B | Center for Technology Innovation at BROOKINGS

MARCH 2017

Profiles in patient privacy protection

How HIPAA omnibus rules effectively reduced the number of data breaches among health care providers' business associates

Niam Yaraghi and Ram Gopal

Niam Yaraghi is a Fellow in the Brookings Institution's Center for Technology Innovation. He is an expert on the economics of health information technologies.

Ram Gopal is the GE Capital Endowed Professor of Business and Chair of the Operations and Information Management Department at the University of Connecticut's School of Business.

INTRODUCTION

Patient privacy and the protection of confidential information are vital elements of the patient-physician relationship. They ensure the patient autonomy and trust in physicians, without which patients would be much less likely to seek medical care.[1] Over the past two decades, these values have been primarily governed and protected under the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[2] The new privacy regulations of the Health Insurance Portability and Accountability Act of 1996 (HIPAA Recent digitization of the U.S. health care system, however, has led to unprecedented challenges with regards to patient privacy, as more personal information is being collected, archived, and transmitted electronically between multiple parties.[3–5] Responding to these challenges, the Office for Civil Rights (OCR) at the Department of Health and Human Services (HHS), implemented the most significant changes to the 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. The omnibus rules expanded the reach of HIPAA to include all *business associates* that "create, receive, maintain, or transmit protected health information." After the implementation of the omnibus rules, business associates not only had to comply with HIPAA, but more importantly, could potentially be held civilly and criminally liable in the 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— they have been taking 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 technology. As medical science advances and health care systems become more complex, an increasing number of professionals are involved in a

patient's medical care and need to have access to confidential information. For example, many modern technologies and health care managerial plans rely on the free flow of data between different parties. The professionals managing these technologies and programs are not caregivers and do not directly provide medical services to patients, but they facilitate the provision of medical care by increasing efficiency in management and administration—and their access to confidential information is necessary. However, unless the confidentiality of patients' information is taken seriously and adequate protections are put in place to safeguard privacy, many patients will remain reluctant to share their medical information with those who are not directly involved in their care. Without addressing patients' privacy concerns, then, technologies such as health information exchanges and economic and managerial plans such as accountable care organizations will not succeed.[9–12]

> As medical science advances and health care systems become more complex, an increasing number of professionals are involved in a patient's medical care and need to have access to confidential information.

Despite the theoretical importance of privacy, prior to the omnibus rules, the business associates of covered entities did not have strong market-based incentives to protect patients' privacy.[13] The HIPAA omnibus rules filled this gap by holding business associates to the same standards as covered entities. In addition, by creating civil and criminal penalties to hold them accountable, the omnibus rules incentivized business associates to comply with HIPAA and safeguard patients' privacy. Had this happened sooner, it could have potentially prevented some privacy breaches from occurring. The purpose of this research is to investigate the extent to which the implementation of the HIPAA omnibus rules have reduced the frequency of privacy breaches among business associates.

STUDY DATA & METHODS

DATA SOURCE

To conduct our analysis, we use publicly available data reported by OCR.[14] The dataset lists all of the privacy breach incidents in the United States between October 2009 and January 2017 that have affected more than 500 individuals.

STUDY DESIGN

To study the effects of the implementation of HIPAA omnibus rules on the frequency of privacy breaches among business associates, we conduct an interrupted time-series design 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. The covered entities are akin to the control group in a randomized controlled trial. They have complied 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 among them. In other words, the frequency of breach incidents among covered entities should not be affected by the implementation of the omnibus rules, but could be affected by factors unrelated to this study, such as increased adoption levels of electronic health record systems.

On the other hand, business associates are akin to the treatment group in a randomized controlled trial. Since they were the focus of the new policy, we can assume that the implementation of the HIPAA omnibus rules have reduced the frequency of privacy breaches among them. 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 numbers of privacy breaches in the two groups as our dependent variable. For example, 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. Examining the difference in the breach incidents of the two groups, rather than focusing on the breach incidents of only one group, allows us to detect and account for other trends that are unrelated to the implementation of HIPAA omnibus rules. This statistical method, interrupted time-series analysis, is the strongest 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

