Center for Technology Innovation at BROOKINGS

May 2016

Hackers, phishers, and disappearing thumb drives: Lessons learned from major health care data breaches

Niam Yaraghi is a fellow in the Brookings Institution's Center for Technology Innovation.

EXECUTIVE SUMMARY

BACKGROUND

Health care services are complex and require many different entities to have access to patients' medical data. Consider a simple office visit: in addition to the physician who sees the patient, it may involve an independent entity that facilitates the scheduling of the visit, an electronic medical records (EMR) vendor that provides software and cloud storage for saving the doctor's notes, an health information exchange (HIE) platform that shares this data with other physicians, another party that creates the bill, the insurance company that pays for it, and sometimes a collecting agency that manages the patient's late payments.

As the complexity of health care services increases, the number of involved entities and the subsequent risk of privacy breaches also increase. Twenty three percent of all data breaches happen in the health care industry[1]. Over the last six years, medical data of more than 155 million Americans have been potentially exposed through nearly 1,500 breach incidents[2]. The per-record cost of health care data breaches is $363, the highest of all industries.[3]

OBJECTIVE

The purpose of this report is to examine recent privacy breaches in the health care industry and uncover the underlying factors leading to these incidents, document the lessons learned, and examine how similar breaches can be prevented moving forward.

---

1 BakerHostetler. *Is Your Organization Compromise Ready?* BakerHostetler; 2016. http://f.datasrvr.com/fr1/516/11618/BakerHostetler_2016_Data_Security_Incident_Response_Report.pdf. Accessed May 3, 2016.

2 U.S. Department of Health & Human Services - Office for Civil Rights. https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf. Accessed May 3, 2016.

3 *IBM 2015 Cost of Data Breach Study - United States*; 2016. http://www-03.ibm.com/security/data-breach/. Accessed May 3, 2016.

METHODS

A set of 22 in-depth interviews were conducted with key personnel at a variety of health care providers, health insurance companies, and their business associates. The lessons learned are generalizable and apply to all different types of health care organizations.

KEY FINDINGS

This research demonstrates that the health care sector is uniquely vulnerable to privacy breaches for several reasons:

Health care data contain valuable information such as social security numbers and home addresses and thus are worth more to hackers than other types of data. Since they can sell these data for a premium price on the black market, hackers have a strong economic incentive to focus their hacking attacks on health care sector.

With the push toward more integrated care, medical data are now being shared with many different types of entities in which many employees have access to patient records. Extended access to medical records increases the potential for privacy breaches.

To comply with legal requirements, health care organizations often store detailed medical information for many years. The probability and consequences of a breach increase according to storage volume and duration.

Government incentives led health care organizations to adopt electronic health records without being ready to adequately invest in security technologies.

Privacy breaches used to have little to no effect on the revenue stream of health care organizations, and thus, they did not have strong economic incentives to invest in digital security and patient privacy. In addition to the high remediation costs, new types of cyber-attacks, specifically ransomware attacks, now threaten the core businesses of hospitals. Thus, they have much higher economic incentives to invest in information security.

Human error was mentioned as the leading cause of the majority of breaches analyzed. As such, this report identifies methods to reduce human error and technologies to prevent the likelihood and consequences of privacy breaches within an organization. The report also addresses factors outside of an organization that may hinder privacy protection efforts, and must be taken into account. These challenges include:

While the Health Insurance Portability and Accountability Act (HIPAA) is clear about the requirement to protect health data, it does not specify how to do so and is open to interpretation. HIPAA is also outdated and falls short of addressing modern cybersecurity challenges.

The manufacturers of medical devices do not ensure the security of their products and instead transfer their responsibility to health care organizations, which are already struggling with securing their own networks.

After a breach happens, the Office for Civil Rights (OCR) at the Department of Health and Human Services initiates an audit process. While one does not expect the organizations that were audited to have a positive view about OCR, most

of them mentioned that the process is very punitive and contributes to the organizations' reluctance to share the details of their breaches with their peers.

Furthermore, audits usually take more than two years and organizations incur significant legal fees during the process. OCR does not share the details of its findings after an audit, and thus, other organizations will not have the opportunity to learn from the experiences of their peers.

Sharing information about cyber threats between the health care industry and federal agencies, such as the FBI, is crucial in preventing breaches and mitigating their consequences. However, the punitive nature of OCR audits coupled with media scrutiny discourages organizations from sharing their experiences and concerns.

Patients are often unaware of the risks associated with providing data to medical providers. If patients were better informed, they would demand higher levels of protection from their medical providers.

CONCLUSIONS

To better protect patient privacy and prevent breaches, this report makes several policy recommendations to both health care organizations and the OCR.

RECOMMENDATIONS TO HEALTH CARE ORGANIZATIONS

Prioritize patient privacy and use available resources to protect it

In many of the interviewed organizations, privacy breaches could have been prevented had the organization spent enough on security technologies or diligently implemented and followed privacy policies. Health care organizations now have access to both the knowledge and technology that is required to ensure the privacy of their patients, and thus should use these resources to their fullest potential.

Better communicate with each other

Information sharing about security technologies, privacy policies, and breach incidents should take place among health care organizations and also between health care organizations and federal agencies. Health care organizations should be encouraged to use the full potential of currently available platforms to better share information amongst themselves.

Embrace cyber insurance

In the long run, a cyber insurance market can fundamentally improve how patient privacy is viewed and managed in the health care sector. To underwrite the privacy risk of health care organizations, cyber insurance companies will be willing and able to conduct timely and efficient audits and proactively manage their clients' privacy protection efforts. Health care organizations will also have a direct economic incentive to reduce their cyber insurance premiums by addressing their security weaknesses and preventing privacy breaches.

RECOMMENDATIONS TO THE OFFICE FOR CIVIL RIGHTS

Better communicate the details of breach incident audits

After a breach happens, OCR conducts a thorough investigation to identify its causes. Through these audits, OCR also ensures that the victim organization has put corrective and preventive policies in place to avoid future incidents. Although the lessons learned from each breach can prevent other similar incidents, OCR does not share the details of its investigations. OCR should provide detailed reports on how each breach happened, and how other health care organizations can avoid similar occurrences.

Establish a universal HIPAA certification system

OCR should prevent more than it punishes. Although the audits that happen after a breach effectively reduce the chances of second incidents, they cannot prevent privacy breaches in the first place. Random audits that take place before a breach occurs will be helpful in preventing one. These random audits are currently conducted very rarely. OCR should accredit certification agencies that can conduct preventive audits in accordance with OCR standards and certify the compliant organizations.

.

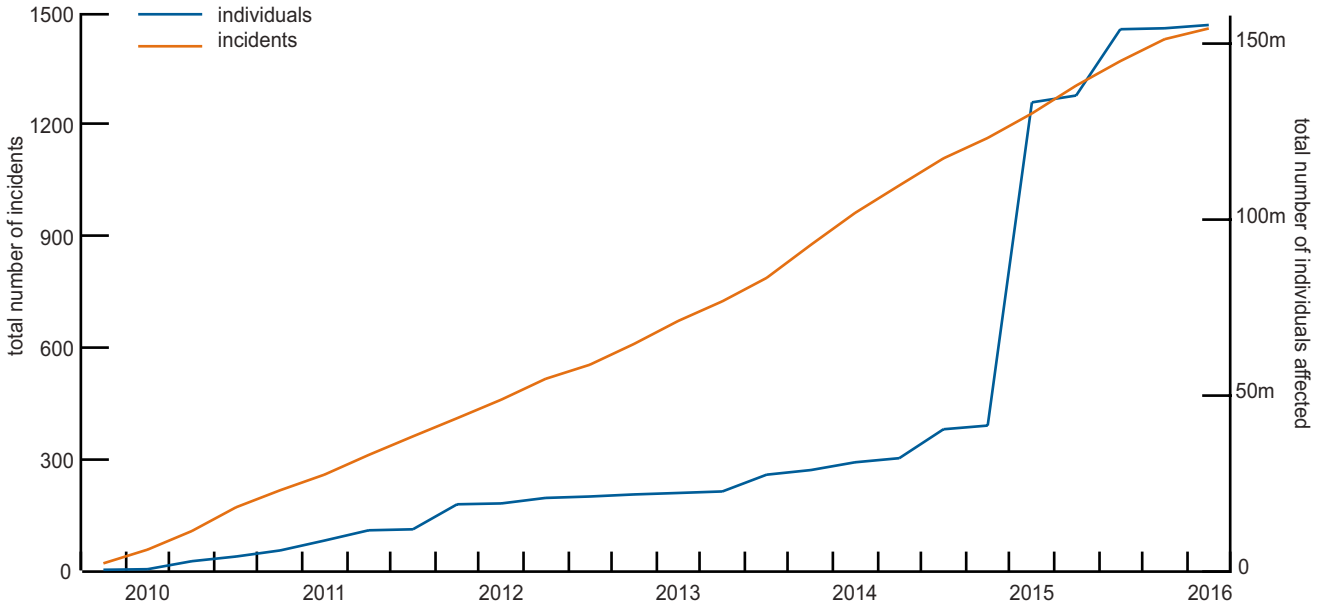
INTRODUCTION

As a result of our recent technological leaps towards digitization of health care, unprecedented amounts of personal health data are collected, shared, and analyzed on an everyday basis and thus, today we have more reasons to be concerned about patient privacy than ever.[4]

