.002	1	.962
Knowledge level								
Excellent	Reference	–	–	–	–	–	–	–
Above average	−0.3	0.486	0.741	0.286	1.921	0.381	1	.537
Average	−0.081	0.773	0.922	0.203	4.198	0.011	1	.917
Prior breach (Y)	1.487	0.576	4.422	1.431	13.663	6.669	1	.010*

CHPS, Certified in Healthcare Privacy and Security; HIM, health information management; IT, information technology; RHIA, Registered Health Information Administrator; RHIT, Registered Health Information Technician; Y, yes.

*$P \leq .05$.

[a]Cox & Snell $R^2 = 0.173$; Nagelkerke $R^2 = 0.235$.

Education levels significantly affected reporting decisions, which may indicate a need for higher participation in degree programs and/or certifications by privacy officers. This is an area that could be expanded upon to ensure that those individuals in a facility making decisions are fully informed regarding the requirements to report a breach, the impact on the patient and facility if the wrong choice is made, and how their own personal background and experience can inform their decisions.

There is an indication of a need for privacy officer qualifications by the credential results. The CHPS credential was a strong predictor, lending credence to the value of the advanced knowledge required to obtain the credential and the impact it has on the decision-making process. An interesting finding was that having a coding credential was a predictor of reporting. A review of the coding credential domains and subdomains may show specific content that is valuable for privacy officers. A focus on compliance aspects of the credentials may be beneficial.

An interesting finding of the study was the demographics of the responses to the 3 breach scenario questions. When reviewing them at face value, there was a change in response to the type of scenario. The first scenario was a simple statement, and the majority responded that they would not report. When provided a detailed scenario based on paper records, the majority chose to report. Finally, when provided a detailed scenario based on ransomware, the

TABLE 3. Logistic Regression: Breach Scenario 2 (N = 123)[a]

Privacy officer characteristics	β	Standard error	EXP(β)	95% CI for EXP(β)		Hypothesis test		
				Lower	Upper	Wald χ^2	*df*	*P*
Intercept	7.662	2.784	2126.323			7.576	1	.006
Age	–0.031	0.032	0.969	0.911	1.031	0.976	1	.323
Gender								
Male	Reference	–	–	–	–	–	–	–
Female	–1.100	0.969	0.333	0.050	2.223	1.290	1	.256
Education level								
High school/associate's degree	Reference	–	–	–	–	–	–	–
Bachelor's degree	–3.318	1.490	0.036	0.002	0.672	4.958	1	.026*
Graduate education	–4.317	1.568	0.013	0.001	0.288	7.585	1	.006*
Credentials								
RHIA/RHIT credential (Y)	0.693	0.569	1.999	0.655	6.100	1.480	1	.224
CHPS credential (Y)	–1.347	0.697	0.260	0.066	1.019	3.736	1	.053
Coding credential (Y)	–3.667	1.270	0.026	0.002	0.308	8.337	1	.004*
Department								
Executive	Reference	–	–	–	–	–	–	–
HIM/IT/joint/other	–0.723	0.754	0.485	0.111	2.127	0.920	1	.338
Compliance	–0.902	0.883	0.406	0.072	2.291	1.043	1	.307
State privacy laws (Y)	–0.331	0.555	0.718	0.242	2.131	0.356	1	.551
Facility classification								
Acute care hospital	Reference	–	–	–	–	–	-	–
Integrated health care delivery system	0.004	0.703	1.004	0.253	3.981	0.000	1	.996
Profit status								
Not for profit	Reference	–	–	–	–	–	–	–
For profit	0.312	0.715	1.367	0.336	5.552	0.191	1	.662
Percentage of years worked in health care privacy	–0.613	0.992	0.542	0.077	3.791	0.381	1	.537
Knowledge level								
Excellent	Reference	–	–	–	–	–	–	–
Above average	0.525	0.542	1.691	0.585	4.889	0.940	1	.332
Average	0.981	1.110	2.667	0.303	23.477	0.781	1	.377
Prior breach (Y)	0.650	0.738	1.915	0.451	8.130	0.776	1	.378

CHPS, Certified in Healthcare Privacy and Security; HIM, health information management; IT, information technology; RHIA, Registered Health Information Administrator; RHIT, Registered Health Information Technician; Y, yes.

