UNIVERSITY OF ILLINOIS AT URBANA-CHAMPAIGN

BUSINESS ADMINISTRATION 458: ENTERPRISE IT GOVERNANCE

MICHAEL J. SHAW

HIPAA: HEALTH INSURANCE PORTABILITY AND ACCOUNTABILITY ACT

MAY 1ST 2008

MICHAEL ELKIND

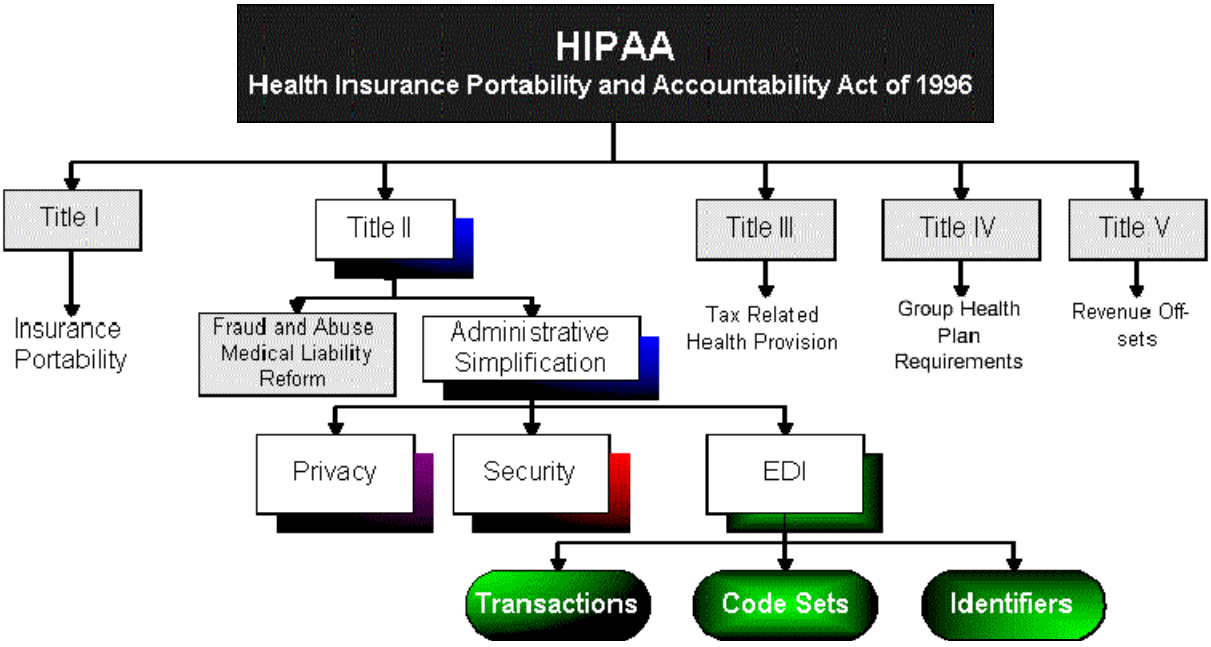
HIPAA: INTRODUCTION

This mission of healthcare has long been the aspiration to combat disease and illness. In today's world of electronic prosperity and growth, this healthcare mission has formed an alliance with information technology extending the battle against "electronic" diseases that threaten and scrutinize privacy of patient information. The Health Insurance Portability and Accountability Act, better known as HIPAA, is a broad federal legislation requiring, among additional things, that healthcare providers and beneficiaries implement and utilize electronic safeguards insuring patients' data protection. This protection scheme encompasses many electronic components requiring consistent confidentiality, integrity, and availability (accountability connotation of HIPAA). In addition, HIPAA enactment and alignment with IT systems significantly reduces paperwork and paper database utilization. Of course, with this push toward "losing a paper trail" comes heightened awareness over secure layering of IT applications interfacing and protecting healthcare information.

