HIPAA security compliance challenges: The case for small healthcare providers

Jim Q. Chen, Allen Benusa

St. Cloud State University, MN, USA

Correspondence to:

Jim Q. Chen, St. Cloud State University, St. Cloud, MN, USA.
jchen@stcloudstate.edu

Abstract

More than 60% of physicians in the U.S. practice as small healthcare providers. The realm of small healthcare providers includes dental offices, orthodontists, chiropractors, massage therapists, optometrists, long-term care facilities and other small, independent clinics that typically have 1 –30 employees. While studies have reported variable levels of Health Insurance Portability and Accountability Act (HIPAA) information security (InfoSec) compliance among hospitals and large medical facilities (Anthony DL, Appari A, Johnson ME. Institutionalizing HIPAA compliance: Organizations and competing logics in U.S. health care. J Health Soc Behav 2014;55(1):108–24; Brady, JW. Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. Proceedings of the 2011 44th Hawaii International Conference on System Sciences, Manoa, Hawaii; 2011.), small healthcare providers face even more challenges in their effort to be HIPAA compliant. This paper will use a case study to examine factors that affect the small healthcare providers' effort in meeting HIPAA InfoSec compliance. The paper also discusses services and technologies available to them to become compliant and how they can maintain continued compliance once they become compliant. Both a process model and an action compass are proposed to guide small healthcare providers. This case study provides support to existing compliance theories. The proposed guidance is useful for not only small healthcare providers but also mid-sized and large businesses in general.

Keywords: HIPAA, Regulatory compliance, Information security management, Healthcare

Introduction

Like many other industries, healthcare is heavily regulated by government legislation and industry standards. The Health Insurance Portability and Accountability Act (HIPAA) is the most significant legislation transforming the healthcare industry. HIPAA was enacted as a broad Congressional attempt at healthcare reform. It was signed into law by President Clinton in 1996 to achieve two main objectives: to ensure that individuals would be able to maintain their insurance between jobs; to ensure the confidentiality and security of patient information.

Since its implementation, additional legislation has been enacted requiring modifications to the HIPAA Rules. For example, the Health Information Technology for Economic and Clinical Health (HITECH) was enacted in 2009 as part of the American Recovery and Reinvestment Act (ARRA). HITECH modifies certain provisions of the HIPAA Rules to strengthen patient privacy, security, and enforcement.[1] HITECH also provides economic incentives for healthcare organizations to adopt electronic medical systems in order to reduce healthcare cost.

Regulatory compliance in patient information security (InfoSec) and privacy has become one of the major challenges in the healthcare industry. In particular, small healthcare organizations are facing major challenges in their compliance efforts. According to a 2008 government report, small healthcare practices provided nearly three-quarters of all ambulatory care visits in the U.S.[2] Nearly two-thirds of U.S. office-based physicians work in practices of fewer than seven physicians.[3] More than 60% of physicians practice in what is considered a small business.[4] However, an alarming number of small medical practices had no security policy and procedures.[5] According to Healthcare Information and

Management Systems Society, 33% of small healthcare providers had never conducted a security risk assessment.[6]

The penalty for non-compliance can be severe. In its December 14, 2015 news release, the U.S. Department of Health and Human Services (HHS) Office for Civil Rights (OCR) announced that The University of Washington Medicine had agreed to settle its potential violations of HIPAA Security Rules for $750K.[7] In 2014, an Alaskan mental health services provider was fined $150K for its failure to apply software patches.[8] In the same year, New York-Presbyterian Hospital and Columbia University Medical Center together were assessed $4.8 million penalty for their HIPAA violations after the electronic protected health information (PHI) of 6 800 patients wound up on Google searches.[9] Blue Cross Blue Shield of Tennessee settled potential violations of HIPAA Rules for $1.5M in 2012 and the UCLA Health System settled potential violations of the HIPAA Privacy and Security Rules for $865 500 in 2011.[10]

This research paper investigates factors that affect small healthcare providers in their effort to be HIPAA compliant or non-compliant. The discussions are based on both literature on compliance theories and the authors' first-hand consulting experience with small businesses, especially experience and lessons gained from working for an Ophthalmology and Optometry practice, named RegEye, for this research. The paper examines compliance theories, challenges, and security threats that small healthcare organizations are most vulnerable to. It recommends services and technologies that are available to them to become compliant, and how they can maintain continued compliance once they become compliant. A process model and an action compass are proposed to guide small businesses in their compliances efforts.

The rest of the paper is structured as follows. The next section will conduct a literature review on the HIPPA requirements, enforcement mechanisms, and compliance theories. Then, the paper introduces RegEye and discusses its path to HIPAA compliance. The third section includes discussions on InfoSec risks that are prevalent in the small healthcare provider setting. Section four will discuss the various solutions available to work towards HIPAA InfoSec compliancy, including a proposed process model and an action compass. Then the paper presents some observations on HER system adoption. Finally, it ends with a summary and conclusions.

Literature review

The health insurance portability and accountability act

The HIPAA of 1996 consists of two distinct parts, portability, and accountability. Portability refers to patients' ability to keep health insurance between jobs. It limits exclusions from preexisting health conditions.[11] However, the part of HIPAA that is of interest to InfoSec professionals is the second part, the accountability. The HIPAA privacy rule defines how personally identifiable information is used and protected. In the industry, personally identifiable health information is known as PHI. The key is 'personally identifiable' or where health information can be directly tied to a particular individual. This is important, as health information can be made public for research and statistical uses as long as it includes no personally identifiable characteristics, such as name, address, birth date, social security number.