While the consequences of many types of data breaches are manageable with minimal or no cost to the consumer, medical data breaches can be catastrophic simply because they contain information that cannot be changed. Consider your credit card information: if it gets breached and someone puts unauthorized charges on it, your card issuer will instantly reverse the charges, freeze the old card, and send you a new one. On the other hand, most medical data now include identifiers such as social security numbers, dates of birth, and home addresses which are nearly impossible to change or reset upon a breach. Precisely because of their constant and unchangeable nature, medical data are worth more than financial data in the black market.[5] Hackers know that your credit card information can at most help them with a few eBay purchases before you notice and disable the card. On the other hand, with your medical data, they can steal your identity and are then able to steal thousands of dollars by submitting fraudulent health insurance claims on your behalf. When you notice that you have been a victim of an identity theft, the process of changing your social security number, home address, name, or date of birth will be a horrible nightmare.

Given the sensitivity of medical data, the Office for Civil Rights (OCR) at the Department of Health and Human Services is assigned with the delicate and important task of protecting patients' health information privacy rights through the Health Insurance Portability and Accountability Act (HIPAA), a part of which includes data breach protections. Despite the public's concerns and government's efforts, the frequency and magnitude of privacy breaches have been on an upward trend. According to statistics from the Identity Theft Resource Center, data braches are

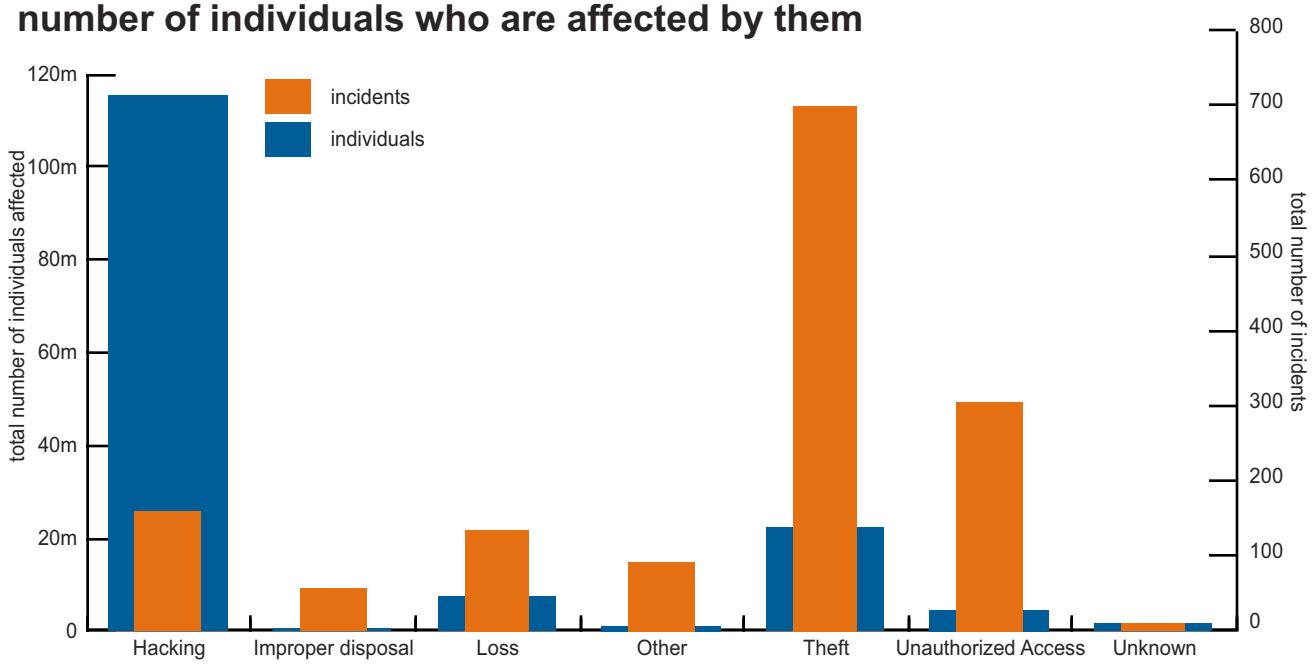
Figure 1: The cumulative number of breach incidents and affected individuals since the third quarter of 2009



4 Madden M. *Public Perceptions of Privacy and Security in the Post-Snowden Era*. Pew Research Center; 2014. http://www.pewinternet.org/2014/11/12/public-privacy-perceptions/. Accessed April 4, 2016.

5 Humer C, Finkle J. Your medical record is worth more to hackers than your credit card. *Reuters*. http://www.reuters.com/article/us-cybersecurity-hospitals-idUSKCN0HJ21I20140924. Published September 24, 2014. Accessed April 4, 2016.

Figure 2: The frequency of different types of breach incidents and the number of individuals who are affected by them



more likely to happen in the health care industry than any other sector.[6] Experian predicts that this sector will continue to experience an increasing volume of hacking attacks in 2016.[7] According to the data provided by OCR, since late 2009, the medical information of more than 155 million American citizens has been exposed without their permission through about 1,500 breach incidents, as shown in Figures 1 and 2.

Every breach is an expensive learning experience for the involved organizations. Yet, the lessons learned from these tragic experiences are rarely documented and are never shared with other entities in the industry. As long as the factors that lead to privacy breaches are not documented and shared, others are equally likely to experience the same incidents in the future.

Health care is an extremely segmented industry. Despite fierce competition, medical services are often provided through close collaboration of multiple entities. Consider a simple office visit: in addition to the physician who provides the main service, it may involve an independent entity that facilitates the scheduling of the visit, an EMR vendor that provides software and cloud storage for saving doctors' notes, an HIE entity that shares this data with other physicians, another party that creates the bill, the insurance company that pays for it, and sometimes a collecting agency that manages patients' late payments. As the complexity of medical services increases, the entities who are involved in providing them also increase. To have a comprehensive understanding of the breaches, one should consider these interconnected and close-knit relationships, and study health care entities as a part of a system rather than isolated units. More importantly, although covered entities[8] and business associates[9] focus on very different types of services, they operate within the same industry and follow the same standards and regulations when it comes to security and patient privacy. Therefore, the experiences of one organization in handling patient privacy

6 Identity Theft Resource Center. *Data Breach Reports*. Identity Theft Resource Center; 2015. http://www.idtheftcenter.org/images/breach/DataBreachReports_2015.pdf. Accessed April 4, 2016.

7 Experian. *Data Breach Industry Forecast*. Experian; 2015. https://www.experian.com/assets/data-breach/white-papers/2015-industry-forecast-experian.pdf. Accessed April 4, 2016.

8 Covered entity is a health plan, health care clearinghouse or health care provider that has access to protected health information.

9 Business associate is an entity that provides data transmission services with respect to protected health information to a covered entity.

and managing security technologies are very relevant to the other organizations regardless of their type. In other words, business associates and covered entities will have a great opportunity to learn from each other's breach experiences. To shed more light on the underlying reasons of such incidents, I conducted a series of interviews with key personnel at a wide variety of health care providers, insurance companies, and business associates that had a breach incident over the last two years. I synthesize and summarize these interviews as other health care organizations, regardless of their type, may find it useful to learn from the experiences of their peers.

The organization of the report is as follows. Data collection and interview procedures are described in section two. Section three describes the unique characteristics of the health care industry and explores its unique vulnerabilities to privacy breaches as compared with other industries. An exemplary set of breach incidents and the lessons learned from such breaches are presented in sections four and five, respectively. Sections six and seven respectively explore the shortcomings in current regulations and how they are enforced. Section eight concludes the report by providing a set of actionable recommendations to address the current limitations and better manage patient privacy in the health care sector.