Furthermore, HIPAA forbids health-care providers and insurers from disclosing sensitive information about patients without their consent. In essence, HIPAA's overarching goal was not only to protect privacy of patient information, but also allowing freedom of transfer and portability after a patient acknowledges and gives consent to healthcare professionals. HIPAA legislation is very complex and its implications are predominantly broken down into two key titles (FIGURE 1 on the following page depicts a complete structure of HIPAA). Title I of HIPAA solidifies health insurance coverage for workers and their families when they change or lose their jobs. In essence, Title I is responsible for maintaining group (family/spouse or work) and

individual health insurance plans. Title II of HIPAA, deemed as the Administrative Simplification (AS) provisions, requires the establishment of national standards for electronic health care transactions and national identifiers for healthcare providers, health insurance plans, and employers.[1] The AS provisions also deal with the security and privacy of health data. These standards are meant to improve the efficiency and effectiveness of the nation's healthcare system by encouraging the widespread use of electronic data interchange (EDI) in the United States. The majority of this document will focus on Title II of HIPAA with a large emphasis on The Privacy & Security Rule's of HIPAA as they pertain vividly to utilizing information technology as the backbone of safeguarding patients' medical information.

FIGURE 1



[1] *Health Insurance Portability and Accountability Act*, http://en.wikipedia.org/wiki/HIPAA (30 April 2008).

HIPAA: THE PRIVACY RULE[2]

Privacy, by dictionary definition, is defined as "the state of being free from intrusion or disturbance in one's private life or affairs." The HIPAA Privacy Rule took effect on April 14, 2003. This enacted rule began regulating how certain health care groups, organizations, and businesses, deemed as covered entities, handle an individual's protected health information (PHI).[3] A very interesting aspect of The Privacy Rule is how healthcare research organizations can continue conducting research on healthcare information. It is important to note that research organizations are not covered entities under The Privacy Rule, thus they are not subject to its underlying regulations. For example, a covered entity such as a chain of regional hospitals can employ an independent research organization that is not subject to the ruling and therefore exempt from HIPAA's protection clause. From a security perspective, this poses a severe threat because it encourages working around legislation and thus potentially exposing protected healthcare information (PHI) in an unacceptable manor. Granted, there are clauses put into The Privacy Rule that anticipate for such misuse and attempt to address and define how an uncovered entity transmits and handles healthcare information in connection to financial records for administrative purposes.

In essence, before The Privacy Rule was established there were no real boundaries, a scary thought; yet, now the overarching idea of The Privacy Rule is to establish and maintain a

[2] *U.S. Department of Health and Human Services: National Institutes of Health*, http://privacyruleandresearch.nih.gov (2 February 2007).

[3] "Summary of the HIPAA Privacy Rule," *United States Department of Health Services*, May 2003, p. 3.

layer of data protection on healthcare information usage. Inevitability, research organizations and medical professionals whose job description is defined for healthcare data-mining, disease registries, health statistics, and growing trends will continue utilizing sensitive health information. However, with a rule in place there finally is a fine line between an acceptable industry practice and plain old abuse which will lead to severe consequences promoting discipline and punishment. In sum, The Privacy Rule depicts a guideline for which PHI is utilized and accepted under law. In many cases, it forces medical professionals to use only the minimal information required to process a patient's information; likewise, the rule also ensures that any incorrect information be properly addressed at the patient's request. A brief interview with A&E Medical Supply's delivery driver relieved that many patients were upset when their height and weight were improperly entered for their PHI. Even though the information regarding the height and weight was irrelevant to the equipment being proved, under HIPAA's ruling, A&E was forced to return to the patient's home and encode a correction of information within the patient's PHI. Luckily, such a mistake is common and an easy fix for a covered entity. However, there are many real offenses against patients' PHI. As with many offenses there are two main categories (civil and criminal) to which HIPAA adheres to. Other violations are prevalent in society, however civil and criminal constitute the majority.

HIPAA: PENALTIES[4]

The first category is deemed as a civil offense. This type of penalty is likely to be imposed when the offender was negligent to the law or did not have knowledge of wrongdoing. Typically, fines for civil penalties are $100 per person per violation with financial severity escalating to $25,000 per year for multiple violations within a $25,000 cap for one year per violator. These violations are subject to change at will from HIPAA's front office, yet the message is clear-cut: know the law or pay the price. Individuals within corporations or working for themselves under a business entity can be held personally liable for such violations.

The latter offense is much more severe hence being classified as a criminal offense. This type of penalty is imposed on individuals who knowingly disclose (includes selling) or receive (includes buying) PHI. Typically, fines include a year in jail along with a $50,000 monetary discipline. Committing an offense under false pretenses, for example pretending to be a doctor or obtaining a doctor's login information to utilize PHI under his status, is a highly frowned upon offense which constitutes a five-year imprisonment and a $100,000 fine. As if pretending to be a medical professional and receiving a five-year sentence was not enough, there is a severer penalty. To Good Samaritans, it is obvious that such an offense truly is degrading to humanity and unacceptable when considering how many people suffer from chronic diseases. Who on earth would ever want to sell PHI or solicit it for personal gain or malicious harm?

