THE MILBANK QUARTERLY
A MULTIDISCIPLINARY JOURNAL OF POPULATION HEALTH AND HEALTH POLICY

Original Scholarship

The Role of HIPAA Omnibus Rules in Reducing the Frequency of Medical Data Breaches: Insights From an Empirical Study

NIAM YARAGHI[*,†] and RAM D. GOPAL[*]

[*]*School of Business, University of Connecticut;* [†]*Center for Technology Innovation, Governance Studies, the Brookings Institution*

Policy Points:

- Frequent data breaches in the US health care system undermine the privacy of millions of patients every year—a large number of which happen among business associates of the health care providers that continue to gain unprecedented access to patients' data as the US health care system becomes digitally integrated.
- Implementation of the HIPAA Omnibus Rules in 2013 has led to a significant decrease in the number of privacy breach incidents among business associates.

Context: Frequent data breaches in the US health care system undermine the privacy of millions of patients every year. A large number of such breaches happens among business associates of the health care providers that continue to gain unprecedented access to patients' data as the US health care system becomes digitally integrated. The Omnibus Rules of the Health Insurance Portability and Accountability Act (HIPAA), which were enacted in 2013, significantly increased the regulatory oversight and privacy protection requirements of business associates. The objective of this study is to empirically examine the effects of this shift in policy on the frequency of medical privacy breaches among business associates in the US health care system. The findings of this research shed light on how regulatory efforts can protect patients' privacy.

Methods: Using publicly available data on breach incidents between October 2009 and August 2017 as reported by the Office for Civil Rights (OCR), we conducted an interrupted time-series analysis and a difference-in-differences

The Milbank Quarterly, Vol. 96, No. 1, 2018 (pp. 144-166)

analysis to examine the immediate and long-term effects of implementation of HIPAA omnibus rules on the frequency of medical privacy breaches.

Findings: We show that implementation of the omnibus rules led to a significant reduction in the number of breaches among business associates and prevented 180 privacy breaches from happening, which could have affected nearly 18 million Americans.

Conclusions: Implementation of HIPAA omnibus rules may have been a successful federal policy in enhancing privacy protection efforts and reducing the number of breach incidents in the US health care system.

Keywords: Health Insurance Portability and Accountability Act, patient privacy.

Patient privacy and the protection of confidential information are vital elements of the patient-physician relationship. They ensure the patient's autonomy and trust in physicians, without which patients would be much less likely to seek medical care.[1] Over the past 2 decades, these values have been primarily governed and protected under the Health Insurance Portability and Accountability Act (HIPAA).[2] One of the major goals of HIPAA is to reduce administration inefficiencies by standardizing electronic transactions in the health care sector. HIPAA was signed into law by President Bill Clinton in 1996, yet it has grown in prominence after the implementation of the Health Information Technology for Economic and Clinical Health Act (HITECH) in 2009, which resulted in widespread adoption of heath information technologies. HITECH has led to unprecedented challenges with patient privacy as more personal information is being collected, archived, and transmitted electronically between multiple parties.[3-5] Responding to these challenges, the US Department of Health and Human Services' Office for Civil Rights (OCR) implemented the most significant changes to health care privacy law in a decade by publishing the final HIPAA omnibus rules on January 25, 2013.[6]

Prior to the omnibus rules, only covered entities, which are defined as "health care providers who conduct health care transactions electronically, health plans and health care clearinghouses," were subject to HIPAA regulations. Examples of health care providers include physicians, psychologists, and dentists as well as clinics and nursing homes. Examples of health plans include health insurers and company health

plans. Health care clearinghouses are those "entities that process non-standard health information they receive from another entity into a standard."

The omnibus rules, however, expanded the reach of HIPAA to include all business associates that "create, receive, maintain, or transmit protected health information." Examples of business associates include third-party administrators that process claims for health plans, pharmacy benefits managers that manage the insurers' pharmacy networks, and hospitals' consultants. After the implementation of the omnibus rules, the business associates not only had to comply with HIPAA but, more important, could also potentially be held civilly and criminally liable in case of a privacy breach.[7] This paper presents the results of an analysis of the effects of this policy on the volume of privacy breaches among business associates.

While the importance of patient privacy has been known to physicians for centuries and they take the Hippocratic oath to protect it,[8] the new era of modern medicine extends the importance of privacy from the realm of medicine to economics and information technology. As medical science advances and health care systems become more complex, the number of professionals who are involved in a patient's medical care and need to have access to confidential information increases. While in many instances these professionals are not caregivers and do not directly provide medical services to patients, their access to confidential information may be necessary since they facilitate the provision of medical care, primarily through increasing efficiency in the management and administrative side of health care. Unless the confidentiality of patients' information is taken seriously and adequate protections are put in place to safeguard patients' privacy, they will remain reluctant to share their medical information with those who are not directly involved in their care. The successful implementation of modern technologies and economic plans that are necessary to support the provision of medical care hinges on the free flow of data between different parties. Without addressing patients' privacy concerns, technologies such as health information exchanges and economic and managerial plans such as accountable care organizations will not succeed.[9-12]

Despite its importance, prior to the omnibus rules, business associates of the covered entities did not have strong market-based incentives to protect patients' privacy.[13] HIPAA omnibus rules filled this gap by holding the business associates to the same standards as covered

entities. In addition, by creating civil and criminal penalties to hold them accountable, the omnibus rules incented business associates to invest in complying with HIPAA and safeguarding patients' privacy. The purpose of this research is to investigate the extent to which the implementation of HIPAA omnibus rules has reduced the frequency of privacy breaches among the business associates.