We first conduct an interrupted time-series analysis using months as our time units. In this analysis, the dependent variable is the difference between the number of privacy breaches in the two groups of business associates and covered entities in a time interval. We fit the dependent variable in each period as a function of three explanatory variables. First, a continuous variable that counts the periods since the start of the time-series. The coefficients of this variable capture the time trends. Second, a binary variable that indicates the shift in policy. This variable is equal to one if the period is post implementation of the HIPAA omnibus rules and zero if the period is before the implementation of omnibus rules. The coefficient of the binary variable indicates whether there is a change in the outcome variable immediately after implementing the rules. Third, a continuous variable that counts the number of periods after the implementation of the HIPAA omnibus rules. The value of this variable in periods before the implementation of the rules is equal to zero. The coefficient of this variable indicates whether there is a change in slope of the outcomes in the period 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] and use the AUTOREG[20] procedure available in the SAS software to test and account for correlation in our dataset by including first order autoregressive parameters in our model.[21]

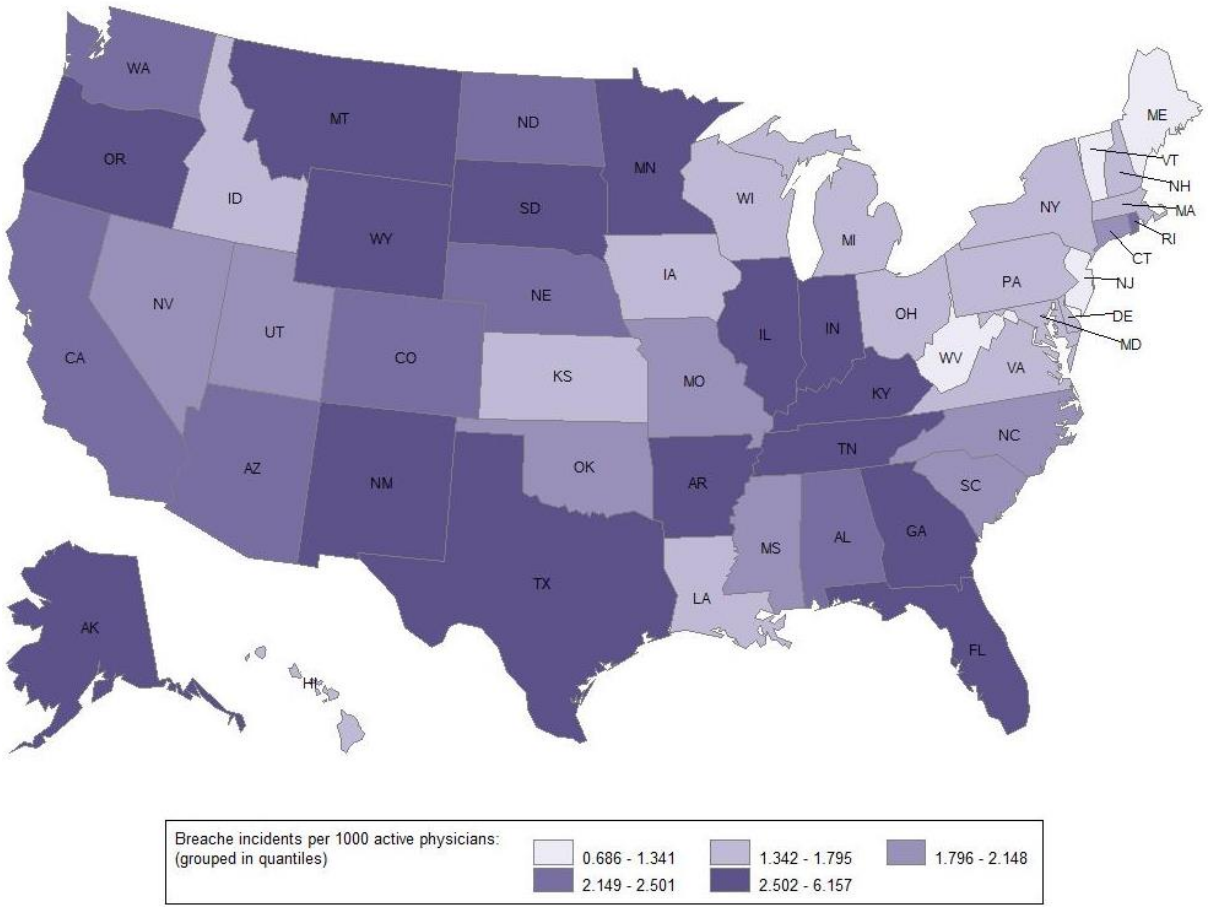
LIMITATIONS

There are two limitations to this study. First, the observations in our dataset are limited to data breach incidents that affected more than 500 individuals. Many smaller breaches affect fewer than 500 patients, but incidents are not reported by OCR and thus are not included in our analysis. Second, in some rare cases, organizations may not immediately realize that they have been the victim of a privacy breach and therefore may report such incidents to OCR with some time lag. To overcome this limitation, we conduct a difference-in-differences (DID) analysis. Because we use the incidents over the whole time interval before and after the policy implementation rather than using the incidents per a specific and fixed time interval such as month or quarter, the estimates in this method do not suffer from the possible time difference between an incident's occurrence and reporting dates.

STUDY RESULTS

During the six-year study period, 1,819 breach incidents occurred, of which 279 incidents happened among business associates. The remaining incidents occurred among covered entities, which, according to HIPAA definitions, include health care providers (1,255 incidents), health plans (230 incidents) and health care clearing houses (four incidents). As shown in Exhibit 1, on average, 2.08 privacy breach incidents take place per 1,000 professionally active physicians in the U.S. Exhibits 2 and 3 show the frequency of different types of breaches and the number of patients who are affected by incidents enabled by covered entities and business associates, respectively. As shown in these exhibits, the average breach incident from a covered entity affects 94,922 individuals, while the average breach incident from a business associate affects 102,563 individuals. So far, these breaches combined have undermined the privacy of 171,283,113 patients in the United States.

EXHIBIT 1: Distribution of privacy breach incidents per 1,000 professionally active physicians in the U.S.



SOURCE: Authors' analysis of OCR data on breach incidents between October 2009 and January 2017.

NOTES: 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 Henry J. Kaiser Family Foundation.[25] The five color groups on the map represent the quantiles of the calculated breach incidents per 1000 physicians.

EXHIBIT 2: Types of privacy breach incidents and the number of patients affected by them, among covered entities