*$P \leq .05$.

[a]Cox & Snell $R^2 = 0.272$; Nagelkerke $R^2 = 0.395$.

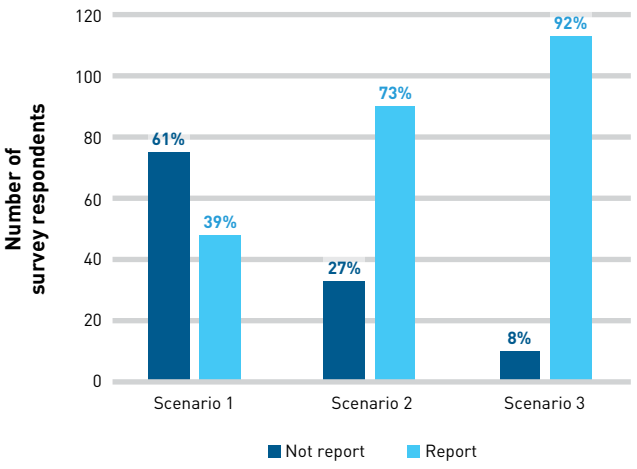
overwhelming majority chose to report. The shift from the second to the third scenario may have been affected by the contextual factors of the study, including the number of records affected and the responses to the 4-factor risk assessment that were provided. Respondents may have chosen to err on the side of caution due to the ambiguity of ransomware attacks, where the level of compromise to the information may not be as evident.

Privacy officers should review the results of this study carefully and utilize them to enhance their ability to manage breach determinations in their workplace. Higher levels of education, credentials, and knowledge base may enable privacy officers to market themselves better in the workplace and enhance their positions within health care organizations.

The results of this study indicate that breach determination is made on a case-by-case basis and dependent on individual decisions. However, health care organizations can utilize these results to develop plans with their internal and external stakeholders in the event of a breach of patient information. Implications of a breach are shaped by the type, category, method of access, and number of patients affected; however, it is important to have these high-level plans in place so everyone involved has a basic understanding. Development of these plans should include discussions of when reporting is appropriate and why it is important to report in cases where it is appropriate regardless of the consequences.

This recommendation is in line with industry trends. The Emergency Preparedness and Security Trends in Healthcare survey

FIGURE. Breach Scenario Responses



identified that cyberattacks are the third-highest safety concern of health care organizations.[23] A recent study found that although facilities may take steps to protect privacy, including the use of advanced information technology systems along with biometric and 2-factor security systems, breaches still occur with paper and electronic records.[24]

An example of the type of plans needed can be found in the case of Anthem, a health care insurance company that experienced one of the largest breaches of 2015, affecting 80 million individuals.[25] From that incident, the author of the PRNEWS article "7 PR Lessons From the Largest Healthcare Data Breach in History" created a set of lessons that companies should consider for a crisis communication plan in the case of a breach of patient information. These lessons include early and easy-to-understand transparency with the public and authorities, which includes a sincere apology and the offer of compensation to victims to help reestablish loyalty.[25] As indicated by this study, privacy officers need the knowledge and education to assist in the development of these plans.

OCR has previously provided guidance on areas of breach determination; however, the process still has gaps where privacy officers are making their own decisions. OCR can use the findings of this study to help identify and address these gaps. Further guidance should be issued to help with the areas of ambiguity and perhaps scenario-based guidance as appropriate.

Limitations

The study included self-reported measures, which may have led to bias in the results, primarily with the self-rating of knowledge level. Furthermore, the study population was restricted to privacy officers who were members of AHIMA, which may affect the generalizability of the results to all privacy officers in the United States. Furthermore, although this study found that education and