DATA COLLECTION AND INTERVIEW PROCEDURES

A team of two research assistants and three interns compiled the contact information of all organizations that --according to OCR website--had a breach in 2014 or 2015.[10] The list included 389 records for medical providers, 106 records for health plans, and 83 records for business associates. Some of these records were referring to the same entity which had experienced multiple breaches. Some other records were referring to organizations that do not operate in the health care industry and were only listed because their employees' medical information was breached, examples of such organizations include 7-Eleven Inc. and Nintendo of America. To keep the focus of the research on the health care industry, such organizations were removed from the list.

The team first sent email inquiries to key personnel[11] at the organizations and invited them to participate in the interviews. At least three emails were sent to all the identified organizations and were followed up with two phone calls or voicemails in weekly intervals. For the reasons that I discuss later in the paper, the majority of the organizations were extremely reluctant to share their experiences, even off the record, and many of them did not respond to the inquiries despite the perseverance of our team. One-hundred and ninety hours between 12/1/2015 and 3/1/2016 were spent compiling the contact information, reaching out to organizations, scheduling the interviews, and conducting them. The details of these efforts are discussed below.

The team reached out to 123 health care providers and received 37 responses, of which 14 accepted to attend an interview, 15 declined, and eight stopped responding after initial conversations. On average, it took two emails or phone calls to persuade them to participate in the study. A total of 44 hours were spent on this group. The team also reached out to 66 health plans and received 19 responses of which 2 accepted to attend an interview, two others initially agreed to participate but then refused to do so, 12 declined and three stopped responding after initial conversations. On average, it took six emails and two phone calls to get them to agree to participate in the study. A total of 52 hours was spent on this group. Finally, the team contacted 94 business associates and received 24 responses of which six agreed to participate in the study, six declined and 12 stopped responding after initial conversations.

10 I am deeply grateful for the tireless support and outstanding research assistance provided by Hillary Schaub, John Karsten, Lucas Wright, Jieyan Zhong and Liana Stiegler. Without this team I would not have been able to finalize this report in its current form.

11 Depending on the type and size of the organization, the titles of these personnel included office managers, public relation managers, chief information officers, privacy officers, chief medical officers and CEOs.

For the six confirmed interviews, on average it took four phone calls and two emails to get them on board. A total of 72 hours was spent on this group.

All of the interviews were conducted over the phone. At the beginning of the interview the purpose of the research was stated and interviewees were asked if they preferred to remain anonymous. The interview consisted of a series of open-ended questions that asked about how the breach happened, how the organization responded to the breach, and what lessons were learned. They were also asked to describe their experience with OCR after they reported the breach. At a higher level, interviewees were then asked how their organization manages patient privacy and if there are any obstacles they face within or outside of their organization to better protect patient privacy. Each interview took about an hour; in total I spent 22 hours conducting the interviews.

WHY DO PRIVACY BREACHES OCCUR MORE FRQUENTLY IN THE HEALTH CARE SECTOR?

Although health care organizations have unique characteristics that make them more vulnerable to privacy breaches, it is worth noting that reporting regulations and media coverage of privacy breaches are not similar across different types of industries.

Given the sensitivity of medical data, the reporting regulations for breaches are much stricter in health care than in other industries. While HIPAA as a federal law has a clear definition of a breach and transparent reporting requirements, there are no similar laws at the federal level that govern the reporting of other types of data.

> As one of the interviewees pointed out, "We assume the worst case scenario and consider any lost patient data as breached. It may not be the case. Many times, a laptop or thumb drive is lost or stolen and we do not have any evidence to believe that data on it is breached and patient privacy has been violated. However, we have to report it anyways and consider it as a breach. In other industries, it may not be the case."

Given the differences in states' privacy laws, it is very difficult to compare the frequency of privacy breaches in health care with other industries. The reason we are aware of more privacy breaches in the health care industry may be partially due to stricter reporting requirements.

Given the differences in the states' privacy laws, it is very difficult to compare the frequency of privacy breaches in health care with other industries. The reason we are aware of more privacy breaches in the health care industry may be partially due to stricter reporting requirements.

Although a higher number of breaches may happen in health care compared to other industries, some of the interviewees believed that another reason we see more reports of medical data breaches is that people are more concerned about their medical data and therefore media attention to the subject is heightened. In other words, such incidents are considered to be more newsworthy and thus are widely covered in the news, while stories about breaches of other types of data are not as widely reported.

HEALTH CARE DATA ARE RICHER AND MORE VALUABLE FOR HACKERS

Health care data are particularly valuable for two reasons: first, if the data belong to celebrities or public figures, they will have high news value. Hackers try to get their hands on these data either out of pure curiosity or for releasing the data to the public. A CIO of one of the hospitals that celebrities frequently visit told me, "As soon as a celebrity checks in, we see a huge spike in our hacking attacks, because people want to see the records of that celebrity. We keep celebrity medical information under alias names. Our best defense against hacking attacks is to keep a low profile and not attract attention." Second, medical data contain a rich set of personal identifiers including full names, addresses, and social security numbers which can be used to create fake identities which could be misused for many different illegal purposes such as collecting insurance reimbursements or purchasing drugs and medical equipment that can be resold. Various sources report that in the black market, stolen medical data are sold at a much higher price as compared to other types of data such as stolen credit card numbers.Given the higher value of medical data, hackers have much stronger economic incentives to attack health care entities.

TOO MANY PEOPLE HAVE ACCESS TO MEDICAL DATA

Medical data are now being shared with many different types of entities. In many, most employees have full access to patients' medical data. This extended access increases the risk of breaches which are mostly due to human error. A business associate described the problem as the following: "Technology does not fail us, we fail ourselves. So, if we create a workflow that minimizes human involvement, we can minimize the risk of breaches." For example, at UCLA hospitals, employees breached celebrities' medical information despite being completely aware of the unlawfulness of their actions. As a CIO put it, "People go out of their ways to get their hands on Protected Health Information and make bad decisions despite all of the technologies."

Although there are methods to limit access to only the employees who are directly involved in the medical care of a patient, the urgency of medical care hinders the implementation of such methods. The CIO of a small mental health care provider told me that his organization is now working with a very big hospital to implement an EHR system and connect their networks. As he said, "The EHR vendor and this large hospital have very relaxed access policies. That is, all of the hospital staff can have access to all patients' data while they have a much stricter policy and have segregated access levels. But when they connect their networks, everyone in the hospital will be able to see their patients' data." It is very difficult to predict exactly which of the many physicians and nurses in a large hospital will need to read a patient's records in a critical time to save his life.

It is very difficult to predict exactly which of the many physicians and nurses in a large hospital will need to read a patient's records in a critical time to save his life.

Considering the fact that the core mission of a health care provider is to treat patients in the best possible way, when comparing the risk of privacy breaches as a result of extended access with the risks of suboptimal medical care as a result of limited access, medical providers lean towards the former choice. This is not the case for business associates and payers because they are not directly involved with the medical care of the patients, and thus do not have any concerns about granting timely access to full information to ensure the best medical care. Many of the business associates that I spoke with have already implemented policies to ensure that their employees only have access to the minimum amount of data which

are absolutely necessary for them to perform their job. One of the business associates described the problem of data access and how to manage it as follows:

> "We receive patient demographics and medical information from a hospital. Although we only need five fields to do our job, the hospital dumps a dataset containing 134 fields of information per observation because it does not want to put in the effort to filter its datasets to provide us with specific and limited data. We have implemented a filter which hospital data goes through and only the five required fields are passed into the databases, the rest of the data does not even enter the database."

"We receive patient demographics and medical information from a hospital. Although we only need five fields to do our job, the hospital dumps a dataset containing 134 fields of information because it does not want to put in the effort to filter its datasets to provide us with specific and limited data."

Another closely-related factor is the highly fragmented IT networks in the health care sector that increase the chances of a breach. Due to the nature of medical care and the structure of the market, many different organizations now have interconnected networks and share some type of information with one another. Not all of these networks are as secure as they should be. Weak spots will be a door for hackers to infiltrate into a much larger network and have access to very large volumes of data. The majority of the organizations stated that although they may be comfortable with the security of their own IT network, they cannot be sure about the others' and believed that they're only as good as their weakest link.