The security requirements in HIPAA were further enhanced by the ARRA of 2009. ARRA amends the Social Security Act by establishing incentive payments to eligible professionals, eligible hospitals, and Medicare Advantage Organizations to promote the adoption and meaningful use of interoperable health information technology and qualified electronic health records.[12]

The adoption of electronic health record systems is widely considered a way to curb rising healthcare costs. In the United States, healthcare costs in 2012 accounted for 18% of U.S. gross domestic product (GDP), roughly $2.8 trillion. If left unchecked, the costs can rise to 25% of GDP and take up approximately 40% of the total federal spending by 2037. Since administrative costs and medical record keeping account for nearly 13% of U.S. healthcare spending, implementing electronic medical records systems has become a major focus to reduce costs and improve healthcare quality.[13] On the other hand, the wide adoption of electronic record systems increases the risk of security breaches, consequently raising the challenges for securing electronic record systems.

Businesses affected by HIPAA rules

The U.S. Department of HHS has detailed information to determine who is considered a covered entity (CE) or a business associate that must abide by HIPAA rules. In general, individuals, organizations, and agencies of the following types are CEs: a healthcare provider, such as a doctor, dentist, optometrist, podiatrist, dermatologist, chiropractor, clinic, pharmacy, and any business entity that generates or uses PHI; a health plan, such as a

health insurance company, a company health plan, or government programs such as Medicare, Medicaid, and military and veterans' healthcare programs; a healthcare clearinghouse where health information is being converted from one format to another. Business associates, such as contractors or consultants, to the above entities are also affected by HIPAA rules.[14]

Basic HIPAA security rules

The HIPAA security rules were written as very general guidelines, with no details regarding current or future information technology. No particular hardware devices, software, nor technologies are mentioned in the rules. As a result the rules, are sometimes quite vague and open to interpretation by InfoSec professionals. Therefore, InfoSec professionals typically implement current best practices.

According to USDHHS,[14] the best practices include the following: (a) Ensure the confidentiality, integrity, and availability of all e-PHI they create, receive, maintain, or transmit; (b) Identify and protect against reasonably anticipated threats to the security or integrity of the information; (c) Protect against reasonably anticipated, impermissible uses or disclosures; and (d) Ensure compliance by their workforce.

Furthermore, CEs are to perform following activities and review them on a regular basis:

Risk Analysis and Management

- Evaluate the likelihood and impact of potential risks to e-PHI
- Implement security measures to address the risks identified in the risk analysis
- Document and provide rationale for chosen security measures
- Maintain continuous, reasonable, and appropriate security protections

Implement Administrative Safeguards

- Designate a security official who is responsible for developing and implementing its security policies and procedures
- Implement policies and procedures for authorized access to e-PHI using role-based access
- Train all workforce members regarding its security policies and procedures.
- Establish appropriate sanctions against workforce members for those who violate policies and procedures
- Conduct periodic evaluation

Implement Physical Safeguards

- Limit physical access to its facilities, yet ensure authorized access is available
- Establish policies and procedures regarding proper use of computer workstations and electronic media.
- Establish policies and procedures regarding the transfer, removal, disposal, and reuse of electronics media.

Implement Technical Safeguards

- Access Control – A CE must implement technical policies and procedures that allow only authorized persons to access e-PHI.
- Audit Controls – A CE must implement hardware, software, and/or procedural mechanisms to record and examine access and other activity that contains or uses e-PHI.
- Integrity Controls – A CE must implement policies and procedures to ensure that e-PHI is not improperly altered or destroyed. Electronic measures must be put in place to confirm that e-PHI has not been improperly altered or destroyed.
- Transmission Security – A CE must implement technical security measures that guard against unauthorized access to e-PHI that is being transmitted across an electronic network.

Above list was verbatim or paraphrased from USDHHS.[14]

HIPAA security enforcement mechanism

The Security Rule is enforced by the OCR within the U.S. Department of HHS. Investigations are usually triggered by complaints of HIPAA violations or media reports, but the OCR has stepped up random compliance audits of CEs in recent years as it starts implementing Stage 2 HIPAA Audits.[15] The HIPAA Breach Notification Rule[16] requires CEs and their business associates to notify affected individuals and the Secretary of HHS breaches within 60 days of the breach discovery. Media notice is required if a breach affects 500 residents of a state or jurisdiction area.

Compliance theory

Regulatory compliance and noncompliance have been a subject of research for decades in business, psychology, sociology, and law. Sommestad *et al.*[17] conducted a systematic review of empirical studies on factors that influence organizations' compliance with InfoSec polices and how important these

factors are. Their study identified the following major factors: subjective norm, self-efficacy, perceived risk, response cost, perceived severity of sanctions, and perceived certainty of sanctions.

Subjective norm is perceived social pressure to engage or not to engage in a behavior.[18] Subjective norm and attitude determine behavior intention, which can lead to increased or decreased effort to perform the behavior.[19] Self-efficacy refers to an individual's belief in his or her capacity to execute behaviors necessary to produce specific performance attainments.[20] It is influenced by resource capacities such as knowledge about the law and regulation, technical skills, and managerial capacity.

Research studies on general deterrence theory[21] have found that both punishment and reward systems were effective to increase employees' intention to adhere to their security policies.[22,23] Good understanding of security risk and organizational commitment to security have a significant influence on users' intention to comply with corporate security policies.[23,24] Security risk is measured based on the probability of a security breach and the resulting cost of the breach. It is the general belief that the higher the risk of a breach, the stronger the intention to comply. However, this effect may be offset by the cost of compliance.