Methods

Data Source

We use the publicly available data reported by OCR.[14] This data set lists all of the privacy breach incidents that affected more than 500 individuals between October 2009 and August 2017 in the United States.

Study Design

To study the effects of implementation of HIPAA omnibus rules on the frequency of privacy breaches among business associates, we conducted an interrupted time-series analysis with control outcome variables. In this design, we utilize the frequency of privacy breaches over a series of equally spaced time intervals among both covered entities and business associates. Covered entities have been complying with HIPAA since the beginning of our observation series and because the omnibus rules did not pertain to them, we can assume that the implementation of the rules did not affect the frequency of privacy breach incidents amongst them. In other words, the frequency of breach incidents among covered entities should not be affected by the implementation of omnibus rules but could be affected by factors unrelated to this study, such as increased adoption of electronic health record systems.

On the contrary, since business associates were the focus of the new policy, we can assume that implementation of the HIPAA omnibus rules has interrupted the frequency of privacy breaches among them. As we mentioned earlier, since factors other than the implementation of omnibus rules could have affected the privacy breaches in the health care sector in general, we use the difference between the number of privacy

breaches in the 2 groups as our dependent variable. For example, the public awareness and concern over privacy breaches may have increased over time and led both covered entities and business associates to be more cautious in managing patients' data. These factors affect the breaches in both groups; therefore, examining the difference in the number of breach incidents of the 2 groups, rather than focusing on the breach incidents of only 1 group, allows us to detect and account for other trends that are unrelated to the implementation of HIPAA omnibus rules. This statistical approach is a suitable quasi-experimental research method to measure the impact of policies on population-level outcomes[15] and is being increasingly used to examine the effects of different policies in health care settings.[16-18]

Statistical Analysis

In our interrupted time-series analysis, the dependent variable is the difference between the number of privacy breaches in the 2 groups of business associates and covered entities in a 3-month interval. We fit the dependent variable in each period as a function of 3 main explanatory variables. The first is a continuous variable that counts the periods since the start of the time series. The coefficients of this variable capture the time trends. The second is a binary variable that indicates the shift in policy. This variable is equal to 1 if the period is post implementation of HIPAA omnibus rules and 0 if the period is before the implementation of the omnibus rules. The coefficient of the binary variable indicates whether there is a change in the outcome variable immediately after implementing the rules. The third is a continuous variable that counts the number of periods after the implementation of HIPAA omnibus rules. The value of this variable in periods before the implementation of the rules is equal to 0. The coefficient of this variable indicates whether there is a change in the slope of the outcomes after the implementation of the rules compared with the trend in the pre-implementation period. To account for correlation in outcomes between consecutive periods, we follow the recommendations of Penfold and Zhang[19] to test and account for correlation in subsequent observations in the time series. Our test results indicated the need for including third-order autoregressive parameters in the models.[20] We also examine the existence of seasonality in our time series and, where necessary, include seasonal dummies in our models to adjust for seasonal fluctuations in breach incidents.

Results

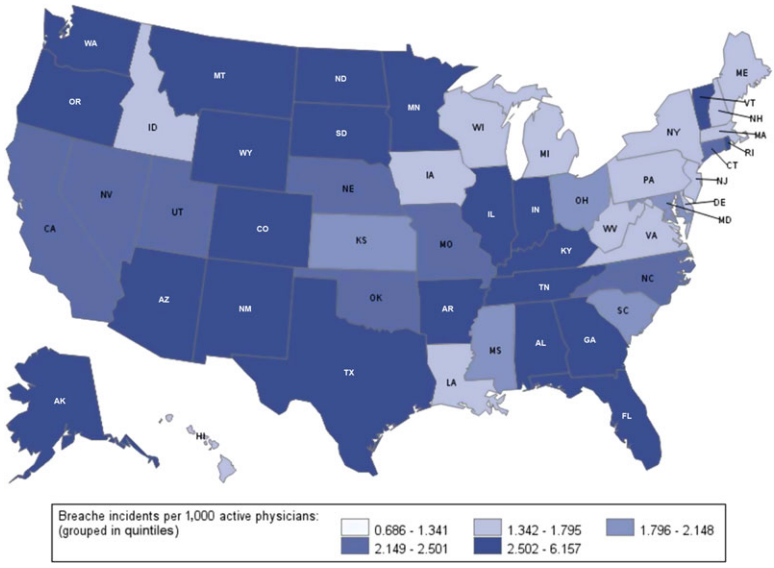
During the study period, 2,010 breach incidents occurred, of which 291 incidents were among business associates. A total of 52 of the breach incidents were not categorized, so we excluded them from the analysis. The remaining incidents occurred among covered entities that, according to HIPAA definitions, include health care providers (1,410 incidents), health plans (253 incidents), and health care clearinghouses (4 incidents). An average of 2.17 privacy breach incidents take place per 1,000 professionally active physicians in the United States. Figure 1 shows the distribution of privacy breach incidents per 1,000 professionally active physicians by state.