TABLE 4. Predicted Probabilities

Privacy officer characteristics	Scenario 1	Scenario 2
Gender		
Male (reference)	0.202	0.875
Female	0.396	0.709
Education level		
High school/associate's degree (reference)	0.482	0.982
Bachelor's degree	0.417	0.716**
Graduate education	0.272	0.562**
RHIA/RHIT credential		
No (reference)	0.371	0.675
Yes	0.396	0.790
CHPS credential		
No (reference)	0.427	0.760
Yes	0.127**	0.575**
Coding credential		
No (reference)	0.401	0.767
Yes	0.130	0.261**
Department		
Executive (reference)	0.441	0.813
HIM/IT/joint/other	0.340	0.715
Compliance	0.468	0.666
State privacy laws		
No (reference)	0.404	0.750
Yes	0.339	0.685
Facility classification		
Acute care hospital (reference)	0.329	0.742
Integrated health care delivery system	0.370	0.763
Other	0.463	0.652
Profit status		
Not for profit (reference)	0.366	0.713
For profit	0.421	0.759
Knowledge level		
Excellent (reference)	0.405	0.657
Above average	0.353	0.765
Average	0.413	0.860
Prior breach status		
No (reference)	0.209	0.666
Yes	0.472**	0.751

CHPS, Certified in Healthcare Privacy and Security; HIM, health information management; IT, information technology; RHIA, Registered Health Information Administrator; RHIT, Registered Health Information Technician.
*$P < .1$; **$P < .05$; ***$P < .001$. Significance denotes differences from reference category.

certifications are predictive of likelihood to report breaches, this survey did not quantify or take into account the quality of education that these privacy officers may have received. The survey did not include an area for respondents to provide a rationale for their decisions to report/not report, which can limit the findings in terms of correlation vs causation. This would be an area to expand upon for future research with qualitative studies.

There was no need to run the third model based on the third scenario, as there was not enough variation in the dependent variable. The data still provided a wealth of information for the theoretical and practical implications, but it was not included in the statistical models.

The subject of the study can be considered sensitive to organizations and could have resulted in nonparticipation from those contacted, as they may have been restricted from participating or felt it inappropriate due to their facility's legal requirements.

CONCLUSIONS

The purpose of this study was to explore the impact that personal and organizational knowledge and scenario framing had on the decisions that privacy officers made in regard to reporting privacy breaches to the OCR. The findings of the study provided industry and policy implications.

Health care privacy is paramount due to the sensitive nature and amount of information collected by care providers. Although there are federal and state policies in place to protect individual patient privacy, the findings of this study show that there is a gap where privacy officers have to make their own decisions, and there is a difference in the types of decisions they are making on a day-to-day basis.

With the significant results of this study identified as education level–, credential level–, and scenario-based, they are indicative of a need for educational opportunities and potential requirements for designated privacy officers. This includes initial levels of education, as well as continuing education requirements to ensure the individuals stay up to date on the current trends and threats in health care. Educational initiatives may also be beneficial at the executive level because these individuals may underestimate the importance of privacy initiatives, which could lead to underreporting of breaches. These educational initiatives may include scenario-based training to identify areas of concern and confusion for their organization. This can assist in developing well-rounded policies and procedures for breach reporting. Future research at the executive level of understanding and decision-making is crucial for policy implications. Both levels, privacy officer and executive positions, would benefit from scenario-based educational opportunities as well.

Health care has a variety of settings, from small individual physician practices to large national integrated delivery systems. The types of care vary from basic preventive care to high-impact invasive treatment. These varieties of settings and care provision types lead to difficulties in identifying a single answer to protecting patient information. The types of systems and information processes used among these are more a best-of-fit than a best-of-breed for this reason. Future guidance and policies need to address these gaps and can use the insight provided by this study of areas that influence the decision-making process.

A driving force behind this study was to understand how privacy officers make decisions, because if they make a wrong decision, it can be extremely detrimental to patients. The findings from the study indicate that higher knowledge levels of respondents equate to a lower likelihood of reporting, which can be positive for a facility. However, if the case was reportable, it may be harmful to patients. It is essential that the federal government take into account the regulatory burden placed on businesses; however, protecting the privacy of patients must still be a priority. ■

Author Affiliations: Department of Health Management and Informatics, College of Health & Public Affairs, University of Central Florida (AW, KC-W, AN), Orlando, FL; Pharmacy Quality Alliance (MHG), Alexandria, VA.

Source of Funding: None.

Author Disclosures: The authors report no relationship or financial interest with any entity that would pose a conflict of interest with the subject matter of this article.