The following section will discuss RegEye's path to HIPAA compliance. The discussions are organized around the above discussed compliance factors. It is the hope that this case study will provide additional insights on compliance theory in the context of small healthcare providers.

The RegEye case study

RegEye was founded in 1974 (under a different name) with humble beginnings and conducted its operations out of a small building. The original founder approached retirement and put the small business up for sale in the late 1980's. Two doctors specializing in ophthalmology purchased and grew the business. In the mid 2000's, they had outgrown their original space, and constructed a much larger facility nearby. The new state-of-the-art facility includes a surgical center and features all the latest medical instrumentation and technology.

Today, RegEye has grown into a business co-owned by two doctors and an optician, has four practicing doctors and a staff of approximately 30. RegEye serves a large rural population center and outlying areas. Patient demographics consist of all age groups, with senior citizens comprising a significantly larger percentage of patients. Senior patients have an increased incidence of eye health issues, resulting in more frequent eye care exams and a higher incidence of mobility and transportation issues. To serve their rural and senior patients better, RegEye doctors and technicians regularly travel to satellite offices. As such, doctors and technicians must be able to access electronic health records from remote locations.

In the 1990s, most data management and compliance work at RegEye was still done manually. There were a few PCs for basic office duties such as word processing, accounting, etc. RegEye purchased some Practice Management software around 1998 to streamline business processes such as scheduling and billing. Since the business was small, they did not have an IT specialist in-house. To obtain some basic IT support with the practice management software, they contracted a consulting business from the Twin Cities, which is about an hour drive from RegEye's main business location.

As the business grew, more exam rooms and IT infrastructure were added; the cost of maintaining IT infrastructure was increasing. After the new building was constructed in 2007, there were 11 exam rooms, with a PC in every room. New staff members and work stations were added. The doctors kept buying new exam instruments; practically every new instrument consists of an integrated PC. Also, a fleet of laptops is needed for when the doctors and staff travel to regional clinics.

On top of that, the business must make sure all its business units meet all the government regulations such as HIPAA, HITECH, PCI DSS. The amount of paper work to prepare for compliance requirements was overwhelming for the small staff at RegEye. These challenges have led the business to rethink its IT support. It has become clear that they need a dedicated local consultant who is not only competent in IT infrastructure management but also knowledgeable about the new legislation and standards. In response to the Federal government's call for computerizing the nation's healthcare systems, RegEye also decided to adopt an Electronic Health Record (EHR) system. RegEye hoped that the new EHR system would bring down its operating costs and automate some of the compliance report generation.

RegEye's path to HIPAA compliance

Like many small healthcare providers, RegEye has been operating under a flat management structure. The three owners are practicing doctors and members of a governing board making strategic decisions such as facility expansion. A General

Office Manager (Chief Operating Officer) is in charge of the daily operations of three major business units: Regional Eye Center, Surgical Center, and Optical Store. Two assistant managers were also appointed to assist the General Manager. RegEye's HIPAA compliance experience can be divided into three periods.

The period of innocence (1996 – 2004)

HIPAA was passed by the U.S. Congress in 1996. Its enforcement did not start until 2003, for most health care organizations. Small healthcare providers whose annual receipts were less than $5 million had until April 14, 2004 to be compliant.[25] RegEye's owners and office managers heard about HIPAA but knew little about the specifics of its Security Rule. In addition, they were unfamiliar with IT security and unaware of any imminent security threats. Occurrence of hacking and data breaches during that time was relatively less frequent. RegEye's management genuinely believed that their business was unlikely to be targeted by hackers because it was small. Nevertheless, an outside consulting company was hired in 1998 and a preliminary security risk assessment was conducted. April 14, 2004 passed quietly and RegEye was not even aware of its compliance status.

The period of awaking (2004 – 2011)

The increased number of reported data breaches and hacking incidents in the news during this period brought the issue of security and HIPAA compliance into the forefront of RegEye's management agenda. In the winter of 2007, a security incident hit home when one of the owners' cars was stolen. In the back seat of the car were hard copy medical record charts of patients. The labels on the lost charts had the patients' names and SSNs, which was the standard practice at that time. Not knowing exactly how many patient records were stolen, RegEye notified all of its patients about the incident and offered credit monitoring for them.

The incident served as a wake-up call for RegEye to step up its effort in security practice. At the same time, reported violations of the HIPAA Security Rule started to appear more frequently in the news media. RegEye's governing board realized that security compliance was not just an obligation to HIPAA but also a self-protection from potential client lawsuits and business reputation damage from a potential security breach.

RegEye's commitment to HIPAA compliance was met with two major challenges: lack of financial resources and lack of technical expertise. The following sections discuss the challenges in general and RegEye's solutions in particular.

Lack of financial resources

The costs associated with HIPAA depend on the type and size of the business. For example, it would cost more for a big hospital to be compliant than for a small clinic or clearinghouse. It also depends on the culture and the business environment.[26] A business that depends heavily on Internet technology for data transactions, with conservative views on privacy and security, would likely spend more on its compliance efforts.

The cost can be divided into one time or reoccurring costs. Big hospitals may hire lawyers, consultants, vendors, and technical writers to work on HIPAA compliance. These costs would be one-time. The recurring costs include collection of confidential trash for shredding, disaster recovery services and/or offsite storage for backup media, printing, and mailing costs of Notice of Privacy Practices to patients, routine privacy auditing and monitoring activities, computer system updates and remediation, and training related costs.[27]

According to a report from Frost and Sullivan,[25] hospitals, managed care organizations, and private practices were expected to spend a combined $1.2 billion on products and services to address provisions of the HIPAA over the 2001–2003 period. Much of the spending was to make electronic health record and electronic data exchange systems HIPAA compliant.