Figures 2 and 3 show the frequency of different types of breaches and the number of patients who are affected by such incidents among covered entities and business associates, respectively. As shown in these figures, while theft incidents are the most common type of incident among covered entities, hacking/IT incidents affect the largest number of people. Among business associates, theft incidents are the most common and also affect the largest number of people. On average, a breach incident among covered entities affects 87,760 individuals, while a breach incident among business associates affects 98,803 individuals. So far, these breaches combined have undermined the privacy of 175,047,905 patients in the United States.

OCR announced the HIPAA omnibus rules on January 25, 2013. These rules became effective on March 26, 2013, with compliance required by September 23, 2013[6]; however, the rules were not heavily enforced until after 2014. As illustrated in Figure 4, the effect of enforcement among business associates is observed in January 2015. The literature explains that the reason for the delay between the official enforcement and actual effect dates could be the role of the media in creating public awareness. For example, Soumerai and colleagues[22] report that media warnings about Reye's syndrome were much more influential than FDA product labeling in reducing the use of aspirin for children. Lu and colleagues[23] report a similar effect of media coverage on suicidal behavior.

Also shown in Figure 4, there is a seasonal trend in breach incidents among both covered entities and their business associates; however, it is canceled out when we use the difference in the number of breach incidents as our main dependent variable. Therefore, we do not need to adjust for seasonality in our analysis of changes in the difference

Figure 1. Distribution of Privacy Breach Incidents per 1,000 Professionally Active Physicians in the United States[a]
[Color figure can be viewed at wileyonlinelibrary.com]

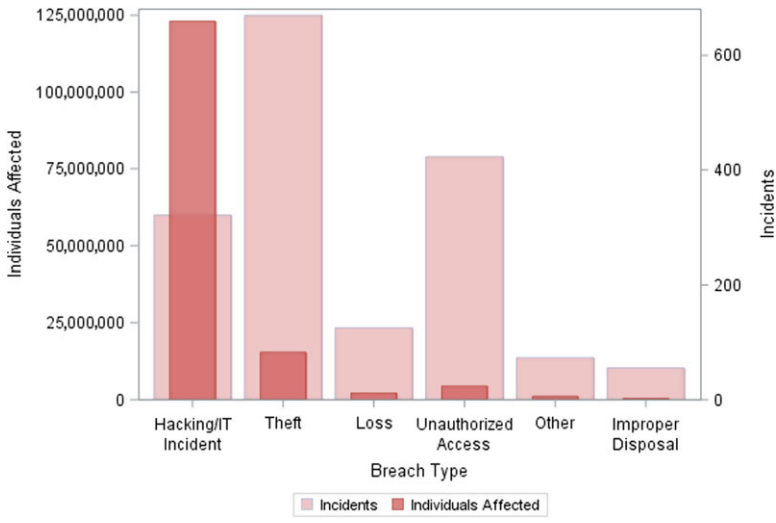


[a]Data derived from authors' analysis of Office for Civil Rights data on breach incidents between October 2009 and August 2017. To calculate the breach incidents per 1,000 physicians, authors divided the number of incidents by the total number of professionally active physicians in each state as reported by the Henry J. Kaiser Family Foundation.[21] The 5 color shades on the map represent the quintiles of the calculated breach incidents per 1,000 physicians.

between breach incidents among the 2 groups. However, the breach incidents themselves do follow a seasonal pattern. We have adjusted for the seasonality in the models that predict the incidents in each of the 2 groups separately. Therefore, in Table 1, the models that are presented in the business associates and covered-entities panels include seasonal dummies, while the models presented under the difference panel do not.

Before the omnibus rules took full effect in January 2015, privacy breaches happened at a relatively constant rate among both business

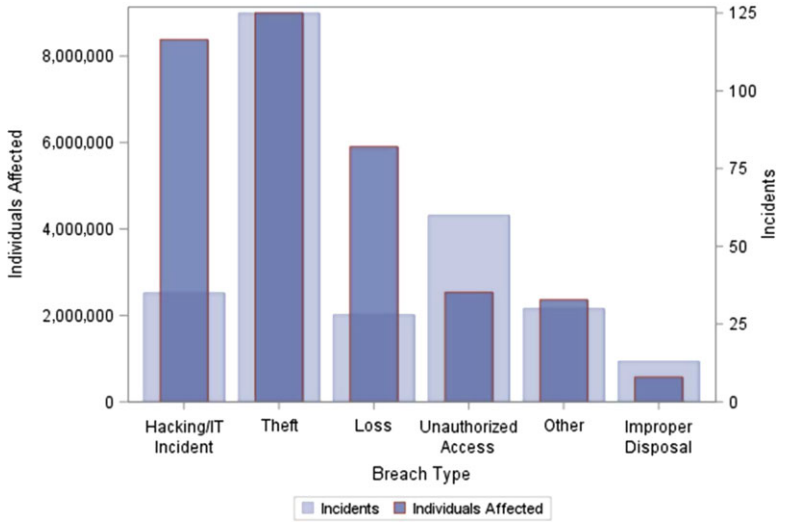
Figure 2. Types of Privacy Breach Incidents and the Number of Patients Affected by Them Among Covered Entities[a]
[Color figure can be viewed at wileyonlinelibrary.com]



[a]Data derived from authors' analysis of Office for Civil Rights data on breach incidents between October 2009 and August 2017. Incidents described as "Unknown," "Other," or that were missing a description were grouped under the "Other" category. Where the type of an incident was categorized in more than one group by OCR, the incident was assigned to the primary group. For example, an incident OCR described as "Theft/Loss" was categorized under "Theft."