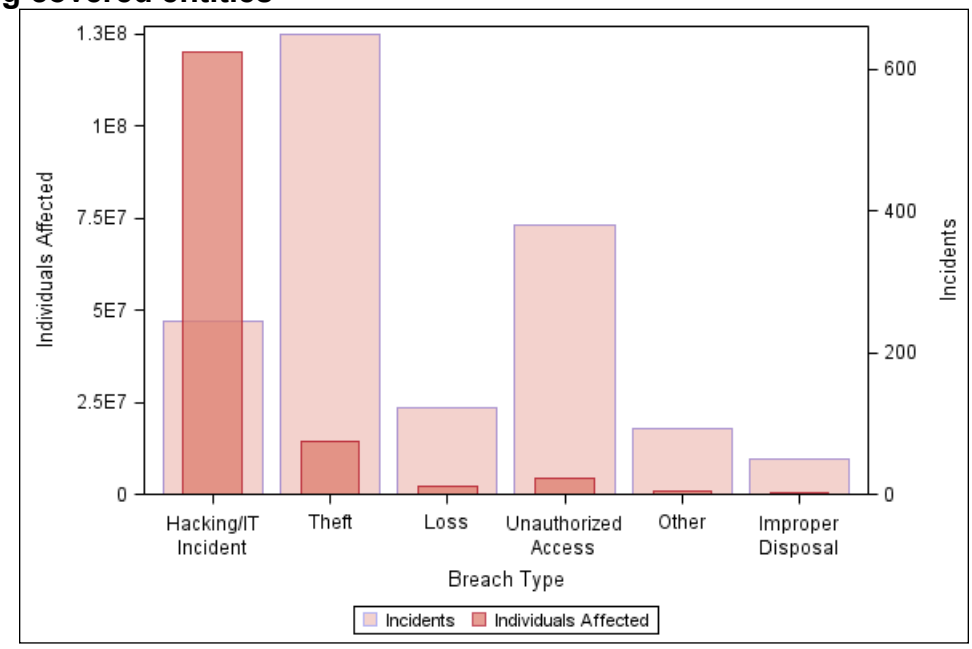
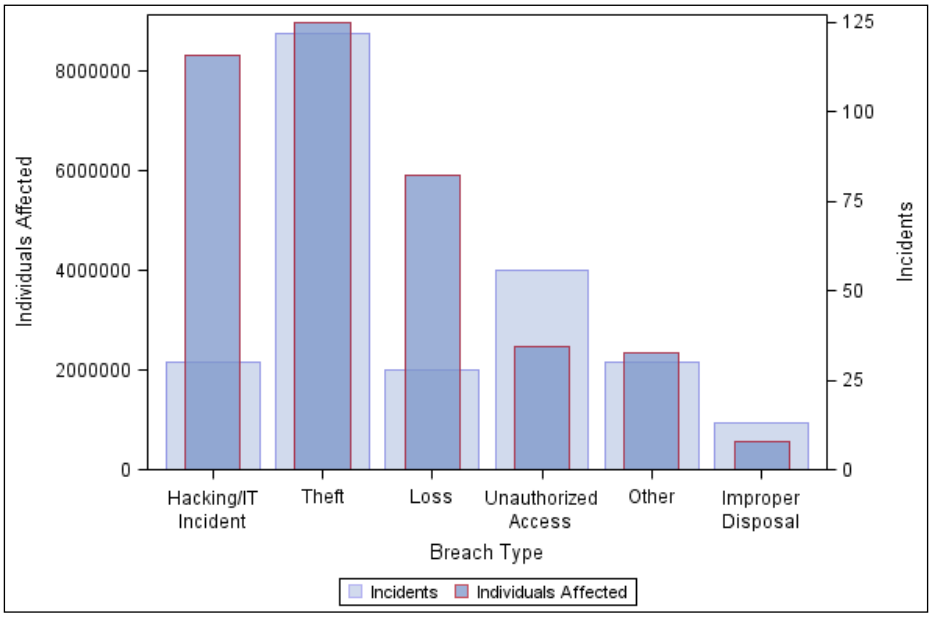


EXHIBIT 3: Types of privacy breach incidents and the number of patients affected by