Small healthcare providers like RegEye do not have a large IT budget and cannot afford in-house IT specialists or lawyers. The only solution is to contract with a reliable IT consultant who is also a HIPAA expert.

Lack of technical expertise

The expertise needed for implementing and maintaining HIPAA compliance includes general IT skills, knowledge in healthcare IT products and services, and deep understanding of the regulatory requirements. None of the mentioned technical skills are readily available in typical small healthcare providers.[28]

These businesses typically start operations with one or two doctors deciding to open their own business. They hire the required receptionist, scheduler, insurance payment processor, and medical technician personnel. Their basic IT infrastructure includes a few PCs, network router, and communication cable lines, which the owner usually obtains from a local retail store or purchases online. A local computer service and repair store may be

called upon to put these IT components together to make them work. Finally, a local telephone or cable company may be hired to provide the internet services.

IT staffing is the last thing on their minds because they do not have the financial resources to acquire IT personnel with the right set of skills, nor the scale of economy justify such hiring. In addition, they cannot afford to compete with big corporations on salary and fringe benefits to attract well qualified candidates.

With pressure from HIPAA compliance requirements and the business' need to drive down operating costs, the RegEye governing board finally decided to seek dedicated outside consulting services. The aim was to hire a local IT consultant who was knowledgeable in both HIPAA and IT security. A local consultant was needed because he or she was likely to be available to provide immediate assistance when unexpected events occurred. In early 2011, RegEye hired Mr B, a local IT consultant with experience in healthcare IT applications and HIPAA Security Rule implementation. Mr B was charged to begin implementing RegEye's new EHR system NextGen. Over the course of a year, the EHR system was tested and then fully implemented. Expansion of the EHR system at RegEye is continuing, as EHR is implemented into the various aspects of the business, beyond exam records, into direct exam data collection from instrumentation and into billing and insurance. The implementation of HIPAA Security Rule was also underway at the same time. A comprehensive risk assessment was conducted and a set of security policies was established and put into practice.

The period of compliance (2011 – present)

RegEye's HIPAA compliance effort is led by the General Manager and is increasingly driven by RegEye's insurance company. A monthly meeting with its insurance company is mandatory and attended by the General Manager, the IT specialist from the insurance company, and Mr B. Routine discussions in these meetings include new changes in policies or current business practices, staff changes, training, and updates on the best HIPAA security practices in the industry. RegEye also holds regular employee meetings, typically once a month. These meetings also include HIPAA compliance topics.

Keeping up with the changing regulatory requirements is a big challenge. As the technology and security landscape keep evolving, the U.S. Congress passes new laws or modifies existing laws to strengthen health information protection or to mend the loop holes. For example, the HITCH passed in 2009 modified certain provisions of the Social Security Act pertaining to the HIPAA rules to strengthen privacy and security, and enforcement. The Act also added new requirements for notification of breaches of unsecured PHI by covered entities and business associates. On January 25, 2013, the HIPAA Omnibus Rule was published as a final rule to implement a number of provisions of the HITECH Act and to strengthen the privacy and security protection.[1]

HIPAA compliance is not a single task. Once the healthcare provider has become HIPAA compliant, it must commit to continuous monitoring and scanning for new risks and vulnerabilities. Security is a moving target in today's fast changing technology world; new risks and vulnerabilities can pop up when implementing new EHR software, upgrading to new operating system, installing new diagnostic equipment, subscribing to cloud computing services or starting to use a new mobile device for work.

RegEye recently upgraded the operating system on all its workstations to Windows 10. Such a seemingly routine upgrade involved many hours of research and remedies in security. For example, by default settings of many Windows 10 new features, data and settings are automatically backed up or sent to remote servers owned by Microsoft. Bitlocker in Windows 10 will automatically backup user's encryption key to OneDrive; Data Sync allows the operating system to sync settings and data into Microsoft's remote servers. If those default settings are not changed, the business is at risk of violating HIPAA privacy and security rules.

In summary, RegEye's HIPAA compliance has gone through three periods in which several factors played important roles: awareness of security threats, knowledge of HIPAA and IT security, personal security incident, resource capacities (financial and technical expertise), cost of security breach and HIPAA violation. Figure 1 illustrates the compliance process and the major impacting factors.

Information security risks for small healthcare providers

Small business in general have limited understanding of InfoSec and they often fail to perform risk assessment or create security policies.[29,30] According to Healthcare Information and Management Systems Society, 33% of small healthcare providers had never conducted a security risk assessment.[6] They are less likely to implement preventive measures when compared to large organizations.[31] Although there are many InfoSec risks in

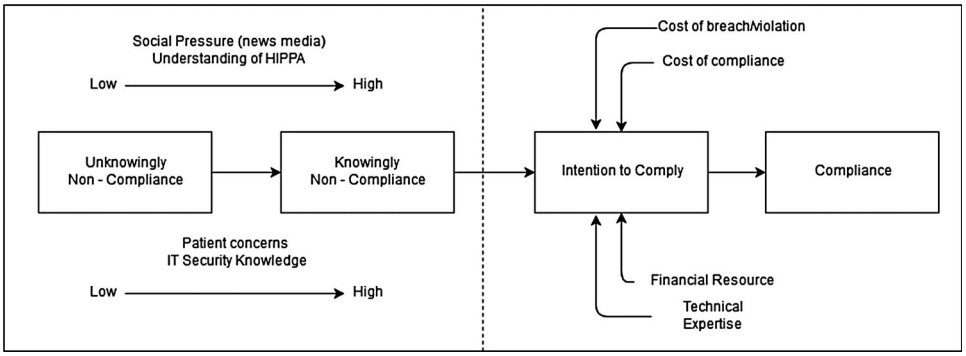

Figure 1 RegEye HIPAA compliance process.

the small healthcare company environment, this paper will discuss the most prevalent risks. They are general lack of IT knowledge and security practices; unauthorized access to the wireless network; physical loss of portable/mobile devices; lack of controlled access and lack of an audit trail; viruses / malware / spyware; and loss of data.