associates and covered entities. While these breach incidents appear to follow a parallel trend before the implementation of the rules, they drift apart after implementation. In our time-series analysis, we eliminate the fourth quarter of 2009 and initiate the time series from January 2010 for two reasons. First, our time intervals are quarters, while the earliest breach incident was reported on October 21, 2009. This means that the time-series value for the fourth quarter of 2009 does not include incidents in the first 20 days of October 2009 and therefore incorrectly undercounts the breach incidents. Second, the right to enforce HIPAA

Figure 3. Types of Privacy Breach Incidents and the Number of Patients Affected by Them Among Business Associates[a]
[Color figure can be viewed at wileyonlinelibrary.com]

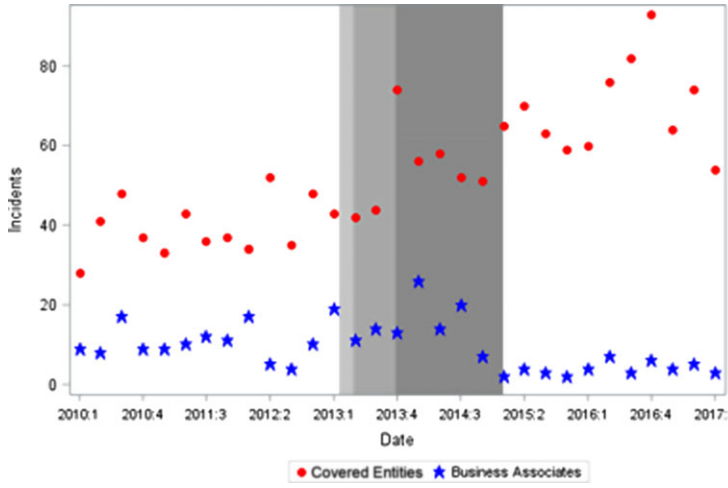


[a]Data derived from authors' analysis of Office for Civil Rights data on breach incidents between October 2009 and August 2017. Incidents described as "Unknown," "Other," or that were missing a description were grouped under the "Other" category. Where the type of an incident was categorized in more than one group by OCR, the incident was assigned to the primary group. For example, an incident OCR described as "Theft/Loss" was categorized under "Theft."

for covered entities was not exercised by attorneys general until after amendments to HIPAA were brought about by the introduction of HITECH in 2010.[24]

After the implementation of the rules in September 2013, both groups experienced an instant spike in breach incidents. Since the increase occurred in both groups, however, while the changes in policy pertained only to the business associates and did not include covered entities, factors other than the shift in policy primarily led to this immediate increase. Note that the immediate increase in the number of breach

Figure 4. Trends of Privacy Breach Incidents Among Covered Entities and Business Associates[a]
[Color figure can be viewed at wileyonlinelibrary.com]



[a]Data derived from authors' analysis of Office for Civil Rights data on breach incidents between January 2010 and August 2017. The light gray area depicts the 1/25/2013-3/25/2013 period, medium gray depicts 3/26/2013-9/23/2013, and dark gray depicts 9/24/2013-12/31/2014. Red dots and blue stars respectively represent regression lines among covered entities and business associates.

incidents is much larger for covered entities. This is also depicted by the widening gap between the number of breaches in the 2 groups, which continued to grow in the months after the policy implementation. These observations show preliminary support for the effects of the HIPAA omnibus rules on breach incidents among business associates.

In the following pages, we present the results of the interrupted time-series analysis. These results confirm our preliminary findings.

As shown in the first panel of Table 1, implementation of the HIPAA omnibus rules had a strong and immediate effect on reducing the number of breaches among business associates by 14.41 units. Utilizing the covered entities as our control group adds insight to our analysis; as

Table 1. The Immediate and Long-Term Effects of HIPAA Omnibus Rules on Privacy Breaches[a]

	Business Associates		Covered Entities		Difference	
	Coefficient	SE	Coefficient	SE	Coefficient	SE
Model 1[b,d,f]						
Intercept	4.9708**	2.3747	32.1735***	5.4357	20.6607***	2.3328
t[c]	0.4171***	0.1206	1.2204***	0.3200	0.9281***	0.1707
Omnibus	−14.4114***	2.5711	8.28210	7.1895	18.2100***	3.6453
t after omnibus	−0.0702	0.3451	−0.3645	1.0177	0.3157	0.5196
Seasonal dummies	Included		Included		Not Included	
AR(3) error terms	Included		Included		Included	
Model 2[c,d,f]						
Intercept	6.9009	4.2022	35.4254***	5.2147	23.6522***	3.5883
t[c]	0.2265	0.3637	0.6982*	0.3965	0.5698*	0.3314
Omnibus	2.3861	4.5728	10.2923*	5.0236	6.1088	4.2006
t after omnibus	−1.2117**	0.4802	0.6257	0.5115	1.9464***	0.4244
Seasonal dummies	Included		Included		Not Included	
AR(3) error terms	Included		Included		Included	