[4] Benton Goon, *HIPAA Privacy: How It Affect You*, http://dirm.state.nc.us/hipaa/hipaa2002/education/doc/presentation/DMH_HIPAA_LV1_Presentation.ppt (25 February 2007).

Unfortunately, there are criminals and eavesdroppers who violate such a sensitive area; luckily, they are penalized with a harsh $250,000 fine along with a ten-year prison sentencing.

HIPAA: THE SECURITY RULE

Security, by dictionary definition, is defined as "something that secures or makes safe; protection; or defense." HIPAA's Security Rule was established to complement The Privacy Rule. The remainder of the document will place a large emphasis on The Security Rule as it is highly correlated to IT infrastructure and security. While The Privacy Rule documented minimum requirements, definitions on entity holders and their status with HIPAA, and applicability to PHI, The Security Rule is primarily concerned with ePHI (Electronic Protected Health Information). The ruling is segmented into three components of security safeguards for ePHI: Administrative, Physical and Technical.[5] The administrative component is a general outline detailing how an entity will comply with The Security Rule. A significant portion of the administrative component is documentation and description of technical and hardware oriented approaches to protecting ePHI congruently with the other two elements. Yet, every accomplished security architect knows the importance of having strong documentation and planning to ensure understanding of implemented details. The strongest technical approach is meaningless if it cannot be properly translated to business users who need to interface and report on the business effectives of technology and engineering. The totality of the administrative safeguards can provide a laundry list of elements that need compliance. Some important to note due to their correlation to IT are properly defining authorization,

[5] *Health Insurance Portability and Accountability Act*, ibid.

establishment, and modification of ePHI. It is all too common for system administrators having difficulty finding a gray area that defines how electronic records will be updated, tracked, and what triggers need to be established to determine abuse or improper usage. The continuous war against hackers and outsiders causes seldom speculation on insiders working with electronic healthcare information. Administrators and senior-level IT personnel need not overlook a potential for internal abuse.

When on the drawing board for security, the first essential integrating layer ought to be backup plan for emergency situations such as outages, system failures, and beyond. A contemporary backup plan is essential and not a traditional backup at all in the twenty-first century IT realm. A stringent and consistent plan of action needs to be written up and documented prior to any organization exercising ePHI transacting, analysis, or support. A rocket ship can hit a warehouse and everything can go out in a tic of a second. A central hub can explode and leave users offline for days. Anything that can happen will happen. An excellent example of being “safe than sorry” was demonstrated by the guest speaker from the Illinois Terrorism Task Force and his story about a business in a tornado susceptible area of Illinois spending a dollar to protect a million (plus more in intangible worth of employees’ lives). By utilizing and building a brick barrier in the business’ bathroom area as a safe spot from a potentially disastrous tornado, not one life was lost in a disastrous storm that hit the building, and the company’s visionaries and financiers understood the fundamental goals of healthcare. Spend money at all costs to protect lives and their identities. Maybe that is why healthcare is

always scrambling for money from the government and taxpayers. Nonetheless, there is no better dollar spent than protecting a life or a history of one's health conditions.

The second component of The Security Rule is classified as administering physical safeguards.[6] The underlying idea behind this component speaks for itself; the control (safeguard) of physical access to protect against malicious use of protected data. In the world of technology, physical typically implies hardware solutions. In spite of this, it is imperative that new hardware solutions with complementary software solutions adhere to previous standards and functionality. A typical scenario would involve allowing employees to standardize a protected database with access to a mainframe through a secure terminal from a laptop computer. The underlying security checkpoints and layers are functioning, yet additional precautions need to be utilized ensuring that fragments of information are not stored in the laptop's temporary files. Likewise, anti-screenshot utilizes need to be applied to ensure a simple gesture as print screen (Print Scrn on most keyboards) cannot be executed while a computer is connected to a secure channel. Obviously a camera picture of the external screen can never truly be prevented nor can simply writing down information, yet there is always the possibility of office cameras that can be functioning or not. However, the real value is their presence is increased discouragement from such malicious activity.