Lack of professional IT knowledge within small healthcare companies is very typical. The core business focus for these companies is healthcare. Many of them do not have a permanent IT person on staff. This lack of professional IT knowledge contributes to the following common problems: lack of security planning and risk assessment; lack of comprehensive security and auditing policies and procedures.

The biggest potential risk is unauthorized access via the wireless network. The simple mistake of not securing the wireless network can result in the neighborhood kids snooping through medical records and documentation. Worse yet, it is not evident this is going on. There is no physical indicator that something is amiss.

The next risk is physical loss of equipment, particularly laptops and mobile devices. These are high theft items. According to the 2014 Healthcare Breach Report from Bitglass, 68% of all healthcare data breaches since 2010 are due to device theft or loss.[32] A 2010 study sponsored by Intel and conducted by Ponemon Institute, appropriately named 'The Billion Dollar Lost Laptop Problem,' revealed the statistical losses are astounding. The average economic consequence per lost laptop is $49 246.[33] It is not the cost of the physical laptop itself that is damaging, rather the lost information, productivity, and reputation. Another risk that is often overlooked is the loss of USB flash drives. We often do not think of these devices because they are kept in the top desk drawer or carried around in pants' pockets. However, again, it is not the cost of the USB flash drive, but rather the e-PHI that might be contained on that device.

A risk that everyone is familiar with is viruses / spyware / malware. The spyware publicized lately in the news media is extremely sophisticated. Spyware purposely goes undetected, and allows hackers a backdoor into a network. Again, this is a case where one is being breached, but does not even realize it. The risk of viruses / spyware / malware is significantly higher in the small business environment as there is not a continuous IT presence to be vigilant against such threats, nor is there regular employee training to reinforce caution against these threats.

Unauthorized access of patient medical records is another risk. HIPAA requires that there be an audit trail of who accessed patient information and when to maintain confidentiality and integrity. It is imperative that those that access medical records have a need to do so to perform their job duties, i.e. on a need-to-know basis. Equally important is to guard against the unexpected change or deletion of medical information, either intentionally, or accidentally.

Another major risk that is often not considered, until a hard drive fails on a workstation or server, is loss of data. Actual verifiable numbers are elusive as to the survivability of a business after a major data loss. At any rate, major data loss would be a huge upset to the business's operations.

Suggested solutions for HIPAA compliancy

Figure 2 below shows a possible HIPAA InfoSec compliancy process model.

The first step in the process model is to fully understand HIPAA requirements. Small business management/owners must take regulatory compliance seriously and be self-educated on the relevant laws and standards. Seeking professional legal advice is advisable when confusions or different interpretations of a clause occur. The self-assessment step is designed to assess how far the business

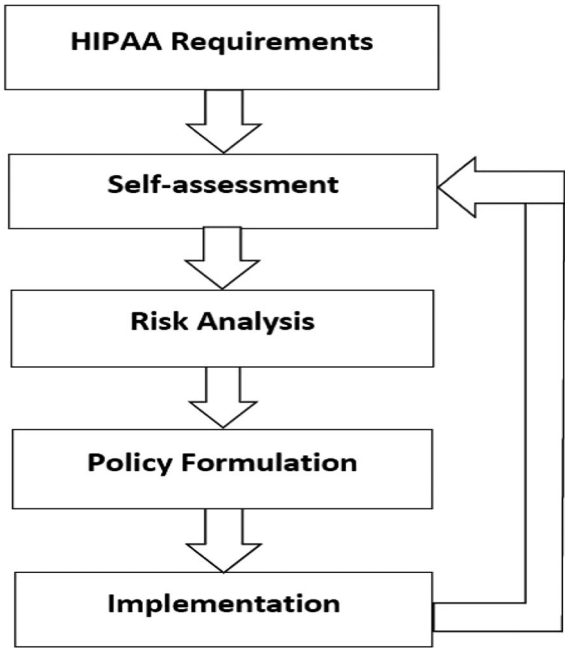

Figure 2 A process model for HIPAA InfoSec compliance.

Figure 3 Compliance action compass for small healthcare providers.

deviates from HIPAA compliance. See the appendix for a representative survey instrument. Risk analysis is performed to determine the greatest risk exposures and priority for protecting the most valuable assets. Then, security policies and procedures are formulated to mitigate exposure to the risks. Policies and procedures must be faithfully implemented and monitored, which can involve multiple measures, such as training, changing old business processes, adopting a new incentive and performance evaluation system. This is a closed-loop continuous improvement process, as requirements, threats, and hardware/software solutions evolve and change over time.

Figure 3 shows an action compass. It suggests specific actions that small healthcare providers can take. Making resources available for HIPAA compliance is the critical step, which represents the management commitment. Successful compliance needs every organizational member's involvement. Therefore, building a compliance culture is equally important. Regular staff training and conversations on HIPAA compliance are strongly encouraged. Security policies and procedures should be in written form and widely distributed. A contingency plan for a possible security breach must be developed and widely discussed. Such a plan should include measures for minimizing business interruption in case of a breach as well as a plan to notify media outlets and affected clients as the law requires. Finally, security awareness should be ingrained in common sense practices. It does always require extra effort to be secure. For example, a RegEye employee used to transfer patient data via a flash drive from exam room to the surgical center when a patient needs surgery. Such practice was stopped because it clearly increases the security risk when the flash drive is lost or stolen. Finally, regular review of compliance should be made mandatory and part of security policies.