them, among business associates



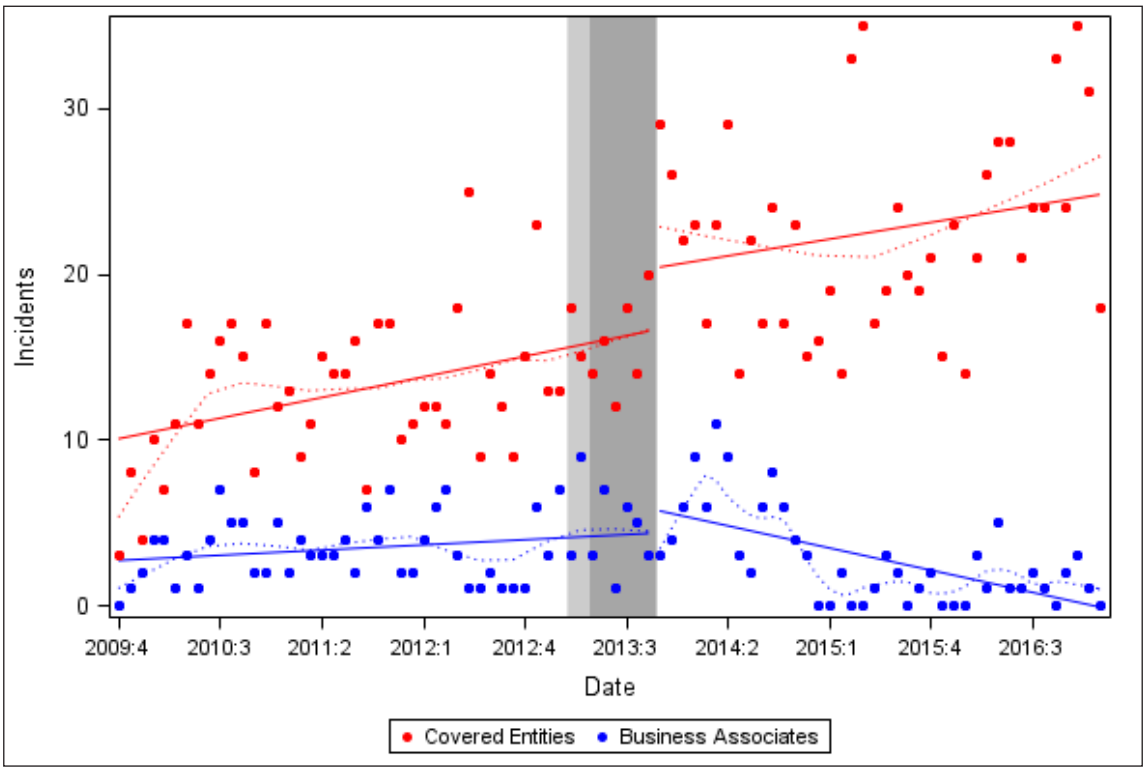
SOURCE: Authors' analyses of OCR data on breach incidents between October 2009 and January 2017.

