SCITECH
RESEARCH ORGANISATION

Volume 9, Issue 5
December 5, 2017

Journal of Research in Business, Economics and Management
www.scitecresearch.com

# U.S. Healthcare Industry: Cybersecurity Regulatory and Compliance Issues

Derek Mohammed
Saint Leo University, School of Business, Florida, 33544.

## Abstract

The health care industry is one of the most vital areas of critical infrastructure in the United States. In recent years, the healthcare industry has faced a barrage of cyberattacks that have disputed vital services and exposed vast amounts of sensitive data. Federal regulations such as HIPPA and the HITECH act were designed to protect this sensitive data, but often are left open for interpretation. For example, HIPPA mandates the protection of personal health information but gives little guidance on how to do it properly. Even with regulatory mandates, the health care industry continues to struggle with complying with current regulations. Various factors such as budgetary constraints and the lack of cybersecurity professionals who understand the security needs of the health care industry affect compliance. Also within the health care industry, there are various sectors which are all governed by different sets of rules and regulations. This can create a level of confusion when trying to create a standard for the industry as a whole. The goal of this paper is to evaluate the current regulatory and compliance landscape of the U.S. health care system.

**Keywords:** Cyberattacks; Healthcare; HIPPA; HITECH; Personal Health Information.

## 1. Introduction

The health care industry is one of the largest and most pivotal sectors in the United States today. According to a PricewaterhouseCoopers (PWC) report, the health care industry is valued at $5 trillion dollars (PWC, 2016). Everyone in the U.S. has been touched by the health care industry in some form or another. In the past few years, the U.S. has seen several large scale cyber-attacks on the health care industry. One of the largest attacks occurred in 2014 when health insurance provider Anthem BC/BS suffered from a cyberattack that exposed the Personal Health Information (PHI) of 80 million members. The breach exposed participant's social security numbers, names, and birth dates. What is concerning about these breaches is that the health care industry is a heavily federally regulated industry. The most common regulation which the American public is aware of is the Health Insurance Portability and Accountability Act of 1996 (HIPPA). The sole purpose of HIPPA is to protect the PHI of U.S. citizens. However, HIPPA and other federal regulations are not as ironclad as they may appear.

The healthcare industry continues to be a target for cyber-criminals. There have been drastic modifications within the industry. Due to revolutionary technology, and the pervasive Internet of Things (IoT), our society is becoming more digital than anything ever seen before. Companies and enterprises throughout the public and private sector have taken notice. In this digital age, compliance stands out as one of the most difficult and controversial issues within cyber-security and specifically the healthcare industry. The Healthcare industry administration and operations have been modernized. Instead of traditional handwritten consultations, revolutionary processes like computerized physician order entry (CPOE) systems, electronic health records (EHR) and various radiology, pharmacy and laboratory systems have emerged. Additionally, these processes can connect to other systems and external networks as well as the internet and the cloud.

With more devices being connected, and companies allowing their employees to operate these devices while at work, the result has been an uptick in cyber-attacks all across the globe. This creates an issue for healthcare

providers. Unfortunately, the miraculous interconnectivity offered by technology is a double-edged sword since it inevitably leads to increased security risks. Cyber-criminals can easily execute attacks resulting in data breaches and fraud via the internet and cloud which is easily accessible for everyone. The purpose of this paper is to evaluate the current compliance and regulatory landscape of the healthcare industry in regards to cybersecurity.

## 2. Healthcare Compliance Issues

In order to minimize the security risk, healthcare providers must ensure that their employees have been properly educated. Experiencing failure first hand allows one to fully grasp the problems that ignorance creates. But because there has been ample failure within this industry to learn from, there is no excuse for being ill-prepared. For example, in 2014 the hacktivist group Anonymous attacked the Boston's Children's Hospital. The attack caused a major disruption in hospital operations for several days. Most recently, the U.S. pharmaceutical giant Merck suffered from a malware attack. It is essential that we continue to grow and develop, keeping pace with the evolution of our technology. Unfortunately, this is not always the case. The Health Insurance Portability and Accountability Act (HIPAA) should be congruent with current technology, however, their regulations and protocols fall short at meeting the current state of technology.