Practical solutions to the before mentioned risks will help meet companies' HIPAA InfoSec Compliancy. Table 1 shows major risks, solutions, and HIPAA goals. Solutions are available at different price points depending on scalability as the organization grows.

The first risk mentioned above, the lack of IT knowledge, can be protected against in several ways. The most cost effective way for the small healthcare provider would be to contract regularly scheduled time with an IT professional they know and trust. The IT professional should have a long term working relationship with the business and must be willing to sign a HIPAA BAA (Business Associate Agreement) which states that the IT professional will follow all HIPAA standards. The IT professional should provide training to employees regarding standard security practices. If the business continues to grow, then eventually IT services could be brought in house and a full-time IT staff member can be hired.

Secure the wireless network. It can be as simple as ensuring that WPA2 encryption is always active, and that the WPA2 encryption passphrase is regularly changed. A more secure approach, which was implemented at RegEye, was to use enterprise grade wireless access points that communicate to a

Table 1 Suggested risk mitigating solutions

Risks for small business	Practical solutions	HIPAA goals met
Lack of IT knowledge	Regular contact with IT professional. BAA signed.	Confidentiality / Integrity Security
Wireless network security	WPA2 encryption. Passphrase regularly changed. Documented regular verification.	Security
Loss/theft of mobile device	Encryption of storage devices. Screen passlock.	Privacy safe harbor rule
Viruses / Malware / Spyware	Centrally managed antivirus product.	Security
Lack of audit trail	Domain controller.	Audit controls person or entity authentication Security
Loss of data	Redundant backup solutions. Encrypted during transit and at rest.	Availability security

centralized controller. Several layers of security on the RegEye wireless network are being employed: the wireless link is using WPA2 enterprise encryption, the user must have an account in Active Directory (AD), and there must be a certificate installed on the mobile device accessing the wireless network. This solution guards against ex-employee unauthorized access, as the ex-employee will no longer have an account in AD. Also, requiring a certificate on the mobile device makes it extremely unlikely that an outside device can gain access.

It is nearly impossible to guarantee a mobile device will never get lost/stolen. So one just has to assume it will happen. Therefore, it is critical that all laptop devices have encrypted storage drives. Once the drive is encrypted, the business is then protected by the 'Safe Harbor Rule' (Meeting HIPAA Encryption Requirements HIPAA Central). The Safe Harbor Rule basically states that if a business has a breach, and the breached data are encrypted, then the business is exempt from reporting the breach. On a similar note, all handheld devices such as tablets and smart phones need to have a lock screen passcode to be protected under the Safe Harbor Rule. To meet the encryption requirement, every laptop drive at RegEye is encrypted using an open-source (free) encryption package called TrueCrypt. Windows 8 has Bitlocker encryption included with the OS that can be used to encrypt a drive. Be aware that the decryption keys must not be stored with the device. Preferably decryption keys should be stored in a locked file cabinet. Also, if the laptop is booted and logged in, then the data are readable. Therefore, as an extra precaution, laptops should be configured to power down when their lids are closed.

Viruses / Malware / Spyware are a constant, ever evolving, threat. Therefore, it is imperative that a high- quality antivirus product be used that can be centrally managed and monitored. The central monitoring aspect is important. Several free antivirus products are available, and Microsoft even includes a free product with their operating systems. Unfortunately, the free products cannot be centrally managed. Without central monitoring, companies are not aware of possible infections on workstations, unless the workstation owner notifies her manager of a potential problem. With centrally managed antivirus solutions, the manager is notified immediately of a potential problem.

HIPAA requires that there be an audit trail of who accessed patient information and when. Although the EHR software has individual user login at the application level and the ability to do auditing, the workstations themselves did not have a specific login at the OS level per user. The workstations had a common username/password. That has now been changed. A Microsoft domain controller server has been installed at RegEye and all workstations have been joined to the domain. With AD, all users and their rights can be controlled. Using AD has also given one the ability to tighten security on the wireless network, as a valid username/password is required to connect to the wireless network. Confidentiality, both at the workstation level and at the EHR application level, are now both enforced. This also protects the integrity of the health information from unexpected change or deletion of medical information, either intentionally, or accidentally.

Finally, for data loss risk, the solution is three words: backup, backup, backup. The current saying is 'if the data is not backed up in three places, then it isn't backed up.' Several solutions are available, such as external hard drives, off-site backups, etc. To meet HIPAA regulations, online

or offsite backup solutions must employ encryption while at rest and also while in transit. The solution adopted at Regional Eye Center was to use a file server hosted by the local telecom that has a Storage Area Network (SAN) that replicates the encrypted data to three datacenters located in separate geographic areas. In theory, with the SAN backup solution chosen for Regional Eye Center, 100% availability of the data at all times is expected.

Observations on EHR system adoption

Healthcare providers have an array of software packages from a multitude of vendors to choose from to implement an EHR system for their business. It is an open market where a healthcare provider carefully analyzes the variety of software packages that fit their particular specialty, such as optometry, dentistry, general medicine, etc. and chooses the package that they think will work best for their healthcare practice. Consequently, each healthcare provider, whether large or small, is responsible for the purchase, implementation, and customization of their particular EHR system.