Authorship Information: Concept and design (AW, KC-W, AN); acquisition of data (AW); analysis and interpretation of data (AW, KC-W, MHG); drafting of the manuscript (AW, AN); critical revision of the manuscript for important intellectual content (AW, KC-W, MHG, AN); statistical analysis (AW); administrative, technical, or logistic support (AW); and supervision (KC-W, MHG).

Address Correspondence to: Amanda Walden, PhD, RHIA, CHDA, Department of Health Management and Informatics, College of Health & Public Affairs, University of Central Florida, 528 W Livingston St, Ste 401, Orlando, FL 32801. Email: amanda.walden@ucf.edu.

REFERENCES

1. Oachs P, Watters A, eds. *Health Information Management Concepts, Principles, and Practice*. 5th ed. American Health Information Management Association; 2016.
2. Office for Civil Rights. Annual report to Congress on breaches of unsecured protected health information for calendar years 2009 and 2010. Kaiser Family Foundation. 2011. Accessed November 16, 2020. https://www.kff.org/wp-content/uploads/sites/2/2012/06/compliancerept.pdf
3. Bendix J. What the HIPAA omnibus rule means for your practice. *Contemp Ob/Gyn*. 2013;58(6):34-42.
4. Analysis of modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. American Health Information Management Association. January 25, 2013. Accessed June 4, 2014. https://library.ahima.org/PdfView?oid=106127
5. American Health Information Management Association. Performing a breach risk assessment. *J AHIMA*. 2013;84(9):66-70.
6. Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; other modifications to the HIPAA rules. *Fed Regist*. 2013;78(17):5565-5702.
7. Liginlal D, Sim I, Khansa L, Fearn P. HIPAA privacy rule compliance: an interpretive study using Norman's action theory. *Comput Secur*. 2012;31(2):206-220. doi:10.1016/j.cose.2011.12.002
8. Coate D, MacDonald K. Projecting the budget impacts of HIPAA. *Healthc Financ Manage*. 2002;56(2):42-48.
9. Fleming NS, Culler SD, McCorkle R, Becker ER, Ballard DJ. The financial and nonfinancial costs of implementing electronic health records in primary care practices. *Health Aff (Millwood)*. 2011;30(3):481-489. doi:10.1377/hlthaff.2010.0768
10. Adler-Milstein J, Green C, Bates D. A survey analysis suggests that electronic health records will yield revenue gains for some practices and losses for many. *Health Aff (Millwood)*. 2013;32(3):562-570. doi:10.1377/hlthaff.2012.0306
11. McMillan M. The cost of IT security. *Healthc Financ Manage*. 2015;69(4):44-47.
12. Khansa L, Cook DF, James T, Bruyaka O. Impact of HIPAA provisions on the stock market value of healthcare institutions, and information security and other information technology firms. *Comput Secur*. 2012;31(6):750-770. doi:10.1016/j.cose.2012.06.007
13. Third annual patient privacy & data security study. Ponemon Institute. December 6, 2012. Accessed June 4, 2017. http://www.ponemon.org/research/ponemon-library/security/third-annual-patient-privacy-data-security-study.html
14. Fourth annual benchmark study on patient privacy & data security. Ponemon Institute. March 26, 2014. Accessed June 4, 2017. http://www.ponemon.org/research/ponemon-library/security/fourth-annual-benchmark-study-on-patient-privacy-data-security.html