Continued

Table 1. *Continued*

	Business Associates		Covered Entities		Difference	
	Coefficient	SE	Coefficient	SE	Coefficient	SE
Model 3[b,e,f]						
Intercept	0.0000120**	5.7284E-6	0.0000417***	0.000012	0.0001850***	0.000021
t[c]	9.823E-7***	2.8954E-7	3.1494E-6***	5.9675E-7	8.3086E-6***	1.5277E-6
Omnibus	−0.00003***	6.0237E-6	4.74908E-6	0.000010	0.0001630***	0.000033
t after omnibus	−1.6945E-7	8.1135E-7	−4.6215E-7	1.3441E-6	2.82637E-6	4.6517E-6
Seasonal dummies	Included		Included		Not Included	
AR(3) error terms	Included		Included		Included	
Model 4[c,e,f]						
Intercept	0.0000167	0.000010	0.0000673***	9.7894E-6	0.0002117***	0.000032
t[c]	5.46624E-7	8.6509E-7	1.3271E-6*	7.5226E-7	5.10094E-6*	2.9668E-6
Omnibus	5.75741E-6	0.000011	0.0000196*	9.4091E-6	0.0000547	0.000038
t after omnibus	−2.938E-6**	1.1541E-6	1.18936E-6	9.3905E-7	0.0000174***	3.7997E-6
Seasonal dummies	Included		Included		Not Included	
AR(3) error terms	Included		Included		Included	

Abbreviations: SE, standard error; AR(3), Autoregressive model of order 3.
[a]Data derived from authors' analysis of Office for Civil Rights data on breach incidents between January 2010 and August 2017.
[b]The effective date is January 1, 2015.
[c]The effective date is September 23, 2013.
[d]The raw numbers of breach incidents are used as dependent variables.
[e]The ratios of breach incidents to the number of group members are calculated and used as dependent variables. The number of group members for business associates is 414,444, for covered entities is 526,150, and for the difference is 111,706.
[f]Variable *t* denotes the time trend and counts the months since the beginning of the time series, Omnibus is a binary variable that indicates if the rules are in effect (any period after the effective date) and *t* after omnibus counts the number of months since the effective date.
$^{***}p < .01$, $^{**}p < .05$, $^{*}p < .10$

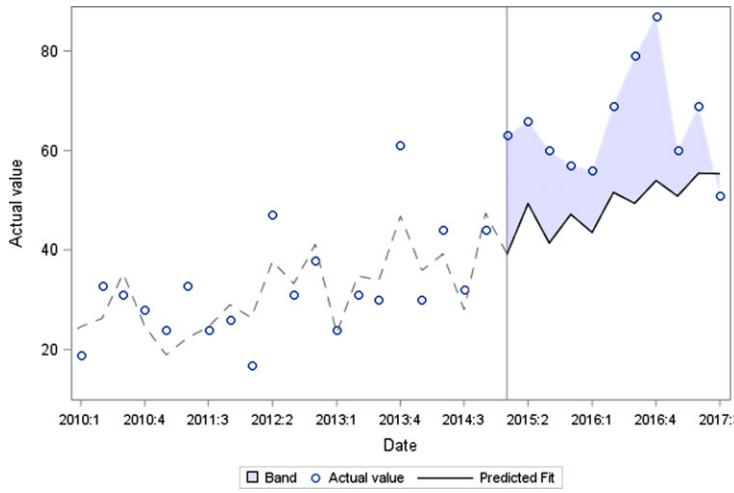
shown in the second panel of Table 1, implementation of the omnibus rules does not have a statistically significant effect on the number of breach incidents among covered entities. This observation provides statistical evidence for the suitability of including covered entities as the control group in our analysis. As shown in the third panel of Table 1, the difference in the number of breaches between covered entities and business associates increases by 18.21 incidents per quarter immediately after the implementation of the rules. In model 2, we considered the compliance deadline (September 23, 2013), rather than the January 2015 date used in model 1, as an effective policy implementation date. Using this alternative effect date, the long-term effects of the omnibus rules are even more salient.

The number of breach incidents is a function of the total number of covered entities and business associates in the health care market. In order to have a better understanding about the effects of the rules, we also examined the ratio of incidents to the number of members in each group. That is, we calculate the ratio of breaches in each group by dividing the number of breaches by the total number of active members and then use the ratios to replicate our interrupted time-series analysis. These estimates are reported under models 3 and 4 in Table 1 and are consistent with those reported in models 1 and 2. In the Appendix, we describe how we determine the total number of covered entities and business associates.

Figure 5 compares the actual and forecasted difference in the number of breach incidents among covered entities and business associates. We calculated the forecasted values based on the observed trend prior to January 2015 and did not consider the immediate or long-term effects of the rules. The dashed line and solid line respectively show the forecasted difference in the number of breach incidents between the 2 groups before and after January 2015. The shaded area shows the difference between the actual number of breaches (shown in blue circles) and the predicted number of breaches had there been no omnibus rules (green line). The actual difference is 180 units more than the forecasted value had the HIPAA omnibus rules not been in effect. That is, the rules have prevented 180 breach incidents among business associates.