MEDICAL DATA ARE STORED IN LARGE VOLUMES AND FOR A LONG TIME

The probability and consequences of a data breach are directly associated with the storage duration and volume of medical data. Many of the interviewed organizations mentioned that they store detailed medical information for many years. This is partly due to current regulations and partly due to the organizations' newly found appetite for data mining. One of larger business associates stated that "It is required by law to keep medical data for seven years. This requirement is passed along to other business associates and whoever works with them, and thus it creates a bullwhip effect that keeps hoarding on data."

The regulations not only mandate providers to keep data for longer than they need but also to collect data that they do not need at all. As a provider told me "All Payers All Claims (APAC) mandates that providers collect race and so many other types of information about patients, although neither providers nor insurance companies need this type of data, it is mandated for other purposes such as quality improvements." One of the other business associates said "If we keep so little data for such a short time, then even if we get hacked, the volume of breached data will be so little and the consequences are manageable. I think we should know that getting hacked is inevitable, no matter how many security technologies we implement, there is still the risk of getting hacked, the point is to reduce the consequences of it and these two strategies are crucial and key for every health care provider."

THE HEALTH CARE INDUSTRY EMBRACED INFORMATION TECHNOLOGY TOO LATE AND TOO FAST

Health care lagged behind other industries in deploying information technologies. Unlike other sectors that implemented IT naturally and gradually over the course of many years, health care went digital overnight after the government allocated billions of dollars to promote adoption of electronic health care records.[12] According to statistics from the Office of National Coordinator for Health IT, while only 9.4 percent of hospitals used a basic EHR system in 2008, 96.9 percent of them were using certified EHR systems in 2014.[13]

This explosive growth rate is alarming and indicates the fact that health care entities could not have the organizational readiness for adopting information technologies over such a short period of time. Many of the small or medium health care organizations I interviewed did not view IT as an integral part of medical care but rather considered it as a mandate that was forced on them by larger hospitals or the federal government.

Precisely due to this reason, health care organizations do not prioritize IT and security technologies in their investments and thus do not allocate required resources to ensure the security of their IT systems, making them especially vulnerable to privacy breaches. One of the health care providers told me,

While only 9.4 percent of hospitals used an EHR system in 2008, 96.9 percent were using them in 2014 ... This explosive growth rate is alarming and indicates that health care entities could not have the organizational readiness for adopting information technologies over such a short period of time.

"After the Meaningful Use program, everything became digital but privacy and security expertise and technologies were not there to protect health data. Medical providers' main mission is to provide health care; they do not know how to protect data. IT is not their job, despite the fact that they hire CIOs and other IT personnel. While big technology companies are like war ships, these health care providers are like small rubber dinghies in a sea of hacker sharks. They cannot protect themselves".

Smaller organizations also lack financial resources to protect electronic data. The senior director of a nonprofit health care provider told me, "This is a not-for-profit organization, although we try our best to protect patient privacy, we do not have all the resources that more affluent organizations have. Encryption is not very cheap. Buying secure and encrypted servers would cost us thousands of dollars, which for our organization, is a lot of money". When I asked how they prioritize their IT spending, he responded, "We operate largely by grants. There are two types of grants: specific grants that have to be spent on a certain project, for example, providing care to poor patients. The general grants can be spent on anything, however, since the core mission of this organization is providing health care, we always end up spending general grants on health care projects rather than IT security. This leaves us with no money to spend on security and therefore we become very vulnerable and cannot adequately protect patient privacy. Now, if there were specific grants for IT and security infrastructure, it would be really helpful."

12 Blumenthal D, Tavenner M. The "Meaningful Use" Regulation for Electronic Health Records. *N Engl J Med*. 2010;363(6):501-504. doi:10.1056/NEJMp1006114.

13 https://www.healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf

Some organizations believed that other industries may have experienced the same rate of breach incidents when they started to implement IT. They believed that as health IT become more mature, the frequency of such incidents will decrease. The CIO of a medical provider who had more than a decade of experience in the banking industry told me "health care is many years behind the financial sector in security, because although HIPAA was designed in 1996, HHS did not enforce it until 2010. So, HIPAA was there but people did not care about it. After enforcing it through OCR, now the health care providers are taking it seriously and investing in their security technologies.".

THE HEALTH CARE INDUSTRY DID NOT HAVE STRONG ECONOMIC INCENTIVES TO PREVENT PRIVACY BREACHES

Protecting the customers' privacy is among the most important activities of businesses in every industry, except health care. Medical providers have less competition than other industries where consumers can choose between many different options and do business with an organization that values privacy protection. For most companies, spending on digital security is considered a strategic investment. It is a necessity without which many current businesses would immediately vanish. Imagine what would happen if the databases of a major online retailer, such as Amazon, were hacked. Customers would immediately react by avoiding Amazon and shopping from other online retailers. It is not hard to guess that after the recent data breaches at Home Depot, many customers preferred to swipe their credit card at other retailers such as Lowe's, rather than risking it at Home Depot. If such breaches happen too often and receive enough publicity, there is an increased probability that the targeted businesses will lose their customers and eventually go bankrupt. This creates a strong incentive for businesses to avoid data breaches through strengthening their defenses. To attract customers, businesses should first earn their trust.

Now consider patients' reactions to the Anthem hacking incident. They are outraged, but lack useful responses. They can't change their health insurer, and often must keep their health care provider. Most patients receive health insurance through work or the government. If they are covered under Medicare, Medicaid, or Military Health insurances, they do not have any choice other than remaining with the same insurer. Employers typically have long-term contracts with insurers to provide coverage for their employees and it is very difficult to terminate such contracts. Even if it was possible, despite their ethical obligations, the employers do not have a direct and immediate interest to do so. After all, the breaches are affecting their employees, not them.

> While big technology companies are like war ships, these health care providers are like small rubber dinghies in a sea of hacker sharks. They cannot protect themselves.

Patients are unlikely to change their doctor if they are impacted by a data breach. Most people choose their health care provider based on proximity to their residence. There is a limited supply of such providers in a given geographical area. In many instances, there is only one specialist, testing center, or hospital within miles of a patient's home. The scarcity of specialized medical services means most patients have no choice. Patients who overcome this barrier must still endure the emotional and medical costs of switching their provider with no guarantee that the new provider will better protect their privacy. The market for health care IT systems is dominated by only a few vendors and the chance that two providers employ IT systems with security features that are virtually the same is very high. It is also conceivable that both providers belong to a larger health care organization and use a single IT system, which suffers from the same security problems.

In a market where such major security breaches have little to no effect on the revenue stream of the organizations, there is no economic incentive to invest in digital security and prevent a data breach. As I will discuss later in the paper, new changes in cyberattacks and the market for cyber insurance are gradually creating incentives for medical providers to protect patient privacy.

DESCRIPTIONS OF PRIVACY BREACH INCIDENTS

Many of the interviewed organizations were not willing to discuss the details of their breach incidents for different reasons including the fact that they were still in the litigation process with OCR, or were concerned about their anonymity. In the following section, I briefly discuss how different types of breaches happened in a variety of organizations. The breaches are categorized into two groups: those that happened through a hacking or phishing attack and those that happened as a result of a loss or theft.

HACKING AND PHISHING INCIDENTS

At a large dental office, a breach happened because a user had visited an unsecure website which had installed malware on his computer and compromised his username and password.

At a small specialty clinic, the breach happened when they were shifting EMR systems. The third party contractor who was transferring their data from the old EMR system to the new one did not follow protocol and did not encrypt the files. The contractors also left some of the files on the old system without deleting them. The unencrypted files were later found on a Russian website.

In a major teaching hospital, staff received a notification from the FBI stating that they have been under potential attack. To ensure that they didn't get hacked, they spent about 10 million dollars and 40,000 hours of work on tightening their IT security. They were attacked by a foreign country.

In a community hospital, hackers sent phishing emails with very sophisticated content to the employees and told them that their Outlook storage space was running out and if they wanted to have more space, they should click on a link and provide their username and password. Many people clicked on the link, and thus hackers could gain access to their Outlook content, which contained some patient information.

A community-based mental health center received a call from Health & Human Services Commission that informed them about unusual activity on their network from China. They realized that one of their FTP servers was hacked and that there were two other intrusions into their systems in 2010 and 2012 from New Jersey and Eastern Europe, respectively. These intrusions were only for a couple of seconds, which means that the hackers knew how to get into their system and sold this information over the black market multiple times to different parties. They realized that their servers were used as a proxy for a pornography website; they do not have evidence that the hackers were after their data.