This approach has led to islands of stand-alone EHR systems, where the EHR system for each healthcare provider is separate from all other EHR systems. Patient data are repeatedly duplicated in each and every EHR system, as there is no centralized data repository of patient information.

Some could argue that a better model would be a national EHR system, where the government would house a centralized database. An example of a country taking this centralized approach is Jordan. The Jordanian government is leading the way and will have the largest national single EHR system in the world with their entire population in a single EHR system.[34] Surprisingly, the EHR package used, is VistA, which is an open-source package developed for and used by the United States Veterans Administration.

Healthcare providers began receiving financial incentives from the United States Federal government starting in 2011 and will continue receiving financial incentives through 2016 to implement EHR. To qualify for the incentive payments, healthcare providers must demonstrate 'meaningful use,' i.e. showing that they have implemented EHR throughout their practice and are using it in their day-to-day business activities.

'Meaningful use' has been a moving target by the federal government as to what exactly constitutes meaningful use. Meaningful use originally was assumed to mean that the EHR system was in place and was in daily business use. But in the past couple of years, the federal government has also included an InfoSec component mandated by HIPAA. Small business healthcare providers do not typically have IT people on staff, nor do they know what questions to ask from contracted IT. Therefore, for a small healthcare provider to implement HIPAA InfoSec compliance into their healthcare practice is a real challenge.

Even with the financial incentives available to implement EHR, adoption has been slow for small healthcare providers. Various studies have been done suggesting that the cost savings of implementing an EHR system may be realized in large healthcare institutions, but may be actually causing financial harm to the small healthcare provider.[35] Much of the cost increase is associated with economies of scale, which the small healthcare provider does not have.

Conclusion

This paper employed a case study method to examine the factors that influence small healthcare providers' HIPAA compliance effort. The study suggests that many small healthcare providers may experience a period of unknowingly non-compliance due to the unique challenges they face, such as limited technical and financial resources. This experience may be relatively uncommon among large healthcare organizations. The study confirmed the existing compliance theory in which social pressure, knowledge of legislation, and self-efficacy contribute to an organization's intention to comply. In addition, this study examined the most common InfoSec risks for small healthcare providers and recommended available techniques to minimize the risks. Finally, the study proposed a HIPAA InfoSec compliancy process model and an action compass for continuous improvement and monitoring. Future case studies should investigate large healthcare organizations' compliance processes.

Disclaimer statements

Contributors None.

Funding None.

Conflicts of interest None.

Ethics approval None.

ORCID

Allen Benusa http://orcid.org/0000-0002-0452-6371

Appendix

Self-assessment survey

The following questions are meant as a self-assessment survey. Depending on the size and nature of your organization, answering 'No' to some questions is not necessarily a HIPAA violation.

Are you a healthcare provider, such as a doctor, dentist, orthodontist, optometrist, chiropractor, massage therapist, or long-term facility that generates or uses PHI? Yes No

Do you regularly contract with an IT professional who you know and trust? Yes No

Do you have a BAA in place with your contracted IT professional? Yes No

Do you provide training on a regular basis to all employees regarding HIPAA and best practices? Yes No

How many PCs (desktops and laptops) are in your business? _____

What operating systems are your PCs running? Windows 8 Windows 7 Windows XP Mac OS X Other

Are your PCs joined to a domain and are you using AD? Yes No

Do you have a commercial grade router / firewall? Yes No

Do you have a wireless network? Yes No

Is your wireless network secured with WPA2 enterprise level encryption? Yes No

Do you access work email or other work documents through your mobile device, such as a tablet or phone? Yes No