Since there were 43 breach incidents among business associates after January 2015, we estimate that in absence of these rules, there would have been 223 breach incidents. Considering that every breach among this group effects on average 98,803 individuals, we estimate

Figure 5. Difference in the Number of Breach Incidents Between Covered Entities and Business Associates With and Without HIPAA Omnibus Rules[a]
[Color figure can be viewed at wileyonlinelibrary.com]



Abbreviations: HIPAA, Health Insurance Portability and Accountability Act; OCR, Office of Civil Rights.
[a]Data derived from authors' analysis of OCR data on breach incidents between January 2010 and August 2017. The dashed line shows the actual difference in number of breaches between business associates and covered entities. The solid line shows the corresponding forecasted values. The lower values on the solid line show that in the absence of omnibus rules, the number of incidents among business associates would have been closer to that of covered entities.

that the HIPAA omnibus rules have protected the privacy of at most 17,784,540 patients since their effects were fully observed in January 2015. Note that an individual's medical records could be breached in multiple incidents and therefore this figure is the highest estimate based on the assumption that individuals affected by each breach are unique. Instances in which the privacy of a single patient is violated in multiple breach incidents would lower our estimate of the total number

Table 2. Difference-in-Differences of Breach Incidents Among Business Associates and Covered Entities Before and After Implementation of Omnibus Rules[a]

	Pre-Omnibus	Post-Omnibus	Difference
Business associates	12.25	3.91	−8.34[b]
	(5.42)	(1.58)	(4.48)
Health care providers	44.60	69.09	24.49[b]
	(10.70)	(11.41)	(10.95)
Difference (business associates – health care providers)			−32.83[b]
			(10.41)

[a]Data derived from authors' analysis of Office for Civil Rights data on breach incidents between January 2010 and August 2017. The values in the pre-omnibus and post-omnibus columns show the average number of quarterly breaches in the 2 groups before and after the implementation of omnibus rule. The values in the third column show the difference between the values in the first two columns. The value in the last row is the difference-in-differences (DID). Significance of the DID values is based on the *t*-test statistic. Standard deviations are shown in parenthesis.

[b]$p < .01$

of individuals whose privacy has been protected as a result of omnibus rules.

Although the exact number of business associates in not known, it should be proportionate to the number of covered entities. The health care market has consistently grown over the period of this study, and the number of both covered entities and their business associates has grown with it. Therefore, the reduction in breach incidents cannot be attributed to a decline in the total number of business associates.

As a robustness test, we also implement a difference-in-differences design to estimate the changes in average quarterly privacy breaches from the pre-implementation period to the post-implementation period of the HIPAA omnibus rules among the business associates compared to concurrent incidents among the covered entities.

As shown in Table 2, the average number of breaches per quarter among business associates decreases by 8.34 units after January 2015. Alternatively, the average number of quarterly breach incidents among covered entities increases by 24.49 units. The difference in differences is a

reduction of 32.83 in the average number of breaches per quarter. These results are consistent with our findings from the former analyses and further confirm the role of the omnibus rules in reducing the frequency of breach incidents.

Discussion

We observe that unlike business associates, covered entities have experienced a growing number of breach incidents throughout the study period. This becomes more worrisome as sophisticated ransomware attacks have recently emerged as a new threat to security and privacy in the health care sector.[25] Further research is required to investigate the reasons for the alarming growth of breaches among covered entities. Moreover, we observe a significant variation in the number of incidents across states. For example, while there are only 0.68 breach incidents per 100,000 physicians in the state of Maine, there are 6.16 incidents per 100,000 physicians in the state of Wyoming. Uncovering the drivers of this state-level variation in the number of incidents could be an interesting domain for future research.

The findings of this research are particularly relevant to 2 recent federal policies. First, the OCR recently announced that it now investigates smaller breach incidents that affect fewer than 500 individuals.[26] Given the volume of resources required to conduct such audits, it is necessary to have an understanding of their potential benefits. This research estimates the effects of the omnibus rules and therefore enables the regulators to conduct a cost-benefit analysis of their decision to enforce the rules on smaller breaches. Given the findings of this research about the positive role of omnibus rules on reducing breach incidents among business associates, the OCR's decision to enforce the regulation on smaller breach incidents should lead to an even lower number of breach incidents among both covered entities and business associates. While this study reveals the benefits of the omnibus rules, OCR should also carefully examine the enforcement and compliance costs of omnibus rules in order to have a comprehensive analysis of the costs and benefits of further expansion and stricter enforcement.

Second, the Substance Abuse and Mental Health Services Administration (SAMHSA) has proposed an update to the Confidentiality of Alcohol and Drug Abuse Patient Records, Title 42 of the Code of Federal Regulations (42 CFR).[27] Given the social stigma and sensitivity of

the records of alcohol and drug abuse, SAMHSA is proposing stricter regulations to ensure that entities that collect and hold such records adequately protect their patients' privacy. Interestingly, the proposal only includes a negligible criminal penalty of "$500 in the case of a first offense and not more than $5,000 in the case of each subsequent offense." In comparison to penalties for HIPAA violations (which can be as much as $1.5 million), the penalties proposed in 42 CFR are very small. Further research is required to investigate the effect of penalty size on the rate of compliance and subsequent effectiveness of the policy.

Limitations

This study has several limitations. First, the observations in our data set are limited to the incidents that affected more than 500 individuals. Many smaller breaches affect fewer than 500 patients. These incidents are not reported by OCR and thus are not included in our analysis.

Second, in rare cases, organizations may not immediately realize that they have been a victim of a privacy breach and therefore may report such incidents to the OCR with some time lag. To overcome this limitation, we conduct a difference-in-differences analysis. In this method, because we use the incidents over the whole intervals before and after January 2015, rather than using the incidents per a specific and fixed quarterly interval, the estimates do not suffer from the possible time difference between an incident's occurrence and reporting dates.