NOTES: Incidents that were described as "Unknown", "Other", or had a missing description were grouped together under the "Other" category. In cases were the type of an incident was categorized in more than one group by OCR, the incident has been assigned to the primary group. For example, we authors categorized an incident that OCR describes as "Theft/Loss" under "Theft".

OCR announced the HIPAA omnibus rules on January 25, 2013. These rules became effective March 26, 2013, with compliance required by September 23, 2013.[6] Exhibit 4 illustrates this period in the gray shaded area. As shown there, privacy breaches occurred at a relatively constant rate of 3.3 incidents per-month among business

associates before the implementation of the rules, while privacy breaches occurred at an increasing rate among the covered entities during that same time. After the implementation of the rules, breach incidents among both of the groups experienced an instant spike. We can assume that factors other than the shift in policy lead to this immediate increase because it occurred in both groups, while the change in policy only pertained to the business associates. Note that the immediate increase in the number of breach incidents is much larger among covered entities. This is depicted by the widening gap between the number of breaches in the two groups, which continues 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 section, we present the results of the interrupted time series analysis. These results confirm our preliminary findings.

EXHIBIT 4: Trends of privacy breach incidents among covered entities and business associates



SOURCE: Authors' analysis of OCR data on breach incidents between October 2009 and January 2017.

NOTES: Light gray area depicts 1/25/2013-3/25/2013 period. Dark gray area depicts 3/26/2013-9/23/2013 period. Red and blue solid lines respectively represent regression lines among covered entities and business associates

As shown in the first panel of Exhibit 5, implementation of the HIPAA omnibus rules seems to have an immediate effect on the number of breaches among business associates; however, over time, it leads to a decreasing trend in the occurrence of breaches. Utilizing the covered entities as our control group adds insights to our analysis. As shown in the second panel of Exhibit 5, the average number of breaches among covered entities increases by 3.75 units immediately after the full implementation of the omnibus rules. This effect indicates that there are factors other than the omnibus rules in play and that the compliance deadline of the omnibus rules coincided with a spike in the number of privacy breaches in the health care market. Based on this observation, one could argue that had the omnibus rules not been in place, we would have observed a similar spike in the number of privacy breaches among business associates. In the absence of omnibus rules, we would have expected the business associates to experience

privacy breaches in a trend similar to that of covered entities, as they were before the announcement of the rules. In other words, implementation of the rules has dampened the effects of an otherwise powerful driver of privacy breaches among business associates. The long-term effects of the rules are more salient in subsequent periods. As shown in third panel of Exhibit 5, the difference in breaches between covered entities and business associates continues to grow by 0.16 units per-month over time. We redo our analysis using different times as effective policy implementation dates. In model two, we consider the beginning of the implementation period and in model three, we consider the announcement date, as our as alternative effective dates for policy implementation. As shown in Exhibit 5, the results from these models are consistent with those of model one.