Furthermore, beyond the fundamentals including limiting use to authorized personnel and adequate policy structuring insuring alignment and effectiveness, a vital concept of the physical safeguard is promoting reasonable judgment of equipment containing protected

[6] *Health Insurance Portability and Accountability Act*, ibid.

information. IT personnel do not enjoy being babysat day in and day out on the job. Eager and optimistic employees enjoy some level of freedom of portability and use of their intellect to interpret what is right and what is wrong (teachings proper ethics and instilling strong leadership is key). All too common, senior-level decision-makers develop an environment with austere working conditions and unacceptable pressures to comply with miniature demands. Contrary to what decision-makers deem will ensure protection of their systems and data storages, a vital piece of the puzzle is satisfying employees' needs and preventing a high internal employee turnaround rate. The real scary stories are the ones with disgruntled workers who abused system policies and regulations due to retaliation tactics. Many displeased employees completely become oblivious to their gestures hurting the holder of the protected information they expose more so than the managers they have grown to despise. In light of such employee psychology, it is important for mangers and policy makers to find the best fit line for safeguarding physical rules by HIPAA, yet not becoming oblivious to employees' human needs. The best managers and leaders can balance both and secretly behave differently to each employee based on his or her gut instinct on the employee's intentions and desired future state with the organization he or she works for. IT needs managers to instill stability in a hostile environment and complicated infrastructures. Yet, it is frivolous to overlook strong leadership to deal with concurring changes in organizational structure. Many companies are over-managed and under-led, thus the best approach can only be developed through experimentation and logical understanding of outputs and security credentials.

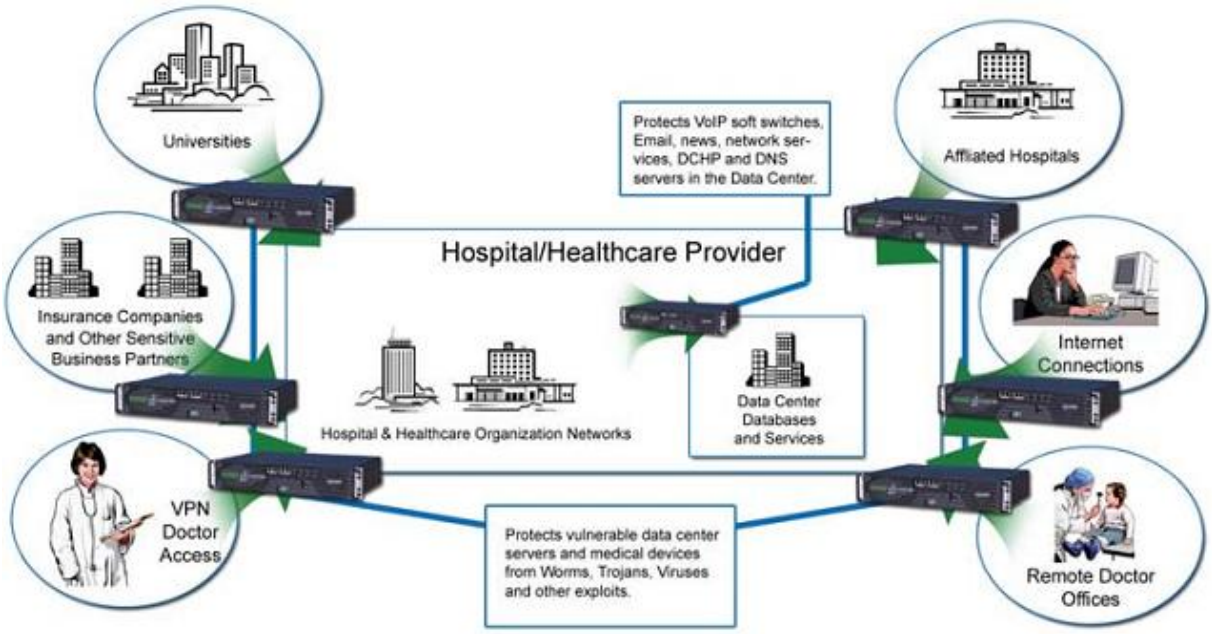
The final component embedded in HIPAA's Security Rule is implementation of technical safeguards.[7] This element deals primarily with ensuring that every technical component is fully operational to foster an electronic data interchange (EDI) that has only the intended recipient receiving the appropriate PHI. In essence, the technical safeguards attempt to establish a best practice approach to manifesting an environment of premier data integrity. This component can commonly be used by computer technology to foster the strongest data encryption for the given form of transmission. Speed of transfer is also of the essence in the medical world, thus layer upon layer of encryption can be irrational, yet the best approach can be established by proven experts in implementation and security. Without mincing words, "data corroboration, including the use of check sum, double-keying, message authentication, and digital signature may be used to ensure data integrity**.**"[8] A fully developed and interconnected medical network has many components that transfer data and information from different technologies. The graph (FIGURE 2) on the following page depicts a common overview of the various components that come into play when a network is live and operational. Data corroboration is a vital ingredient in such a maze because it supports a best-of-breed practice by implementing layers of data protection in a world that is ever so digitally weary and unpredictable. The figure shows the common use of a VPN (Virtual Private Network) for doctor access to sensitive information. This type of tunneling technology is a strongly accepted practice due to integration with virtually any network device (e.g. a PDA or palm pilot a doctor can heavily rely on).