THEFT AND LOSS INCIDENTS

In a large academic hospital, one of the doctors kept a laptop and did not encrypt it despite organizational policies. He left the laptop in the backseat of his car, again despite organizational policies. When the laptop was stolen, to

avoid delays in his upcoming vacation, the doctor did not report the incident until he returned from his vacation after a couple of days.

A small business associate had requested a provider send them only the paper records of a sample of patients. The provider sent a thumb drive including electronic copies along with the paper records inside an envelope without letting the business associate know about it. The business associate had discarded the envelope without knowing that there was a thumb drive inside it because they were not expecting it. When the practice told them that there was also a thumb drive inside the envelope, they had already discarded their trash and could not retrieve it.

A provider sent to a business associate an envelope containing paper reocrds as well as a thumb drive including electronic copies. The business associate discarded the envelope without knowing that there was a thumb drive inside it, because they were not expecting one. When the practice told them that there was also a thumb drive inside the envelope, they had already discarded their trash.

In a midsize nonprofit mental health institute, a laptop was stolen. Although laptops and computers were all encrypted, their Outlook content was not. So, if someone copied the .pst folders to another laptop, they could access emails which included patient data.

In a medium-size nonprofit provider, although all laptops and desktops were encrypted, the servers were not due to technical and economic considerations. Their servers were stolen from a locked room while being bolted on a rack over the weekend.

In a large insurance organization, a breach happened when they were moving from one building to another. They had to move a file cabinet with index cards inside it and along the way, one of the drawers rolled out, and the files inside it fell out. Because their moving staff did not know what kind of documents they were, they just discarded the files

LESSONS LEARNED FROM PRIVACY BREACHES

In the following sections, I discuss less trivial lessons learned by victim organizations which could be implemented by all business associates and covered entities alike. First,I address privacy policies that focus on reducing the chances of breaches by reducing human error. The second part focuses on smart uses of security technologies to mitigate the risk of security breaches. A security breach, like other types of risk, has two components: probability of happening, and consequences. To minimize the security risks, organizations can implement technologies to mitigate each of these two components. Following this definition of security risks, the lessons learned from the breaches can be grouped into two categories: those that eliminate or reduce the probability of a breach incident and those that eliminate or reduce the consequences of a breach after it has actually happened.

POLICIES TO REDUCE HUMAN ERROR

The interviewed organizations unanimously believed that technology on its own is not enough to protect patient privacy. Most of the breach incidents happen as a result of human error rather than technology glitches, and thus, it is very important to pay special attention to how employees interact with data. The interviewees believed that all of the employees in the organization should know the privacy risks of their job and have a full understanding of

compliance and its benefits. To do this, IT and compliance personnel should establish trust and open lines of communication with other personnel. This can only happen with the full support of senior leadership, and thus, it is the responsibility of CIOs and privacy compliance officers to effectively communicate with the organization's senior leadership about the importance of security technologies and compliance with privacy policies. If the senior leadership understands and appreciates the necessity and benefits of security and privacy efforts, they can facilitate them by providing resources and creating an organizational culture that values privacy.

Some of the interviewees stated that they have routine annual audits conducted at their organization by third-party, independent entities. This is a common practice in the financial industry. Given the lack of regular audits through OCR or independent accreditation agencies, health care organizations should seriously consider independent audits as a strategy to continuously improve their security technologies and privacy policies.

Another training strategy is to send phishing emails to employees and observe how they behave when they receive suspicious emails. Those employees who click on suspicious links through these fake phishing emails can be informed through the IT department and may receive additional training and reminders.

Awareness about patient privacy among all employees in an organization should be ensured through proper training and frequent reminders. Although most health care organizations now have annual HIPAA training sessions, their employees should be constantly reminded about information security, privacy risks, and compliance benefits through effective manners. One successful strategy toward this end is a short, monthly email that provides quick HIPAA tips.

Organizations should make sure that the HIPAA training sessions are taken seriously by their employees, this is especially important in academic institutions and volunteer organizations. In these organizations, it is important to persuade the highly educated and skilled professionals to consider HIPAA training sessions and compliance with organization's privacy policies as critical elements of their responsibilities.

Another training strategy is to send phishing emails to employees and observe how they behave when they receive suspicious emails. Those employees who click on suspicious links through these fake phishing emails can be informed through the IT department and may receive additional training and reminders. These trials and experiments should be conducted on a regular and controlled basis in order to keep employees alert.

SECURITY TECHNOLOGIES TO PREVENT OR REDUCE THE CHANCES OF BREACHES

The fact that health care is a local business should be used as a security advantage. The overwhelming majority of access requests to servers of health care organizations from out of the country or even out of the state are malicious hacking attacks. Limiting access to local and trusted IP addresses is one way to protect against outside hacking attacks.

To further make sure that sensitive information is safe, health care organizations can limit access to their servers to only the work-issued devices that are equipped with required security technologies. For example, hospitals may only allow their physicians to access the EMR system on an encrypted work-issued laptop.

Health care organizations should also carefully consider the information needs of their personnel and provide them with different levels of access authorizations so that they can only access the minimum data that they require for their job. For example, after diagnosis, nurses may not need to have access to the mental health records of patients.

Limiting Internet access to a set of trusted websites is another way to ensure that employees do not visit unsecure websites that may install malware on their computers.

Security is not limited to information technology and should also include physical security. This is especially important as many of the breach incidents happen as a result of theft. Organizations should have that in mind and consider solutions such as installing cameras, card readers, and biometric locks to tighten the physical security and prevent breaches, as well as thefts that lead to breaches.

SECURITY TECHNOLOGIES TO PREVENT OR REDUCE THE CONSEQUENCES OF BREACHES

Encryption ensures that even if a breach happens, data cannot be read or used by unauthorized parties who do not have access the encryption key. In other words, it eliminates the consequences of a breach. Although encryption is not required under HIPAA, many organizations voluntarily encrypt the content of their emails to outside parties, but often neglect to also encrypt their internal messages. This is especially important if the organization has multiple locations and protected health information is exchanged among different internal networks.

Many of the breach incidents happen through unsecure email communication with parties outside of the organization. Encrypting emails that contain sensitive information is the cheapest and easiest way to cover a very important security hole and can easily be done with a Microsoft Outlook add-on.

Since many of the breaches happen as a result of loss or theft of thumb drives, it makes economic sense for the organizations to invest in purchasing high-security thumb drives that have encryption software embedded in them and have the ability to be wiped of data remotely in case they are lost or stolen.

Most of the interviewed organizations did not keep up-to-date backups, without which, upon an intrusion or loss of data, they could not identify patients whose data were compromised, and thus, had to assume the worst case scenario and consider the data of all of their patients as compromised. While backing up data does not reduce the chances of a breach, it can significantly reduce the organizations' responsibilities after the breach. If an organization knows precisely whose data have been breached, it can limit its post-breach response and reactions to that limited number of patients who have actually been a victim of the breach.

Encrypting emails that contain sensitive information is the cheapest and easiest way to cover a very important security hole and can easily be done with a Microsoft Outlook add-on.

This will not only reduce the costs of notifying patients and providing them with identity theft protections, but also prevents unnecessary anxieties among patients whose data have not been exposed, consequently reducing the extent of public scrutiny of the organization.

REGULATORY LIMITATIONS

The efforts to prevent privacy breaches shouldn't be limited to within an organization. Improving the factors outside of an organization can sometimes have a more salient effect on preventing breaches. Health care in the United States is a heavily regulated free market, and thus, improvements in such regulations can significantly help health care organizations to better manage and protect their patients' privacy. In the following sections, I lay out some of the most important regulatory limitations that hinder privacy protection efforts.

HIPAA IS NOT PRESCRIPTIVE

Most of the interviewed organizations complained about the lack of prescriptiveness in HIPAA. While HIPAA is clear about what to do, it does not specify how to do it. For example, one of the business associates told me that, "HIPAA requires us to protect health data but does not specify if we have to encrypt all of our data, or if locking down laptops is an appropriate measure for protecting health data." Another health care provider said,

> "HIPAA says that physical security should be in place, but does not mention if you need locks or cameras or both, or how many locks, or what types of locks. It only says that organizations should increase their employees' awareness about privacy, but it does not say if they need annual training or quarterly training or frequent tips. We never know if we are complying with HIPAA or not."

HIPAA was designed to protect patient privacy across entities of very different shapes and sizes. The lawmakers' trade-off between generalizability and specificity of HIPAA has resulted in a piece of regulation that is very open to interpretation. While some of the organizations considered the ambiguity of HIPAA a good thing because "it allows them to implement things based on their own characteristics and needs; otherwise, it could have been a very expensive mandate," many others were frustrated because without a clear set of requirements, it is impossible for them to evaluate the costs of implementation. As I will discuss later in the report, the penalties of noncompliance are also very vague and, consequently, health care organizations are unable to compare the costs and benefits of complying with HIPAA.