If so, does your mobile device have a lock code enabled? Yes No

Do all laptops have their hard drives fully encrypted? Yes No

When the lid is shut on the laptop, does it shutdown? Yes No

Do you use USB flash drives / thumb drives / jump drives? Yes No

Are your USB flash drives encrypted? Yes No

Do all PCs have a reliable antivirus running that auto updates? Yes No

Is your antivirus solution centrally managed? Yes No

Is critical data for your business backed up in at least three places? Yes No

Is your offsite backup encrypted? Yes No

References

1. HSSD. Modifications to the HIPAA privacy, security, enforcement, and breach notification rules under the health information technology for economic and clinical health act and the genetic information nondiscrimination act; Other modifications to the HIPAA rules. [Online]. Available from: www.FederalRegister.gov; 2013.
2. Cherry DK, Hing E, Woodwell DA, Rechtsteiner EA. National ambulatory medical care survey: 2006 summary. National Health Statistics Reports, no. 3. Hyattsville MD, National Center for Health Statistics; 2008.
3. Casalino LP, Pesko MF, Ryan AM, Mendelsohn JL, Copeland KR, Ramsay PP, *et al.* Small primary care physician practices have low rates of preventable hospital admissions. Health Aff 2014;33(9):1680–8.
4. Kane CK, Emmons DW. New data on physician practice arrangements: private practice remains strong despite shifts toward hospital employment. Chicago, IL: American Medical Association; 2013. [Online]. Available from: http://www.nmms.org/sites/default/files/images/2013_9_23_ama_survey_prp-physician-practicearrangements.pdf.
5. Martin, NL, Imboden TR. Information security and insider threats in small medical practices. Proceedings from the Twentieth Americas Conference on Information Systems. Savannah, GA; 2014.
6. Healthcare Information and Management Systems Society. Privacy and security toolkit for small provider organizations. [Online]. Available from: http://www.himss.org/library/healthcare-privacy-security/small-providertoolkit?navItemNumber=16493; 2011.
7. HHS. $750,000 HIPAA settlement underscores the need for organization-wide risk analysis. News Release, [Online]. Available from: http://www.hhs.gov/about/news/2015/12/14/750000-hipaa-settlement-underscores-need-for-organization-wide-risk-analysis.html#; 2015.
8. McGee, MK. $150K HIPAA fine for unpatched software. [Online]. Available from: http://www.databreachtoday.com/150k-hipaa-fine-for-unpatched-software-a-7656/op-1; 2014.
9. McCann E. Groups hit with record $4.8M HIPAA fine. *Healthcare IT News*. [Online]. Available from: http://www.healthcareitnews.com/news/group-slapped-record-hipaa-fine; 2014.
10. HHS. Annual report to congress on HIPAA privacy, security, and breach notification rule compliance for calendar years 2011 and 2012. [Online]. Available from: http://www.hhs.gov/hipaa/for-professionals/compliance-enforcement/examples; 2012.
11. United State Department of Labor. Health Plans and Benefits. HIPAA. [Online]. Available from: http://www.dol.gov/dol/topic/health-plans/portability.htm; 2014.
12. Centers for Medicare & Medicaid Services (CMS). Electronic health records incentive programs. [Online]. Available from: https://www.cms.gov/Regulations-and-Guidance/Legislation/EHRIncentivePrograms/index.html?redirect=/ehrincentiveprograms; 2015.
13. Laudon K, Laudon J. Essentials of management information systems. 11e ed. Prentice Hall;2015.
14. United States Department of Health and Human Services. Office for civil rights. Health information privacy. [Online]. Available from: https://www.hhs.gov/hipaa/index.html; 2016.
15. Lynn, J. Are you ready for stage 2 HIPAA audits? *HealthcareScene.com* [Online]. Available from: http://www.emrandhipaa.com/emr-and-hipaa/2016/

06/27/are-you-ready-for-stage-2-hipaa-audits/; 2016.
16. HHS. HIPAA breach notification rule, 45 CFR 165.400-414. [Online]. Available from: http://www.hhs.gov/hipaa/for-professionals/breach-notification/; 2009.
17. Sommestad T, Hallberg J, Lundholm K, Bengtsson J. Variables influencing information security policy compliance: a systematic review of quantitative studies. Inform Manag Comput Sec 2014;22(1):42–75.
18. Colman A. Theory of reasoned action. A dictionary of psychology (4th ed.). Oxford: Oxford University Press; February; 2015.
19. Ajzen I, Fishbein M. Understanding attitudes and predicting social behavior. Nebraska symposium on motivation, Vol. 27, Englewood Cliffs, NJ: Prentice-Hall; 1979. pp. 65–116.
20. Ormrod JE. Educational psychology: developing learners (5th ed.). Upper Saddle River, NJ: Pearson/Merrill Prentice Hall; 2006.
21. Straub DW, Welke, RJ. Coping with systems risk: security planning models for management decision making. MIS Quart 1998;22(4):441–69.
22. Chen Y, Ramamurthy K, Wen K. Organizations' information security policy compliance: stick or carrot approach? J Manage Inf Syst 2013;29(3):157–88.
23. Herath T, Rao R. Protection motivation and deterrence: a framework for security policy compliance inorganizations. Eur J Inf Syst 2009;18:106–25.
24. Dojkovski S, Lichtenstein S, Warren M. Fostering information security culture in small and medium size enterprises: An interpretive study in Australia. Proceedings of the 15th European Conference on Information Systems, St. Gallen, Switzerland, June 2007. Pp.1560–71.
25. Worrell B. Analyst: HIPAA compliance proves costly for health care providers. Healthcare Strat Manage 2002;20(12):6.
26. Patlak M, Smith A, Cox K, Shah P, Young R. The costs of HIPAA to patients, to progress, and to the nation's health. C-Change Strategic Initiative. [Online]. Available from: http://c-changetogether.org/websites/cchange/images/hipaa/c-change_hipaa_cost_study_web_version.pdf; 2012.
27. Walsh T. What will HIPAA cost? and HIPAA privacy and proposed security standards: a tandem approach to compliance. Advanced Health Care Network. [Online]. Available from: http://health-information.advanceweb.com/Article/What-Will-HIPAA-Cost-and-HIPAA-Privacy-and-Proposed-Security-Standards-A-Tandem-Approach-to-Compliance.aspx; 2014.
28. Sterling Ron. Defend your practice against HIPAA violations. Med Econ 2015;52–7.
29. Dimopoulos V, Furnell S, Jennex M, Kritharas I. Approaches to IT security in small and medium enterprises. Proceedings of the 2nd Australian Information Security Management Conference. Perth, Western Australia; 2004.
30. Gupta A, Hammond R. Information systems security issues and decisions for small businesses: an empirical examination. Inform Manag Comp Sec 2005;13(4):297–310.
31. Kankanhalli A, Teo HH, Tan BCY, Wei KK. An integrative study of information systems security effectiveness. Int J Inform Manag 2003;23(2):139–54.
32. Bitglass. Healthcare breach report 2016. [Online]. Available from: http://www.bitglass.com/healthcare; 2016.
33. Ponemon Institute. The billion dollar lost laptop problem. [Online]. Available from: http://www.intel.com/content/dam/doc/white-paper/enterprise-security-the-billion-dollar-lost-laptop-problem-paper.pdf; 2010.
34. Campaign for NHS Vista. [Online]. Available from: http://nhsvista.net/; 2015.
35. Congressional Budget Office. Evidence on the costs and benefits of health information technology. [Online]. Available from: http://www. cbo.gov/publication/41690?index=9168; 2008.