Since its legislation in 1996, HIPAA hasn't undergone any major new iterations. The regulation centers more on what areas must be protected as opposed to specific methods to bolster security. There is an absence of guidance for concepts like firewalls and wireless networks because they weren't mainstream when the legislation came into effect. While HIPAA requires companies to implement security measures to protect their systems against any unauthorized access, it fails to elaborate on those measures. HIPAA's primary compliance concern is patient health information. The HIPAA rules have become outdated, and it is impossible to guard against threats that are ill-defined. This points to an even bigger problem within the industry. In order for an organization to properly protect their information systems, HIPAA rules and regulations must be amended.

A few similarities between the healthcare environment and the industry overall is the amount of money being spent to better protect critical infrastructures. In 2017, an HIMSS survey of the health care industry found that: 71% of organizations budget for cybersecurity; on average, the amount allocated for cybersecurity is just over 3% of their overall budget; organizations are spending more on cybersecurity than in past years; and budgets are used to hire more security professionals and to improve overall security (Conaty-Buck, 2017). These findings points to the fact that companies within the healthcare industry are beginning to realize that cybersecurity isn't just an IT problem, it's a business problem. Regrettably in healthcare, security has predominantly been a HIPAA compliance issue. The intent was to ostensibly satisfy the Security Rule and Privacy Rule. When asking enterprise employees about the top priority for security, the answer was resoundingly one aspect: risk assessments (Snell, 2017). In the past, CEOs and executive members took more of a hands-off approach towards cybersecurity, now these issues are in the forefront, which shows a change in philosophy. Businesses are acutely aware that a cyber-attack can destroy their bottom line, and have begun to take an active role in their prevention.

Another similarity within the industry is the alternative framework being adopted by healthcare providers. The National Institute of Standards and Technology (NIST) has developed a framework that compliments HIPAA. In the areas where HIPAA falls short, NIST picks up the slack. Since HIPAA is not aimed at helping organizations keep their entire enterprise secure, NIST has introduced the PROTECT function. This process examines an organization and determines how it should protect patient information. Furthermore, the PROTECT function includes cybersecurity education and awareness for its employees which ensures that administrators know their larger roles in cybersecurity protection (Whitman & Mattord, 2016). With an emphasis on training, the NIST cybersecurity framework involves employees in the overall protection of data. NIST is a framework that highlights that data protection of an enterprise comprises people and technology at all levels.

The healthcare industry must address the issue of cyber-security on a united front. Financial issues should have no effect on the progression of future cyber-security advances. Because patient information is shared amongst healthcare providers due to third-party business relationships, hence, it is just as important to protect the small business as it is the big business. If these issues are truly important to everyone, competition should not impede the progress of cybersecurity. Only through cooperation can any headway be made.

## 3. Healthcare Compliance Challenges

The healthcare industry faces several compliance issues when conforming to Healthcare Cybersecurity regulations. The healthcare industry is entrusted with sensitive customer data, but fails to use tools and programs ensure that information is protected. They employ personnel who primarily are trained to focus on cybersecurity. They also require sensitive data to be shared across different systems to ensure patient safety, while simultaneously ensuring it is kept secure and unmodified.

The first difference in healthcare compliance environments is based on the divergent requirements for various subsets within that industry. These subsets in healthcare range from pharmacies and hospitals to medical device companies, with each industry having its own compliance issues. For instance, a medical device company may need patient data for the use and operation of a medical device, but has no need to maintain this information. The system needs to be designed in a way that allows for safe and effective removal of this information. There is a "vast array of special-purpose computers for medical devices, many of which have the potential to put patients at risk" (Andre, 2017). Also in the medical device field, there are a multitude of personal medical devices, such as glucose monitors and heart monitors, which collect a large amount of data about a person. These devices are often designed to work with low power Bluetooth connections, and connect to apps on smartphones. This can provide a pathway into a device through a trusted port, which can then be exploited to gain access to other parts of the system. In order to ensure that the system complies with privacy requirements, the medical device manufacturers should ensure that their devices are not exploitable.