EXHIBIT 5: The immediate and long-term effects of HIPAA omnibus rules on privacy breaches

	Business Associates	Covered Entities	Difference
Model 1			
Intercept	2.5433*** (0.8428)	9.8839*** (1.4287)	7.2349*** (1.4572)
t	0.0388 (0.0298)	0.1382*** (0.0508)	0.1035** (0.0518)
Omnibus	1.3557 (1.2022)	3.7497* (2.0934)	2.2391 (2.1351)
t after Omnibus	-0.1850*** (0.1057)	-0.0258 (0.0838)	0.1578* (0.0855)
Model 2			
Intercept	2.5048*** (0.9023)	9.7456*** (1.5540)	7.1231*** (1.5657)
t	0.0422 (0.0365)	0.1480** (0.0630)	0.1117* (0.0634)
Omnibus	1.4165 (1.2162)	1.5264 (2.1086)	-0.0650 (2.1245)
t after Omnibus	-0.1604*** (0.0487)	0.0300 (0.0836)	0.1849** (0.0842)
Model 3			
Intercept	2.7377*** (0.8995)	9.8077*** (1.5940)	6.9654*** (1.6057)
t	0.0265 (0.0381)	0.1435* (0.0678)	0.1224* (0.0683)
Omnibus	2.1666* (1.1801)	1.4415 (2.1122)	-0.8755 (2.1277)
t after Omnibus	-0.1456*** (0.0482)	0.0388 (0.0851)	0.1791* (0.0858)

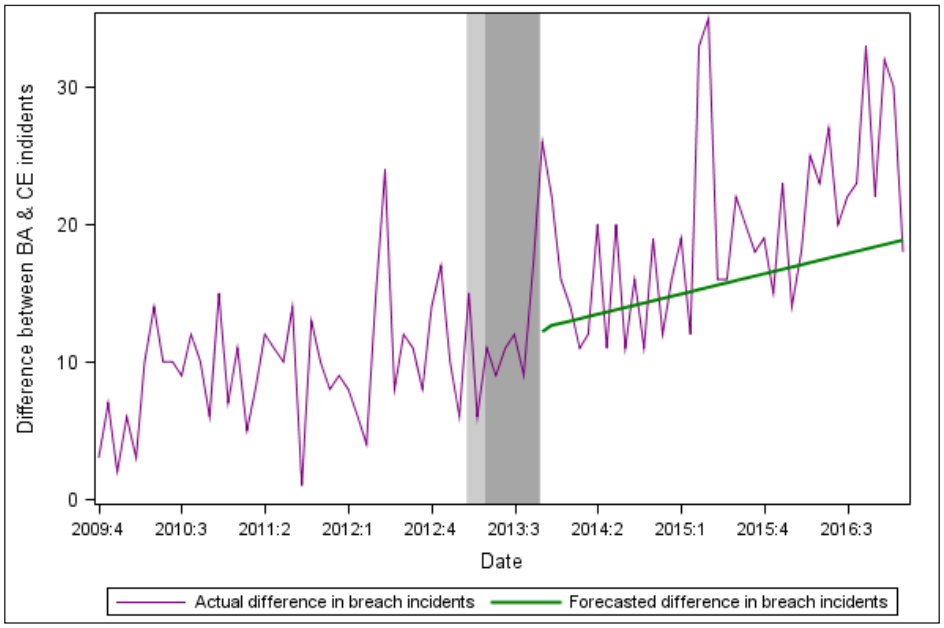
SOURCE: Authors' analysis of OCR data on breach incidents between October 2009 and January 2017.

*NOTES: In model 1, the effective date is the compliance deadline (09/23/2013). In model 2, the effective date is the beginning of the implementation period (03/26/2013). In model 3, the effective date is the announcement date (01/25/2013). In all models, variable denotes the time trend and counts the months since the beginning of the time series, is a binary variable that indicates if the rules are in effect (any period after the effective date) and counts the number of months since the effective date. ***: P<0.01 **: p<0.05 *: p<0.10. Standard errors are shown in parentheses.*

Exhibit 6 compares the actual and forecasted differences of breach incidents among covered entities and business associates. We calculated the forecasted values based on the observed trend prior to the implementation date of the omnibus rules and did not consider the immediate or long-term effects of the rules. The purple and green line

respectively show the actual and forecasted difference in breach incidents between the two groups. The actual difference is 165 units more than the forecasted value had the HIPAA omnibus rules not been enacted. That is, the rules have prevented 165 breach incidents among business associates. Considering that every breach among this group on average affects 102,563 individuals, we estimate that the HIPAA omnibus rules have protected the privacy of 16,922,895 patients since their implementation on September 23, 2013.