Third, the interrupted time-series analysis assumes that the 2 groups are similar and independent. Covered entities have more direct exposure to patients and are more likely to house large data sets that would be subject to a breach notification. Business associates operate in a different environment than covered entities. They may not focus solely on health care and may provide services to clients other than health care providers. This difference between the 2 groups may undermine the assumption of independence and similarity of the groups in the interrupted time-series analysis. However, visual inspection of the trends of breaches in the 2 groups shows that before the implementation of the rules, they were parallel; after the implementation, they diverge. Also, when we analyze the effect of the policy on business associates only (rather than looking at the difference between business associates and covered entities), we observe a significant drop in the number of breaches.

Finally, while this study uncovers the benefits of the omnibus rules, further studies are warranted to examine the enforcement and compliance costs of the omnibus rules by, respectively, OCR and business associates.

Conclusion

To the best of our knowledge, this is the first study that examines the effects of the HIPAA omnibus rules on reducing the frequency of privacy breaches among business associates. Our results indicate that implementation of the rules could have led to a significant decrease in the number of incidents and thus has protected millions of Americans from unwanted privacy exposures. Therefore, we conclude that the federal policy appears to have achieved its intended goal of enhancing privacy protection efforts and reducing the number of breach incidents among business associates.

References

1. Moskop JC, Marco CA, Larkin GL, Geiderman JM, Derse AR. From Hippocrates to HIPAA: privacy and confidentiality in emergency medicine—part I: conceptual, moral, and legal foundations. *Ann Emerg Med*. 2005;45(1):53-59. https://doi.org/10.1016/j.annemergmed.2004.08.008.
2. Annas GJ. HIPAA regulations—a new era of medical-record privacy? *N Engl J Med*. 2003;348(15):1486-1490.
3. Choi YB, Capitan KE, Krause JS, Streeper MM. Challenges associated with privacy in health care industry: implementation of HIPAA and the security rules. *J Med Syst*. 2006;30(1):57-64. https://doi.org/10.1007/s10916-006-7405-0.
4. Berner ES, Detmer DE, Simborg D. Will the wave finally break? A brief view of the adoption of electronic medical records in the United States. *J Am Med Inform Assoc*. 2005;12(1):3-7. https://doi.org/10.1197/jamia.M1664.
5. Steward M. Electronic medical records: privacy, confidentiality, liability. *J Leg Med*. 2005;26(4):491-506. https://doi.org/10.1080/01947640500364762.
6. Hirsch R, Deixler H. Final HIPAA Omnibus Rule brings sweeping changes to health care privacy law: HIPAA privacy and security obligations extended to business associates and subcontractors. *BNA Priv Secur Law Rep*. 2013;12(PVLR 168):1-11.

7. Wang CJ, Huang DJ. The HIPAA conundrum in the era of mobile health and communications. *JAMA*. 2013;310(11):1121-1122. https://doi.org/10.1001/jama.2013.219869.
8. Rothstein MA. The Hippocratic bargain and health information technology. *J Law Med Ethics*. 2010;38(1):7-13. https://doi.org/10.1111/j.1748-720X.2010.00460.x.
9. Yasnoff WA, Sweeney L, Shortliffe EH. Putting health IT on the path to success. *JAMA*. 2013;309(10):989-990. https://doi.org/10.1001/jama.2013.1474.
10. DeVore S, Champion RW. Driving population health through accountable care organizations. *Health Aff (Millwood)*. 2011;30(1):41-50. https://doi.org/10.1377/hlthaff.2010.0935.
11. Miller RH, Sim I. Physicians' use of electronic medical records: barriers and solutions. *Health Aff (Millwood)*. 2004;23(2):116-126. https://doi.org/10.1377/hlthaff.23.2.116.
12. Yaraghi N, Sharman R, Gopal RD, Ramesh R. Drivers of information disclosure on health information exchange platforms: insights from an exploratory empirical study. *J Am Med Inform Assoc*. 2015;22(6):1183-1186.
13. Yaraghi N. *Hackers, Phishers, and Disappearing Thumb Drives: Lessons Learned From Major Health Care Data Breaches*. Washington, DC: The Brookings Institution; 2016. https://scholar.google.com/citations?view_op=view_citation&hl=en&user=jbq8JnkAAAAJ&citation_for_view=jbq8JnkAAAAJ:5nxA0vEk-isC. Accessed January 10, 2017.
14. Cases currently under investigation. US Department of Health & Human Services, Office for Civil Rights website. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed February 1, 2017.
15. Wagner AK, Soumerai SB, Zhang F, Ross-Degnan D. Segmented regression analysis of interrupted time series studies in medication use research. *J Clin Pharm Ther*. 2002;27(4):299-309.
16. Singhal A, Caplan DJ, Jones MP, et al. Eliminating Medicaid adult dental coverage in California led to increased dental emergency visits and associated costs. *Health Aff (Millwood)*. 2015;34(5):749-756.
17. McGinty EE, Busch SH, Stuart EA, et al. Federal parity law associated with increased probability of using out-of-network substance use disorder treatment services. *Health Aff (Millwood)*. 2015;34(8):1331-1339.
18. Patrick SW, Fry CE, Jones TF, Buntin MB. Implementation of prescription drug monitoring programs associated with reductions

in opioid-related death rates. *Health Aff (Millwood)*. 2016;35(7):1324-1332.