---

[7] *Health Insurance Portability and Accountability Act*, ibid.

[8] *Health Insurance Portability and Accountability Act*, ibid.

FIGURE 2



Furthermore, VPN security offers three superior forms of cryptographic technologies (encryption, authentication & integrity, and key management) to ensure that an organization is implanting required elements to promote electronic protection.

A striking fundamental of the HIPAA Security Rule is that it does not demand a particular technological solution to be implemented as a safeguard.[9] This implies that security experts have a wide area of arsenals they can choose to implement based on applicability. This also potentially induces a saturated market of never ending applications and programs that do the same things. From this, it is possible that program diversification is present, yet patching and updating could create more difficulty for all administrators in the industry. Also, with a larger selection of programs and architectures to select from, potential hackers and malicious minds have a wider array of programs to fire vulnerability attacks against. Nonetheless, it is vital to

[9] Norma K.S. Kenigsberg, eta all, "A Framework for HIPAA IT Security Compliance: Leveraging for Security," *Educause* Volume 2004 Issue 25 (7 December 2004): 1-13.

ensure that regardless of the technology put into play, it needs avid resources maintaining a level of perfection and countless training to ensure every user and admin is on the same page.

In sum, the HIPAA Security Rule is by far the most extensive ruling in its connectivity to information technology. In order to foster a strong and secure e-healthcare environment, implementation requires an institutional plan that governs, defines, and depicts required commitments by all involved parties to ensure complimentary visions and end-goals. In the midst of a dynamic and ever-changing IT environment, it is critical to avoid complacency at all costs. Leaders need all eyes and ears open at all times to ensure the latest and greatest practice is used in their organization. A spoiled healthcare reputation from poor measures can forever tarnish a reputation inevitably causing bankruptcy or costly lawsuits. Thus, organizational IT leaders are increasingly shifting focus to risk analysis and risk management as a safety net for emergency situations. Risk analysis is a decisive component because it allows an entity to target its main security loopholes and deficiencies.[10] No security plan or structure is "bulletproof" or flawless; therefore, thinking outside the box for a potential worst-case scenario and implementing emergency tactics is a key ingredient for strong IT performance. System administrators need to have clear-cut pictures on how their ePHI is distributed in terms of storage and interconnectivity with significant parties who utilize and interpret this information along a Hospital/Healthcare Provider chain (FIGURE 2). Furthermore, risk management is crucial prior to full system utilization because it details potential uncertainty and related threats in a highly sensitive environment.

[10] Norma K.S. Kenigsberg, eta all, ibid.

All of these key components encompass a bible of must-dos for a highly successful healthcare organization involved heavily in ePHI management. With never ending metrics, statistics, and survey analysis, it is clear that everyone involved in healthcare transmissions is not fully equipped to battle the certainty along with the uncertainty. Therefore, in the constant battle against a known and unknown evil, leaders need to focus on the details revolving around IT applications and security safeguards; yet, overlooking the most basic component of a safe network should not be an option. Communication is singly handedly the most important factor in ensuring a safe and prosperous healthcare environment. However, not just any type of communication, quality communication and proper channeling through individuals in positions of power within the division of labor and availability to key resources will generate ample response times to potential environmental dangers. In a world where one attempts to get ahead of another at any and all costs, it is important to remain understanding of a fellow engineer, manager, or worker at another firm. If everyone keeps their secrets to themselves, industry professionals could consistently be reinventing the wheel and utilizing efforts individually instead of communally. Thus, it is imperative that healthcare professionals of all caliber, whether head doctor or chief system architect for a security network, promote communication of threats, uncertainties, and breakthroughs inducing a industry-wide power that can overcome uncertainty in a highly volatile and fierce IT and healthcare sector.