EXHIBIT 6: Difference in breach incidents between covered entities and business associates, with and without HIPAA omnibus rules



SOURCE: Authors' analysis of OCR data on breach incidents between October 2009 and January 2017.

NOTES: The purple line shows the actual difference in number of breaches between business associates and covered entities. The green line shows the corresponding forecasted values. The lower values on the green line shows that in the absence of omnibus rules, the number of incidents among business associates would have been closer to that of covered entities.

Considering that every breach among this group on average affects 102,563 individuals, we estimate that the HIPAA omnibus rules have protected the privacy of 16,922,895 patients since their implementation

As a robustness test, we also implement a difference-in-differences design to estimate the changes in average monthly privacy breaches from the pre-implementation period to the post-implementation period of the HIPAA omnibus rules among business associates compared to concurrent incidents among covered entities. As shown in Exhibit 7, the average number of breaches per-month among business associates is reduced by 0.73 units after the implementation of the rules. On the other hand, the average monthly breach incidents among covered entities increases by 9.30 units. The difference-in-differences is a reduction of 10.03 in the average number of breaches. 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.

EXHIBIT 7: Difference-in-differences of breach incidents among business associates and covered entities, before and after implementation of omnibus rules

	Pre Omnibus	Post Omnibus	Difference
Business Associates (BA)	3.57 (2.10)	2.84 (2.88)	-0.73 (2.49)
Health Care Providers (HC)	13.27 (4.35)	22.57 (5.88)	9.30*** (5.10)
Difference (HC-BA)			**-10.03***** (5.43)

SOURCE: Authors' analysis of OCR data on breach incidents between October 2009 and January 2017.

*NOTES: The values in the pre omnibus and post omnibus columns show the average number of monthly breaches in the two 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. ***: p<0.01 **: p<0.05 *: p<0.10*

DISCUSSION

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 has 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 has achieved its intended goal of enhancing privacy protection efforts and reducing the number of breach incidents among business associates.

Unlike business associates, we observe that 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.[22] Further research is required to investigate the reasons for the alarming growth of breaches among covered entities. Moreover, we observe a significant variation in 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 the same number of physicians in the state of Wyoming. Uncovering the drivers of this state-level variation in the number of incidents can be an interesting domain for future research.

Given the findings of this research about the positive role of the omnibus rules on reducing breach incidents among business associates, the OCR's decision to enforce the regulation on smaller breach incidents should lead to even lower numbers of breach incidents among both covered entities and business associates.

The findings of this research are particularly relevant to two recent federal policies. First, OCR recently announced that it now investigates smaller breach incidents that affect less than 500 individuals.[23] 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 the omnibus rules on reducing breach incidents among business associates, the OCR's decision to enforce the regulation on smaller breach incidents should lead to even lower numbers of breach incidents among both covered entities and business associates.

Without serious violation penalties, the Substance Abuse and Mental Health Service Administration cannot enforce these regulations appropriately and may not achieve their intended purpose to protect patients' privacy.

Second, our findings have bearing on the Substance Abuse and Mental Health Service Administration's (SAMHSA) proposed update to the Confidentiality of Alcohol and Drug Abuse Patient Records, Title 42 of the Code of Federal Regulations (42 CFR).[24] Given the social stigma and sensitivity of records pertaining to 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 levied against HIPAA violations (which can total as much as $1.5 million), the penalties proposed in 42 CFR appear to be insufficient. The guidelines provided in the proposed regulations are effective only when providers comply with them. In the absence of adequate penalties for noncompliance, providers do not have strong financial incentives to bear the costs of compliance. Without serious violation penalties, SAMHSA cannot enforce these regulations appropriately and may not achieve their intended purpose to protect patients' privacy.

CONCLUSION

The results of this research provide evidence that implementation of the HIPAA omnibus rules has led to a significant decrease in the number of privacy breach incidents among business associates. The success of national reforms in the finance and administration of health care services hinges on the free and secure flow of data in a connected and digitized health care system, and protecting the privacy of patients is more important now than ever before. The findings of this research shed light on the benefits of privacy-protecting regulations and inform government on how to design and implement policies and regulations to enhance privacy protections in the health care system.