15. Fifth annual benchmark study on patient privacy & data security. Ponemon Institute. May 27, 2015. Accessed June 4, 2017. http://www.ponemon.org/research/ponemon-library/security/fifth-annual-benchmark-study-on-privacy-security-of-healthcare-data.html
16. Sixth annual benchmark study on patient privacy & data security. Ponemon Institute. May 12, 2016. Accessed June 4, 2017. http://www.ponemon.org/research/ponemon-library/security/sixth-annual-benchmark-study-on-privacy-security-of-healthcare-data.html
17. Campbell K, Gordon LA, Loeb MP, Zhou L. The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *J Comput Secur*. 2003;11(3):431-448. doi:10.3233/JCS-2003-11308
18. Khansa L, Liginlal D. Quantifying the benefits of investing in information security. *Commun ACM*. 2009;52(11):113-117. doi:10.1145/1592761.1592789
19. Andoh-Baidoo F, Amoako-Gyampah K, Osei-Bryson K. How internet security breaches harm market value. *IEEE Secur Priv*. 2010;8(1):36-42. doi:10.1109/MSP.2010.37
20. Certified Health Data Analyst (CHDA). American Health Information Management Association. Accessed September 1, 2017. https://www.ahima.org/certification/chda
21. Sample size calculator. Raosoft. Accessed June 6, 2017. http://www.raosoft.com/samplesize.html
22. Dillman DA, Smyth JD, Christian LM. *Internet, Phone, Mail, and Mixed Mode Surveys: The Tailored Design Method*. 4th ed. John Wiley & Sons Inc; 2014.
23. Rave Mobile Safety survey unearths discrepancies about which emergencies occur at facilities and the preparedness plans they have in place. News release. Rave Mobile Safety; October 23, 2018. Accessed November 4, 2018. https://www.prnewswire.com/news-releases/rave-mobile-safety-survey-unearths-discrepancies-about-which-emergencies-occur-in-healthcare-facilities-and-the-preparedness-plans-they-have-in-place-300735983.html
24. Gabriel MH, Noblin A, Rutherford A, Walden A, Cortelyou-Ward K. Data breach locations, types, and associated characteristics among US hospitals. *Am J Manag Care*. 2018;24(2):78-84.
25. Keeve A. 7 PR lessons from the largest healthcare data breach in history. PRNEWS. February 1, 2016. Accessed September 23, 2018. https://www.prnewsonline.com/7-pr-lessons-from-the-largest-healthcare-data-breach-in-history/

Visit **ajmc.com/link/88546** to download PDF and eAppendix

eAppendix. QUESTIONNAIRE

As you answer this survey, please respond keeping your ***current*** facility in mind.

Screening Question:

1. Are you currently employed?
    a. Yes
    b. No – Conclude Survey

2. Are you the current designated Privacy Officer for your facility?
    a. Yes
    b. No - Conclude Survey

3. Date of Survey Completion:_____

---

4. What is your Age (in years)? Continuous.

5. What is your Gender?:
    a. Male
    b. Female
    c. Other
    d. Prefer not to disclose

6. Select your highest completed level of education:
    a. High School
    b. Associate's Degree
    c. Bachelor's Degree
    d. Master's Degree
    e. Doctoral Degree

7. Select all AHIMA credentials that you are currently certified to hold:
    a. RHIA- Registered Health Information Administrator
    b. RHIT- Registered Health Information Technician
    c. CCA- Certified Coding Associate
    d. CCS- Certified Coding Specialist
    e. CCS-P- Certified Coding Specialist- Physician-based
    f. CDIP- Certified Documentation Improvement Practitioner
    g. CHDA- Certified Health Data Analyst
    h. CHPS- Certified in Healthcare Privacy and Security
    i. CHTS- Certified Healthcare Technology Specialist
    j. CPHI- Certified Professional in Health Informatics

8. Your Privacy role in your current facility falls into which of the following departments, choose only one.
    a. Executive Team
    b. HIM Department

c. IT Department
d. Joint HIM/IT Appointment
e. Other - Text Box for fill-in

9. Is your facility located in a state with additional healthcare specific privacy breach notification laws?)

States with additional healthcare specific privacy breach notification laws are as follows:

Arkansas
California
Delaware
Florida
Illinois
Kentucky
Maryland
Missouri
Montana
Nevada
New Hampshire
North Dakota
Oregon
Rhode Island
Texas
Wyoming

a. Yes
b. No

10. How would you classify your healthcare facility?

a. Acute Care Hospital
b. Ambulatory Surgery Center
c. Behavioral/Mental Health
d. Clinic/Physician Practice
e. Consulting Service
f. Education
g. Health Information Exchange
h. Home Health/Hospice
i. Integrated Healthcare Delivery System
j. Long Term Care
k. Non-Provider Setting (e.g., govt., vendor, assoc.)
l. Other Provider Setting (e.g., rehab)
m. Regional Extension Center