HIPAA: Final Thoughts About IT & Healthcare's Effect On Society

Another growing trend in information technology is the use of outsourcing data warehouse solutions to third-party entities. Under many manipulative fashions, these entities fail to fall under typical scrutiny from HIPAA. However, the administrative safeguards ensure that any entity involved in such outsourcing operations force its third-party partners to adhere to HIPAA compliant framework for security standards. As with any technological solution, the more boundaries information needs to cross, the higher the chances of confusion, manipulation, interception, corruption, and misuse.

Therefore, it is imperative that large players in the healthcare industry set their own internal standard code of ethics within their employees. Employers need to attempt to motivate their workforce to excel for intrinsic values of satisfaction. Working to better peoples' lives and help keep a sick child's information remain safe should in itself pay off. Before emotions get can get the better half of the writing, and by being an employee in the healthcare sector for a few years now, it is a sensational feeling knowing that the job done is done to help someone's life prosper, prevail, and remain secretive. Healthcare workers have lots of regulations to abide by, yet the most important safeguard of all, not documented in any HIPAA ruling, is an internal safeguard between oneself and the beauty of inspiring oneself to help make the world a better place. Anyone can make a decent living as any honest working professional, yet the golden nature of healthcare and healthcare IT operations is aspiring to keep a heart beat on and on bit by bit of computer code, reengineering, and relentless creativity to overcome the evil eye.

HIPAA: CASE STUDY – Q/A WITH A&E MEDICAL SUPPLY, INC.[11]

There is no better way to get a behind the scenes overview of HIPAA applicability and functionality in the real world than going straight to a flourishing Chicagoland HIPAA compliant DME (Durable Medical Equipment) provider. A&E Medical Supply, Inc was founded on a deeply rooted mindset to provide superior medical equipment for an unbeatable price. Founded by two longtime friends and guided by a successful father who had been in the field for decades, A&E Medical quickly became a prosperous provider who had built a clientele base due to strong commitment and understanding to patient's needs. I sat down with big brother, David Elkind (co-founder of A&E Medical), a University of Illinois at Urbana-Champaign graduate from Electrical and Computer Engineering in 2001, to discuss his managerial expertise in governing a strong HIPAA compliant culture within his organization. The following seven questions and answers proved very helpful in fortifying a complete understanding of HIPAA, IT, and healthcare.

Q1: After researching HIPAA extensively, I have noted that many extensions were given to HIPAA rulings due to confusions and difficultly in implementation. How have you and Leo (co-founder) managed to stay on top of all your regulatory needs and remain ahead of the game in compliance issues?

A1: The most important part of HIPAA deals with patient privacy. There are two sides of the equation relating to privacy. One side deals with patient privacy, while the latter deal with

[11] David Elkind, interview held during regular business hours of A&E Medical Supply, Chicago, Illinois, April 2008.

the company's way to protect the information. By understanding the HIPAA compliance, we have made it our goal to educate our patients on the HIPAA privacy rules. We provide an outline of the HIPAA requirements to all of our patients so that they can easily understand their rights as outlined by HIPAA. Then, once we have the HIPAA acceptance with patients we go to great length to protect their information. All files are locked when our staff is out of the office and the patient database is protected via stringent passwords and encryptions. In addition, we track when a patient record was looked at by an employee and require a written explanation as to the reason why the patient record was looked at. These measures let the managers of A&E Medical have detailed logs of all patient access activity.

Q2: How common is it for state and federal health insurance agencies such as Medicaid and Medicare to alter payment reimbursements causing potential changes in financial projections?

A2: It is not that common for the federal and state programs to affect payment flow if a company shows constant compliance. Our company was recently accredited by a federal accepted organization JCAHO that did an extensive policies and procedure compliance check which we passed.

Q3: What kind of information technology networks do you utilize to share information between equipment suppliers and medical professionals issuing medical necessities for your patients?