ENDNOTES

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 Jan;45(1):53–9.
2. Annas GJ. HIPAA regulations--a new era of medical-record privacy? N Engl J Med. 2003 Apr 10;348(15):1486–90.
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 Feb 1;30(1):57–64.
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 Jan 1;12(1):3–7.
5. Steward M. Electronic Medical Records: Privacy, Confidentiality, Liability. J Leg Med. 2005 Dec 1;26(4):491–506.
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 Feb 4;12(PVLR 168):1–11.
7. Wang CJ, Huang DJ. The HIPAA conundrum in the era of mobile health and communications. JAMA. 2013 Sep 18;310(11):1121–2.
8. Rothstein MA. The Hippocratic Bargain and Health Information Technology. J Law Med Ethics. 2010 Mar 1;38(1):7–13.
9. Yasnoff WA, Sweeney L, Shortliffe EH. Putting Health IT on the Path to Success. JAMA. 2013 Mar 13;309(10):989–90.
10. DeVore S, Champion RW. Driving Population Health Through Accountable Care Organizations. Health Aff (Millwood). 2011 Jan 1;30(1):41–50.
11. Miller RH, Sim I. Physicians' Use Of Electronic Medical Records: Barriers And Solutions. Health Aff (Millwood). 2004 Mar 1;23(2):116–26.
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):1183–6.
13. Yaraghi N. Hackers, phishers, and disappearing thumb drives: Lessons learned from major health care data breaches [Internet]. The Brookings Institution; 2016 May [cited 2017 Jan 10]. Available from: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=jbq8JnkAAAAJ&citation_for_view=jbq8JnkAAAAJ:5nxA0vEk-isC
14. U.S. Department of Health & Human Services - Office for Civil Rights [Internet]. [cited 2017 Feb 1]. Available from: https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf
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, Momany ET, Kuthy RA, Buresh CT, et al. Eliminating Medicaid adult dental coverage in California led to increased dental emergency visits and associated costs. Health Aff (Millwood). 2015;34(5):749–56.

17. McGinty EE, Busch SH, Stuart EA, Huskamp HA, Gibson TB, Goldman HH, 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):1331–9.

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):1324–32.

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. SAS Institute. The AUTOREG Procedure. In: SAS/ETS 92 User's Guide [Internet]. Cary, NC: SAS Institute; 2008 [cited 2017 Feb 7]. Available from: https://support.sas.com/rnd/app/ets/procedures/ets_autoreg.html

21. Hyndman RJ. Yule-Walker Estimates for Continuous-Time Autoregressive Models. J Time Ser Anal. 1993;14(3):281–96.

22. Max Green. Hospitals are hit with 88% of all ransomware attacks. Becker's Hospital Review [Internet]. 2016 Jul 27 [cited 2017 Feb 7]; Available from: http://www.beckershospitalreview.com/healthcare-information-technology/hospitals-are-hit-with-88-of-all-ransomware-attacks.html

23. Elizabeth Snell. OCR Aims to Improve Smaller Data Breach Investigation Process. Health IT Security [Internet]. 2016 Aug 22 [cited 2017 Feb 7]; Available from: http://healthitsecurity.com/news/ocr-aims-to-improve-smaller-data-breach-investigation-process

24. Substance Abuse and Mental Health Services Administration (SAMHSA), HHS. Confidentiality of Substance Use Disorder Patient Records [Internet]. 81 FR 6987 Feb 9, 2016 p. 6987–7024. Available from: https://www.federalregister.gov/documents/2016/02/09/2016-01841/confidentiality-of-substance-use-disorder-patient-records

25. Kaiser Family Foundation. Total Professionally Active Physicians [Internet]. 2017 [cited 2017 Feb 3]. Available from: http://kff.org/other/state-indicator/total-active-physicians/

GOVERNANCE STUDIES

The Brookings Institution
1775 Massachusetts Ave., NW
Washington, DC 20036
Tel: 202.797.6090
Fax: 202.797.6144
brookings.edu/governance.

EDITING
Liz Sablich
PRODUCTION & LAYOUT
Cathy Howell

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU

Support for this publication was generously provided by California Health Care Foundation based in Oakland, California.