11. What is the profit status of your healthcare facility?
    a. Non-Profit
    b. For-Profit

12. How many years have you been employed in the healthcare field? – Continuous

13. How many years have you been employed in the healthcare privacy field? – Continuous

14. How would you rate your knowledge of healthcare privacy?
    a. Excellent
    b. Above Average
    c. Average
    d. Below Average
    e. Poor

15. During your time at your current employer, has your facility reported a breach of Protected Health Information (PHI) to the Office for Civil Rights?
    a. Yes

b. No- Skip to Question 19

16. During your time at your current employer, how many breaches of patient Protected Health Information (PHI) has your facility reported to the Office for Civil Rights? – Continuous

17. What classification were the breaches indicated in the previous question?
    a. Fewer than 500 patients per incident ONLY
    b. More than 500 patients per incident ONLY
    c. Cases of both 'Fewer than 500 patients per incident' and 'More than 500 patients per incident'

18. What were the outcomes of the breaches from the Office for Civil Rights? Choose all that apply.
    a. Corrective Action Plan
    b. Criminal Penalties
    c. OCR Fine
    d. None

19. If a breach of patient PHI occurs in the future that is not clearly identified as reportable, will you report or not report?
    a. Report
    b. Not Report

20. Your healthcare facility was unlawfully entered. The individual who broke in potentially had access to 450 paper patient records that were held in that office. There were no security cameras to record events, although office supplies were gone through, only a printer with no PHI was taken. Your policies and procedures are up to date, however they do not specifically address breach determination for break-in for your facility. All policies, procedures, training and risk assessment and management are in compliance.

Your next step is to review the four factor risk assessment to determine if the potential breach is reportable to the patients and the Office for Civil Rights. Upon review:

1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. – The records are paper based and included multiple types of unsecured PHI including sensitive patient identifiers.
2) The unauthorized person who used the PHI or to whom the disclosure was made. – The unknown individual who broke into the facility was not authorized to view the records and their intent is unknown.
3) Whether the PHI was actually acquired or viewed. – Employees cannot distinguish if the records have been disturbed, accessed or read.
4) The extent to which the risk to the PHI has been mitigated. – No records were missing.

Choose one of two options, 'report' or 'do not report'.

If you report, you will bear the cost of reporting but your facility benefits by having your liability reduced.

If you do not report one of 2 options occur. (A) OCR investigates for any other reason, may find your facility made an inappropriate determination, fines and/or corrective actions of unknown levels may be made. OR (B) OCR does not investigate this incident and your facility benefits by incurring no costs or corrective actions.

a. Report
b. Not Report

21. An employee at your facility clicked on a link from a Phishing e-mail which led to a ransomware attack on your facility. Payout was required and access was restored to your system. The attacker potentially had access to 750 unsecured (unencrypted) patient

records in the system. All policies, procedures, training and risk assessment and management are in compliance.

Your next step is to review the four factor risk assessment to determine if the potential breach is reportable to the patients and the Office for Civil Rights. Upon review:

1) The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification. – The records are electronic based and included multiple types of unsecured PHI, including patient identifiers.

2) The unauthorized person who used the PHI or to whom the disclosure was made. – The attacker was not authorized to view the records. No idea of whether other malware was left behind.

3) Whether the PHI was actually acquired or viewed. – The system cannot distinguish if records were viewed or copied.

4) The extent to which the risk to the PHI has been mitigated. – malware infection was removed and PCs reformatted and reloaded.

Choose one of two options, ‘report’ or ‘do not report’.

If you report, there are negative public relations consequences from media reporting and the incident posted on the OCR website but there is no real possibility of a fine.

If you do not report one of 2 options occur. (A) OCR does not investigate this incident and your facility incurs no costs/corrective actions/negative public relations. OR (B) A compliant or other reason allows OCR to open an investigation where they review the breach determination and decide it was improper, with potentially large fines being issued with resulting negative media exposure and increased public relations issues.

a. Report
b. Not Report

The April 2017 cover story for the Journal of AHIMA was titled "Is HIPAA Outdated?" What are your thoughts regarding the HIPAA legislation in terms of breach notification and its ability to adapt? Please add any additional comments regarding breach notification that you feel would be useful to this study.