The Chief Information Officer of a large academic hospital summarized this problem as follows:

> "The federal government should be more prescriptive with regard to security and privacy requirements. There should be a very clear and crisp set of requirements by the federal government that as long as providers meet them, they are immune to fines from OCR. This will enable us to have an exact assessment of the investment that we need to make on our security technologies. There should also be a very clear set of rules that govern the fines of the privacy breaches. Currently, OCR acts more like a court, in which the judgments for the same crime vary based on the judge's interpretation of law and how well the lawyer represents the client. The lack of clear costs and benefits of security technologies make it very hard for us to make a rational and informed choice on this topic, it also makes it very difficult for the CIOs to justify their expenses for the senior leadership."

The CIO of a community hospital told me that over the past five years, they have increased their security budget from one to two percent to 26 percent of their overall IT budget. Yet they are still not sure if they have done enough because "the government is not prescriptive." The CIO of another academic hospital told me, "Even different EMRs implement the HIPAA differently. Although they are essentially all the same, the configurations are different based on the organization's resources and their understanding of the law. For example, the same Epic software may have different controls, tracks, and audits configurations in two different hospitals".

HIPAA DOES NOT ADDRESS MODERN CYBERSECURITY CHALLENGES

The opinions of health care organizations about HIPAA varied based on their size. Smaller organizations found HIPAA regulations helpful, despite being burdensome and difficult to implement. The manager of a small specialty clinic told me, "Complicated and sometimes burdensome privacy rules led to patient dissatisfaction. There are four or five pages of privacy rules which patients have to sign without completely understanding them. Patients are sometimes asked multiple times to sign different consent forms at different practices or even inside the same practice". Another business associate believed that "HIPAA is a set of best practices; although it creates a lot of responsibilities and burdens, it is a good thing and helps protect patient privacy."

As the CIO of a very large academic hospital put it: "HIPAA reflects how nerds thought about security 20 years ago. I do not refer to it to help me do my job better except in some minor issues such as personnel trainings."

Larger academic hospitals complained that HIPAA falls short of addressing modern cybersecurity challenges. As the CIO of a very large academic hospital put it, "HIPAA reflects how nerds thought about security 20 years ago. I do not refer to it to help me do my job better except in some minor issues such as personnel trainings." He told me that "HIPAA is in complete disconnect with the realities of today's digital technology and we cannot expect a national standard to be agile enough and be in pace with cyber technology. For example, HIPAA has nothing about malware and ransomware, intrusion detection, specific cyber incident responses, or multifactor authentications." The CIO of another academic hospital told me,

> "While hacking attacks get more complicated and sophisticated over time, HIPAA remains the same and does not adapt with the pace of developments in cybersecurity. Back in the day, phishing emails used to be from a Nigerian Prince who was asking for your bank account to transfer you millions of dollars. It was obvious that it was a phishing email. Nowadays the phishing emails are very sophisticated, they look like real emails sent by your colleague down the hall."

In summary, HIPAA's one-size-fits-all design provides a basic set of recommendations that are very helpful and act as road map for small organizations with little or no experience in managing patient privacy and security technologies. However, it falls short of expectations when it comes to more advanced challenges of modern cybersecurity that larger organizations with more sophisticated IT capabilities are facing. HIPAA is like the basic driving lessons that teach one how to drive under normal conditions in the city. However, these basic lessons are not enough to become a professional race car driver.

MEDICAL DEVICE MANUFACTURES AND INFORMATION TECHNOLOGY VENDORS ARE NOT HELD ACCOUNTABLE

Large academic hospitals were also concerned with the security of medical devices. The manufacturers of these devices do not ensure the security of their products and sign contracts with medical providers in such a way that removes all of their responsibility in regards to the security of such devices. Thus, medical providers themselves should bear the responsibility of securing these devices. Many smaller medical providers do not have the capability to do this and thus remain very vulnerable to potential cyberattacks. The CIO of a large academic hospital believed that "This is a really serious issue and can have catastrophic consequences because if some terrorist organization really wants to hack into these devices and, for example, change the settings of the IV pumps overnight, they can do so and no one knows how many patients will die because of that." The overall consensus among the medical providers was that the FDA should include the IT security of medical devices as a criterion of their certification procedure.

"If some terrorist organization really wants to hack into medical devices and, for example, change the settings of the IV pumps overnight, they can do so and no one knows how many patients will die because of that."

Some of the small and mid-size medical providers also suggested that vendors of all kinds of medical software should ensure the security of their products. One of the CIOs said, "There are about 600 different types of software in the same hospital network and only EHRs are certified." For many smaller medical providers with limited IT capabilities, it is very difficult to make sure that all medical software is secure and HIPAA compliant, and thus, a certification program would be very helpful. The same model was successfully implemented by ONC which required EHR software to be compliant with a set of security standards. Some other CIOs warned that "complying with the security standards such as NIST would be extremely difficult for many software developers."

GOVERNMENT OVERSIGHT LIMITATIONS

Except for one of the business associates who stated that their "experience with OCR has been very pleasant" and they have found OCR "to be very reasonable, objective and supportive," the majority of the interviewed organizations believed that there are still opportunities for improvement at the OCR.

THE AUDIT PROCESS IS VERY PUNITIVE

While one does not expect the organizations that were audited by OCR to have a positive view about the office, they also mentioned some valid and important points.

The Vice President of a nonprofit health care provider told me:

> "One of the reasons that organizations are not willing to share information about their breaches is how OCR treats them. After a breach, there is a spectrum on which an organization can be: at the far left, as a victim whose data is being breached, on the far right, you have an organization that has not been responsible and has not protected health data properly and thus is considered as perpetrator. OCR considers you as the perpetrator; the process is designed like that: It has a very punitive nature of investigation with very prolonged waiting times, a lot

of requirements, just like a deposition. And also there is public scrutiny. The current way in which OCR handles the breaches is very similar to how the health care industry was treating medical errors decades ago, rather than having a systematic approach to identifying the root causes of breaches and trying to address them, OCR focuses on individual instances and only blames and penalizes victim organizations. The system is not open and even the reporting is not transparent. Health care has matured and does not follow its old approach anymore, but OCR is still doing the same thing. The system should be nonpunitive, open, and transparent, and focused on error identification rather than blaming individuals."

Another health care provider mentioned the same concerns: "We feel like a victim that is being punished. The OCR process is very disheartening. Even their website is called the wall of shame!"

"We feel like a victim that is being punished. The OCR process is very disheartening. Even their website is called the wall of shame!"

THE AUDIT PROCESS IS VERY SLOW

The most frequent concern about OCR that organizations mentioned was its lengthy and burdensome audit process. After a breach happens, health care organizations have to notify OCR, which will then initiate an investigation to understand the details of the breach, its underlying reasons, and the organization's preventive and corrective actions before and after the breach.

These investigations are often conducted through lengthy reports (which in some cases were 900 pages), in which victim organizations answer numerous questions asked by OCR attorneys. Many interviewees stated that it often takes more than six months for OCR to review their reports and issue a response or ask for further documentation. Overall, it will usually take more than two years until OCR reaches a conclusion and closes the breach case.

Most of the interviewed organizations believed that the lengthy response time of OCR is due to its diligence. They applauded the OCR's careful examinations of the breach incidents and believed that such investigations help them to detect and address their weaknesses in security and privacy. These organizations also believed that OCR's audit process is very lengthy and exhausting. Responding to multiple requests by OCR can be overwhelming, especially for smaller organizations. If OCR expedites its audit process and reaches a conclusion over a shorter period of time, the benefits and corrective outcomes of the audit process will be realized faster, especially in cases that lead to a penalty or settlement.

The CEO of a large specialty clinic described their experience with OCR as follows:

> "OCR has an attorney that is not a technical person and asks for some information and then is not available for a response for the next couple of months and then comes up again after months with some more questions. It would be much better if, rather than a single attorney, a team of experts of privacy and security technologies were leading the organization through a collaborative process to fix the problem. Now there is a culture of guilty unless proven otherwise at the OCR."

The CIO of a large academic hospital had the same point of view: "OCR questions are coming from an attorney with limited knowledge about security technologies. This leads to extreme expectations for technology to solve

everything. They intend to solve every problem with a technological solution (they forget about the people problem) and this leads to very expensive demands that undermine user-friendliness of technologies."