A3: For many years the industry standard was using analog telephones lines to transmit fax documents and to upload and download data from health insurance carries. In the recent years the healthcare world is catching up by implementing secure web portals where the exchange of HIPAA compliant can take place. A&E technical staff is currently administering these additions as we speak.

Q4: What growing trends are you witnessing in the healthcare industry that is potentially causing you to redefine your business objectives and projections for sustaining stability in a slumping American economy?

A4: The biggest trend that we are seeing is the push towards a paperless office. While there are still major hurdles in accomplishing this task, our company is laying down the groundwork to use this in the future. A paperless office will allow companies to save time by accessing files faster and drastically reduce the office expenses such as paper and toner when documents are send to and from healthcare organizations. Security is an overarching concern that must be addressed prior to a paperless implementation.

Q5: What organizational and technological techniques/policies do you utilize to prevent your employees from accessing more PHI than required?

A5: As mentioned in the earlier question, our management team gets daily reports of patient records that have been accessed throughout the day as well as detailed reports of all the active patients that our staff is currently working on. Each employee has a unique username and password that lets us track what patient records they are working on.

Q6: What forms of state or national training do you attend to ensure up to date knowledge and understanding of HIPAA applicability? Do you require any other employees to adhere to such training?

A6: The owners of the company and all members of our management team attend yearly HME Expos that provide classes on the changes in our industry. There we learn about changes in the HIPAA compliance, billing requirements, and changes in patient care. It is then the job of our managers to train our office personal on the new policies and make sure that they follow them to sustain strong compliance.

Q7: Lastly, you had mentioned that the majority of your information is still paper based; nonetheless, imagine the year is 2015 and A&E is still up and running successfully, is everything done electronically and a paper trail nonexistent?

A7: I certainly hope so. The documentation requirements are getting more complex every year and the best way to follow them is to simply change the files that the changes effect. In addition, digital storage is getting cheaper and cheaper, and that will allow companies to store and backup large volumes of data cost effectively. There are still a lot of hurdles that need to be overcome before the healthcare industry can completely move away from a paper signature of a doctor, but the technology is there. It will take a great amount of education in the healthcare field to go paperless, but I feel it can be done. As a former engineer and IT guy, I sure hope so as it will make my job significantly more intriguing.

HIPAA: CONCLUSION

In conclusion, HIPAA, The Health Insurance Portability and Accountability Act, is a forever changing regulation that has paved the way for increased patient protection and portability of health information in prospering healthcare and IT environment. The implications of HIPAA and its underlying rulings will forever shape the way healthcare is performed, analyzed, and evaluated in the United States. American society and business has forever been on the forefront of medicine and its fundamental disciplines. It is a blessing that contemporary information technology has been able to sculpt an environment to foster increased security, prosperity, and sustainability. Internet and "technology doctors" can proudly hang their hats at night knowing that they, too, have helped changed the lives of millions of Americans by influencing the nature of the healthcare industry in the past decade. Together, as a team of organized and highly communicated individuals, the American healthcare industry can proudly fight diseases both internally in human nature and externally by human malicious nature.

This document has discussed major factors in shaping a growing IT healthcare environment along with giving multiple perspectives on HIPAA applicability. Financial data has been predominantly absent for a large part of the document to remain focused on the true alliance between healthcare and IT strategic goals for supporting its growth and HIPAA compliance. Nonetheless, it is always worthwhile to leave on a strong note. Based on a Gartner study in 2004, it was predicted that healthcare industry spending will continue to grow

into 2007 by a significant 7% annually.[12] In retrospect, after analysis and research, it was indeed truthful that such predictors became a reality. It is very welcoming that speculation on hardware, software, and IT services spending actually became a realization for implementation. According to Healthcare IT News, healthcare providers were estimated to spend upwards to $40 billion on information technology in 2008.[13] Lastly, with all the go-green speculation in our society today, it is comforting to know that today's leaders are spending wisely to ensure the protection of the children of tomorrow. With every IT dollar spent on healthcare, someone somewhere in the U.S. got faster, more efficient and secure access to medical resources thanks to information technology.

[12] Michael W. Davis and Joanne Galimi, "North American Healthcare IT Spending Forecasts to 2007," *Gartner* Research (24 April 2004): 1-3.

[13] Bernie Monegain, *Report: Healthcare IT spending to grow to $39.5 billion by 2008*, http://www.healthcareitnews.com/story.cms?id=4242 (6 January 2006).