19. Penfold RB, Zhang F. Use of interrupted time series analysis in evaluating health care quality improvements. *Acad Pediatr*. 2013;13(6):S38-S44.
20. Hyndman RJ. Yule-Walker estimates for continuous-time autoregressive models. *J Time Ser Anal*. 1993;14(3):281-296.
21. Total professionally active physicians. Kaiser Family Foundation website. http://kff.org/other/state-indicator/total-active-physicians. Published February 3, 2017. Accessed February 3, 2017.
22. Soumerai SB, Ross-Degnan D, Kahn JS. Effects of professional and media warnings about the association between aspirin use in children and Reye's syndrome. *Milbank Q*. 1992;70(1):155-182. https://doi.org/10.2307/3350088.
23. Lu CY, Zhang F, Lakoma MD, et al. Changes in antidepressant use by young people and suicidal behavior after FDA warnings and media coverage: quasi-experimental study. *BMJ*. 2014;348:g3596. https://doi.org/10.1136/bmj.g3596.
24. Connecticut attorney general first to take action for HIPAA violations. *HIPAA J*. July 7, 2010. https://www.hipaajournal.com/connecticut-attorney-general-first-take-action-hipaa-violations. Accessed October 13, 2017.
25. Green M. Hospitals are hit with 88% of all ransomware attacks. *Becker's Hosp Rev*. July 27, 2016. http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html. Accessed February 7, 2017.
26. Snell E. OCR aims to improve smaller data breach investigation process. *Health IT Secur*. August 22, 2016. http://healthitsecurity.com/news/ocr-aims-to-improve-smaller-data-breach-investigation-process. Accessed February 7, 2017.
27. Substance Abuse and Mental Health Services Administration (SAMHSA), HHS. *Confidentiality of Substance Use Disorder Patient Records*. 2016:6987-7024. https://www.federalregister.gov/documents/2016/02/09/2016-01841/confidentiality-of-substance-use-disorder-patient-records. Accessed February 8, 2017.
28. Special Projects Staff SSSD. North American Industry Classification System (NAICS) Main Page. Executive Office of the President; 2017. https://www.census.gov/eos/www/naics. Accessed October 13, 2017.
29. US Census Bureau. Statistics of US Businesses (SUSB). https://www.census.gov/programs-surveys/susb.html. Accessed October 13, 2017.

Funding/Support: This study was generously funded by California Health Care Foundation.

Conflict of Interest Disclosures: Both authors have completed and submitted the ICMJE Form for Disclosure of Potential Conflicts of Interest. No conflicts were reported.

Address correspondence to: Niam Yaraghi, School of Business, University of Connecticut, 1 University Pl, Stamford, CT 06901 (email: niam.yaraghi@uconn.edu).

Appendix

Identifying the total number of covered entities: Following the HIPAA definition of covered entities, we identify the businesses that provide health care and medical insurance services. We use the North American Industry Classification System (NAICS)[28] to determine the industry codes that encompass such businesses, and then use the data set of Statistics of US Businesses (SUSB)[29] provided by the US Census Bureau to determine the number of businesses in the United States that are active within those NAICS codes. As shown in Table A1, the total number of businesses that are considered as covered entities is equal to 526,150.

Table A1. Number of Active Covered Entities by NAICS Code

NAICS Code	NAICS Description	Number of Active Businesses
621	Ambulatory health care services	483,522
622	Hospitals	3,293
623	Nursing and residential care facilities	38,455
524114	Direct health and medical insurance carriers	880
Total		526,150

Identifying the total number of business associates: It is more difficult to identify the total number of business associates because under HIPAA

any business, regardless of its type of services, is considered a business associate as long as it does business with a covered entity. Therefore, theoretically all active businesses in the United States could be considered a business associate.

To overcome this issue and create a manageable list of business associates, we first identified the NAICS codes of all of the business associates that were reported to have a breach by OCR. This was done by manually searching for the business name on the sidecode.com and manta.com websites. After we compiled the NAICS codes of all the business associates, we identified the top 20 most frequent NAICS codes among them. We then identified the number of active businesses within each of the top 20 NAICS codes from the SUSB data set. We acknowledge the fact that this list is not comprehensive as any company with a different NAICS code could enter into a business associate agreement with a covered entity. However, this list is a pragmatic solution because it covers the industry sectors that are most common among current business associates. As shown in Table A2, the total number of businesses who are considered as a business associate is equal to 414,444.

Table A2. Number of Active Business Associates by NAICS Code

NAICS Code	NAICS Description	Number of Active Businesses
323111	Commercial printing (except screen and books)	17,681
423450	Medical, dental, and hospital equipment and supplies merchant wholesalers	7,370
492110	Couriers and express delivery services	4,399
511210	Software publishers	6,757
518210	Data processing, hosting, and related services	9,565
524291	Claims adjusting	3,389
524292	Third-party administration of insurance and pension funds	2,773

Continued

Table A2. *Continued*

NAICS Code	NAICS Description	Number of Active Businesses
541211	Offices of certified public accountants	53,332
541219	Other accounting services	37,918
541511	Custom computer programming services	62,768
541512	Computer systems design services	41,382
541611	Administrative management and general management consulting services	67,541
541612	Human resources consulting services	6,270
541618	Other management consulting services	8,878
541860	Direct mail advertising	2,403
541990	All other professional, scientific, and technical services	16,230
561110	Office administrative services	29,020
561410	Document preparation services	3,801
561990	All other support services	11,727
624190	Other individual and family services	21,240
Total		414,444