THE AUDIT PROCESS AND ITS RESULTS ARE NOT TRANSPARENT

When a health care information breach happens, health care organizations must report it to OCR, and if it has exposed 500 or more patient records, the civil rights office is required to post it publicly on its website: in industry terms, the "wall of shame."

In its current format, the OCR's wall of shame neither creates awareness nor motivates privacy protection efforts in the health care industry.

Some interviewed organizations believed that the OCR penalties depend on how well a case is presented and defended rather than the actual realities in the organization. The CIO of a community hospital told me,

"The OCR fines are very variable. Sometimes small organizations get the same fine for very minor offences as the large organizations for very severe offences. For example, a small provider who has lost a thumb drive may get the same penalty as a large hospital who has not installed a basic firewall. I think that there are various OCR branches across the country that operate semi-independently from each other and you may get a different vote on your case depending on the office that handles it. OCR penalties are also affected by how an organization presents and defends itself in its reports to OCR. It is just like going to the court and defending a case."

The CEO of a large specialty clinic told me,

"After the breach, we were not aware of the available consultants and we chose an incompetent one who included unnecessary and wrong information in our report to OCR. For example, the consultant unnecessarily mentioned that printers are not password protected while OCR was not asking for that, or he incorrectly mentioned that an additional laptop was lost while it was only unaccounted for in the IT inventory and was soon located. These misrepresentations led OCR to be much harsher on us and be more demanding. If we had a better consultant, we could have avoided many OCR demands."

Transparency is inherently good, as it intends to create awareness among patients. Similar public reporting initiatives in the health care industry have proven effective at improving performance by creating competition among organizations. However, in its current format, the OCR's wall of shame neither creates awareness nor motivates privacy protection efforts in the health care industry.

Privacy breaches happen for various reasons and under many different circumstances. On one end, an organization may be ignorant of its security technology and lack accountability when it comes to patient privacy; on the other end, a password-protected laptop may be stolen or an unencrypted thumb drive may be lost, even if the organization had the necessary precautions in place. OCR posts all of these incidents on its website without stating how exactly the breach happened and whether or not the organization is found responsible for the breach. In other words, the office publishes a list of the indicted without its own rulings, leaving us wondering if an organization is a victim of

the breach or is indeed responsible for it. Moreover, the details of the audits are not published by OCR, and thus, other organizations will not be able to learn from the experiences of their peers.

The privacy officer of one the large insurance companies stated,

> "One important aspect that the OCR breach report website should include is the type of the breached information. For example, someone's status of Medicaid enrollment and his social security numbers are both considered private information, and their exposure constitutes a breach. However, the sensitivity of these data are different from each other; the latter can have much more significant consequences. The other point about the OCR reporting is that many times it is not an actual breach; rather it is a mishandling of data. For example, in one incident, a manifest was left at a restaurant and when they realized, they went back and retrieved it. There was no evidence that someone had accessed this data, yet it is still reported on OCR's website."

THE AUDITS CANNOT PREVENT FIRST BREACHES

The interviewed organizations unanimously agreed that OCR takes every single breach incident very seriously and makes sure that the root causes of the first breach are adequately addressed so that there will be no second offenses. The audits that happen after a breach guide organizations to implement suitable corrective actions. However, random audits before a breach occurs could potentially prevent one.

The director of compliance and contracting of a midsize health care provider told me:

> "Although there is a set of rules that are designed to prevent breaches, there is no enforcement process to make sure that people are following them. Because of this, many covered entities and business associates do not take them very seriously. For example, there have been many times that I received patient health data by mistake or incorrectly and when I informed the sending organization, they said, 'Oh just make sure you put it in trash!' or 'Oh, don't worry about it!' In summary, I think the rules are good, but they do not have teeth."

Although OCR does some random audits before a breach happens, they are very limited. There are hundreds of thousands of health care providers and business associates, but OCR only has the capacity to audit a few hundred organizations.

THE HEALTH CARE SECTOR LACKS INCENTIVES FOR INFORMATION SHARING

The punitive nature of the OCR audits coupled with public and media scrutiny discourages organizations from sharing their experiences about the breaches. Even those organizations that have not experienced breaches are not willing to openly discuss their policies and technologies due to security concerns. While cybersecurity firms such as Verizon and CISCO publish regular reports on the status of IT security, they are very technology-oriented and do not focus on the health care industry. In the absence of such specialized and industry oriented outlets, health care organizations find it increasingly difficult to learn about their peers.

The CIO of a community hospital told me:

"I recently sent an email to a group of CIOs in the health care sector to ask them how they manage their security and patient privacy, I only received one response from them despite the fact that this is a group of people who are very responsive and also know and trust each other. They are very reluctant to discuss what they do. We need to be able to share information about the breaches, our privacy policies and security technologies with each other and with government without concerns of being labeled or penalized."

Sharing information about cyberthreats between the health care industry and federal agencies, such as the FBI, is crucial in preventing breaches and mitigating their consequences. The large health care providers were especially concerned about this issue. The CIO of an academic hospital stated that. "We need to share information about potential attacks with the federal government without being concerned with potential negative consequences. There should be incentives for them to share such information with other organizations. Currently, there are not any."

AWARENESS OF PATIENTS AND ACCOUNTABILITY OF MEDICAL PROVIDERS AND BUSINESS ASSOCIATES SHOULD BE INCREASED

A comprehensive approach to protecting patient privacy should take patient awareness into consideration. The compliance officer of a large dental office told me that "HIPAA regulations create this sense of false security among patients. They think that although data is being collected, it is OK, because they cannot be shared with unauthorized people. However, the point is that if someone wants to get access to data, he will not care if it is legal or not, especially when data is so valuable."

"HIPAA regulations create this sense of false security among patients. They think that although data is being collected, it is OK, because they cannot be shared with unauthorized people. However, the point is that if someone wants to get access to data, he will not care if it is legal or not, especially when data is so valuable."

Patients should have a clear understanding about HIPAA and, more importantly, the risks associated with providing data to medical providers. If patients know the risks and the protections that are available to them, they will become more cautious in sharing medical information and will consequently demand higher levels of protection from their medical providers. Currently, it seems that such awareness and concern does not exist among patients. The CIO of a community hospital told me that they had a breach that affected more than 10,000 patients. After notifying the patients, they "received only 26 calls from the patients who had further questions or concerns about this breach." Many other organizations had similar experiences and believed that patients do not seem to pay enough attention to such notices, maybe because they are not fully aware of the risks associated with such breaches.

The Vice President of Operations at another business associate believed that:

"One of the ways that we can increase the pressure on business associates is to increase the pressure on medical providers and other covered entities to consider their business associates' security capabilities more seriously. Right now, the business associate agreement is just a way of transferring the OCR penalties, not the risk of losing patients' business. Because at the end of the day, consumers do not care or maybe do not have any other alternatives, so the medical providers do not care about the breaches that much. But if the patients were more

concerned about their privacy breaches, then medical providers would also be more careful, and thus, increasing patient awareness is one way to do it."

Many of the other business associates mentioned that after revised HIPAA rules, which hold business associates accountable for breaches, went into effect, they took privacy protection efforts much more seriously than before. One of the large business associates that primarily contracts with the federal government believed that:

"Government can play an important role in creating a sense of responsibility and accountability among its health IT vendors. Currently, this is not the case. For example, the government is not doing the Federal Information Security Management Act (FISMA) audits and instead askes the business associates to do the audits themselves. This creates a situation in which many business associates do not consider privacy serious enough because they can sense that it is not of priority to the federal government. Although there are security standards designed, they are not enforced and do not have ramifications for business associates. The federal government also has to increase awareness and educate people about privacy and security. There used to be a monthly newsletter about this subject by the federal government which has been discontinued for many years now, again it signals the lack of accountability from the government side."

Many business associates mentioned that after revised HIPAA rules, which hold business associates accountable for breaches, went into effect, they took privacy protection efforts much more seriously than before.

RECOMMENDATIONS TO BETTER PROTECT PATIENT PRIVACY

As discussed earlier, privacy breaches can be a result of factors both within and outside of an organization. The internal factors are better addressed by organizations themselves. External factors on the other hand, have much less variability and can be addressed within a single policy framework. With a focus on external factors, I lay out a set of actionable recommendations that government and health care markets can implement to reduce privacy breach incidents. While I believe that in the long run, market based solutions can better enhance privacy protection efforts, in the short run, government actions can lead to significant improvements. These recommendations are not limited to a specific type of health care entity and cover business associates, health care providers, and payers in a similar way.