The next difference in healthcare compliance environments is in regards to pharmacies. Pharmacies differ from hospitals and doctors' offices in the information they maintain because they track which prescriptions have been filled at any given time. They need to ensure that their databases are secure, complete and unmodified, and that employees are trained correctly in patient privacy. Because a lot can be learned from a list of prescribed medications, pharmacies need to safeguard against the accidental disclosure of medical treatments. Someone other than the actual patient is often able to pick up prescriptions, and pharmacies need to ensure privacy by verifying that the person picking up the medication is authorized to do so. If they fail to do this, controlled substances can be dispensed to those without a prescription, or medication can be dispensed to unauthorized people, exposing the diagnosis of individual patients. This could lead to a large privacy violation through the exposure of a patient's medical diagnosis with a chronic or acute condition.

Doctors' offices have their own concerns when it comes to cybersecurity compliance. Doctors' offices are often smaller businesses that may not have the budget to properly fund cybersecurity, potentially exposing patient information to compromise. As more companies are moving towards electronic health records, the cybersecurity costs continue to increase. This means that smaller practices need to find solutions to address the cybersecurity of their networks. Also, smaller practices that do not have a dedicated IT person may also "have software on their system or hardware attached to their network that is no longer needed" (Lanz, 2016). The office needs to periodically review the installed software and hardware, and remove obsolete and unneeded resources that are no longer receiving updates, which are a vulnerability that would allow attacks to succeed against a network. Medical records have vast amounts of personally identifiable information, and present an enticing target for cyber attackers. Smaller practices often do not have the budget to purchase appropriate custom security, so to ensure HIPAA compliance, they need to implement a quality off the shelf solution and train their employees in best practices. Because there are no recurring costs, using best practices is a cost-effective way to address compliance since the only cost is the time to train the employees.

Larger practices with several doctors have a different set of concerns than smaller practices. Larger offices with many different doctors tend to have a system that is more advanced, and shares more information throughout the practice. Since a "growing number of medical devices are connected to networks through wired or wireless connections" (Chaudhary & Hamilton, 2016), strong security needs to be set up to protect the network. There are many doctors working in the same office, often with the take home devices and other portable devices; these practices must implement other types of security to address compliance. They need to ensure that all devices being used are up to date against vulnerabilities, especially those that can be compromised when being used on outside networks. The practices also need to verify that the system is hosted in a secure location and is encrypted correctly. This is especially important for practices that have multiple offices in geographically dispersed areas, leading to the need for data to be accessed over the open Internet. Lastly, a larger practice needs to check that they have the appropriate access levels set up to defend the networks against users accessing unauthorized information, thereby potentially lowering the access possibilities for attackers.

Another area of the healthcare field that has a unique concern when it comes to cybersecurity compliance is the hospitals and medical centers themselves. Many hospitals and medical centers allow other doctors to use their facilities for surgeries, tests, and other such needs that are too expensive for a traditional doctors' office. Because of this, these large centers are required to protect patient data, while allowing varied users to access the network. Often, these users are not employees of the center, but need full access to the data collected by the center about the patient, or need access to the tools and devices that are present in the center. These large centers need to ensure that they can effectively provide the required access to these doctors, while simultaneously protecting the network and patient data from compromise due to the large number of varied users in varied roles, which rarely use the center's network. It "is easy for organizations to lose track of all the contractors that have elevated, remote or physical access rights" (Douglas, 2015). Medical centers need to periodically review the access of various users and address inactive users, users that no longer need a certain level access, and any other concerns that arise.

### Insurance Industry

Insurance companies also have unique concerns when it comes to compliance with cybersecurity regulations. Insurance companies are a great target for cybercrime because they often have the most complete and comprehensive digital data about a patient. If a patient goes to a primary care doctor that is not using electronic medical records, the only digital record of the patient's medical information is with the insurance companies. The insurance companies are often the only place where data on all prescriptions, health diagnoses, and other medical data is stored, since it is all coded and submitted to the insurance companies for payment of services. The insurance companies also keep employment data, personally identifiable data, and a range of other information about customers. They also have many more patients on file than any medical center or doctors' office would have. The vast amount of comprehensive data makes it imperative that insurance companies maintain the highest levels of data security and encryption to ensure that data is kept secure. While insurance companies are less likely to need to provide access to many different users with varying amounts of connection to the actual company, the sheer size of the data available makes them a large target for cyberattacks, and the company needs to defend against these attacks.