HEALTH CARE ORGANIZATIONS SHOULD PRIORITIZE PATIENT PRIVACY AND USE AVAILABLE RESOURCES TO PROTECT IT

In many of the interviewed organizations, privacy breaches could have been prevented had the organization spent enough on security technologies or diligently implemented and followed privacy policies. Health care organizations now have access to both the knowledge and technology that is required to ensure the privacy of their patients, and thus should implement these resources.

OCR SHOULD BETTER COMMUNICATE THE DETAILS OF ITS AUDITS

While OCR invests a lot on creating training and educational materials to help different types of health care organizations and their employees understand the importance of patient privacy, it neglects the education opportunity that every single breach provides. OCR does not publish any details about the hundreds of breach incidents that it audits each year, and thus, other organizations will lose the chance of learning from the experiences of their peers. Consider the popular Anthem breach. After more than a year since the incident, OCR is still investigating and no one except Anthem and OCR (and of course the hackers) knows how it happened. Even after OCR finishes the investigation, it only announces its final decision about a penalty or settlement. This leaves the health care community wondering if there are other payers with similar security vulnerabilities in their networks. By keeping this information private and depriving others from the opportunity of proactively addressing their similar security weaknesses, OCR is unintentionally helping hackers to attack other payers with the same method and through the same unknown weak links that they used to attacked Anthem.

Consider the prominent Anthem breach. After more than a year since the incident, OCR is still investigating and no one except Anthem and OCR (and of course the hackers) knows how it happened. This leaves the health care community wondering if there are other payers with similar security vulnerabilities in their networks.

In its current format, OCR's website does very little to share information and is rather more suited to shame victims of privacy breaches. As mentioned earlier, such practices indirectly create a negative culture of pointing fingers rather than systematically addressing root causes. As the very first step, OCR should overhaul its website and provide very detailed information about each incident, including the root causes, the preventative and subsequent corrective actions, and more importantly, OCR's ruling after the audit and the exact amount of penalties and settlements, if any.

HEALTH CARE ORGANIZATIONS SHOULD BETTER COMMUNICATE WITH EACH OTHER

Information sharing should not be limited to that between OCR and health care entities. It should also happen between different health care organizations. The CIO of an academic hospital believed that collaboration and information sharing between larger and smaller health care institutions can be an effective strategy in preventing privacy breaches: "Larger academic hospitals and other organizations such as CHIME and AHA should collaborate with smaller hospitals and share their best practices with them. This will also help smaller hospitals with justifying the expenses of implementing similar technologies and policies. Also, maybe larger hospitals could provide technical and financial help to the smaller ones who are a part of their medical group to help with security and privacy."

While most of the interviewees complained about the lack of such information sharing practices, the CIO of a community hospital had a better experience:

> "We do not have to compete with each other in technology. We can share a lot of information about our security practices with the other medical providers at the technical level and mutually benefit from information sharing. We

are currently doing that. Information that we are sharing includes general information about security practices. For example, rather than trying to come up with the answer to a difficult question, we post this question on the forum and many experts at other health care organizations provide very good feedback. It saves our time and money. Also, when an intrusion happens, we share relevant information, suspicious IP addresses, to prevent similar breaches from the same hacker groups to other hospitals."

A national forum and online platform that can be very helpful for information sharing is the National Critical Infrastructure Information Sharing & Analysis Centers (ISACS)[14]. ISACS validates the identity of its members to make sure that they are IT professionals in the health care industry. It has also categorized the members so that a specific question can be posted to a certain group of users. It is informal, so people can share information without concern about legal liabilities. More importantly, since it is a national forum, health care providers will not face the usual barrier of local competition, and thus share information more willingly. Organizations such as ISACS are not very well-known in the industry (just two of the interviewees mentioned it), but can be of great help to prevent the breaches.

OCR SHOULD ESTABLISH A UNIVERSAL HIPAA CERTIFICATION SYSTEM

OCR should prevent much more than it punishes. The OCR's random audits are effective in preventing initial breaches. Given the limited capacity of OCR in conducting preventive audits, I believe that independent certification entities, which can have accreditation from OCR, will be a scalable solution. These certification entities can conduct thorough audits at different types of organizations, point out their weaknesses in security and privacy policies, and ultimately certify them as HIPAA compliant. Many of the interviewed organizations preferred to be randomly audited through a universal certification program. Some organizations indicated that they are even willing to pay for such audits. A CIO with experience in the financial sector pointed to similar audits in the financial sector: "In the banking industry, they do annual IT audits which include risk assessments, penetration tests, recovery plans, etc. These audits are conducted by the federal government through the National Credit Union Administration. There is no such thing in the health care industry. Since 2008, when the online banking became ubiquitous, they now have an additional cybersecurity audit on top the IT audits".

These voluntarily audits will not only help with preventing privacy breaches, but also lead organizations toward a common interpretation of HIPAA and bridge its lack of prescriptiveness. Through these audits OCR will enforce its own interpretation of HIPAA on all health care organizations in a consistent manner. A CIO of a nonprofit health care provider gave an example of a similar audit program: "Joint Commission of Behavioral Health audits our clinical and physical environment every three years to see if we comply with their standard and gives us accreditation. Since there is one entity that performs this audit, after a while, the interpretation of this entity will become the norm and every one will follow their interpretation."

Finally, the third and most important benefit of a certification system is that it will enable health care organizations to make informed and better decisions about their business associates. Currently it is very difficult for a typical health care provider that works with hundreds of business associates to carefully examine each of them and ensure that they have all the security safeguards in place. Health care providers are now using Business Associate Agreements (BAA) as a strategy to protect themselves from OCR penalties by transferring the responsibility of safeguarding

14 http://www.nhisac.org/

patient data to their business associates. However, such agreements are just transferring risk rather than mitigating it. If business associates could be HIPAA certified, then health care providers could actually mitigate the breach risks by contracting with the compliant associates. The vice president of operations of a business associate told me, "We are very confident about our own security. However, we are also working with many other vendors that may not be so secure. Our biggest challenge is how to make sure that other organizations to which we are transferring our data and outsourcing our tasks are also secure."

HEALTH CARE SECTOR SHOULD EMBRACE CYBER INSURANCE

While the above mentioned three recommendations could be easily implemented in the short run, I believe a cyber insurance private market will be able to provide fundamental solutions and long lasting improvements in how privacy is being managed in the health care sector. Cyber insurance in the health care sector is still in its infancy and many health care organizations still do not carry it. As information technology becomes more salient and important in medical care, different types of health care organizations will soon realize the importance of protecting themselves against IT incidents.

Over the next five years, cyber insurance will be as important as malpractice insurance is today; no health care provider can afford the risk of operating without it. As demand for cyber insurance increases, to better manage their risks, the insurance companies will develop robust and updated grading systems through which they can precisely estimate the risks of privacy breaches at different types of health care entities and accordingly provide them with an insurance policy. Improving cyber security grading and reducing cyber insurance premiums will become a priority for health care organizations. As chief medical officers are now evaluated based on malpractice incidents and malpractice insurance premiums, the performance of chief information officers at hospitals and business associates will be evaluated based on how they manage to improve organization's cyber insurance grading and premiums. Information security and patient privacy will become an actual business priority for health care organizations and to improve, they will allocate adequate financial and technical resources. Medical providers, business associates, and health plans will independently address the internal causes of privacy breaches.

Over the next five years, cyber insurance will be as important as malpractice insurance is today; no health care provider can afford the risk of operating without it.

In such a market, all of the current external shortcomings will also be addressed. Cyber-insurance companies will be able to update their grading criteria and auditing systems with the pace of technology improvements. Since they have a direct business incentive to better evaluate their clients' cyber risks, they will design very detailed and prescriptive policies and go far beyond HIPAA to the extent that the outdated law will become obsolete. As current payers in the health care market are currently moving towards managing the health of patients as a strategy to reduce their own costs, the cyber insurance companies will have an incentive to help their clients prevent privacy breaches. For example, when a breach happens, the cyber insurance companies will have a direct business incentive to immediately inform their other clients as an effort to prevent similar breaches. The same economic incentives will lead the audits of cyber insurance companies to be much faster, less punitive, and more focused on finding the root causes of the breach.

GOVERNANCE STUDIES

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

EDITING
Beth Stone

PRODUCTION & LAYOUT
Nick McClellan

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU

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