The last field of healthcare that has unique concerns when it comes to patient privacy and cybersecurity compliance is research entities of various types, be they public or private. When research is being done for either new treatments or effectiveness of existing treatments, research agencies collect data different from that which other healthcare industries will collect. Studies will collect data such as lifestyle information, medications being taken, and day to day results. This can provide an extremely useful view into the life of the patients of the study, and is critical to the success of the study. However, many research agencies are a part of a larger company that may not effectively protect the data collected by the study, since the study may be the only study of its type being conducted at the time. This could mean that the level of security is not adequate for the protection of the patients' privacy.

Research entities also need to verify confidentiality, due to the eventual presentation of research findings in a public forum, since providing too much data about an anonymous participant can compromise their privacy. As data is collected, it needs to be protected, but still easily used. The research entity needs to confirm "that data provisioned to researchers remain secure, yet easy to use" (Shoffner et al., 2013). The research entity needs to have a process in place to certify that any data that is inadvertently identifiable is not produced for public consumption, either through direct identification or identifiers that are so unique that they can be used to identify the participant, compromising their privacy.

## 4. Cyber Security Regulatory Issues in the U.S. Health Sector

The primary regulation that has governed the privacy and security within the health sector is the Health Insurance Portability and Accountability Act of 1996 (HIPAA). This law protects the personal health information (PHI) from being released to other entities unless authorized by the patient. HIPAA fortified the notion of patient confidentiality, as well as established requirements, for medical facilities and personnel to ensure information is protected, to include electronic health records (EHRs), in light of the digital evolution (Rechtman & Rashbaum, 2015). In addition to regulating EHRs, it is worth mentioning that many rural areas still prefer to use paper records due to cost and time of transferring PHI to electronic data and securing that data. Unfortunately, HIPAA only requires that health sector entities protect PHI, but is vague about to what extent those institutions must secure that information. Therefore, over the last twenty years, confusion and complacency has exacerbated the issue of cybersecurity since few institutions have properly implemented or coordinated a cybersecurity program. Even though it is true that securing information by relying on medical personnel on an individual level has been relatively successful, the larger threat involved external attackers that used a variety of means to infiltrate health systems and networks. When these attacks occur, the spotlight is not on medical personnel, but rather on IT employees or programs. Therefore, the lack of communication between IT and medical staff, in conjunction with lack of overall investments in the cybersecurity/information assurance, along with the ambiguous nature of HIPAA, contributes to magnetizing the industry to hackers.

Another regulatory framework that later became crucial to cybersecurity within the health sector is the National Institute of Standards and Technology (NIST). Originally created for federal government agencies and military, the standardization has grown to be adopted by many private sector organizations and small medical businesses as well. The health sector is unique in that it falls under both public and private sectors depending on the practice and location. The primary focus, similar to HIPAA, revolves around securing EHRs, whether in a storage state or during transmissions. Some guidelines include encryption requirements, Privacy Act/HIPAA statements, and digital signatures. Meaningful Use (MU) and usability, while addressed in HIPAA, become more prevalent within the NIST framework and become the foundation for providing regulations not only for PHI on EHRs, but includes medical devices (Cohen, 2016). Vendors involved in developing programs and medical devices alike begin to play a vital role in determining the procedures for MU of both EHRs and medical devices, but confusion still exists about what standards to follow. Vendors don't believe there are standards for health IT. They are borrowing

standards from other domains, developing their own, trying to respond to users and to requirements such as the Certification Commission for Healthcare Information Technology (CCHIT) testing. Which can all lead to confusion among vendors.

In anticipation of nationwide adoption of EHRs, the Health Information Technology for Economic and Clinical Health Act (HITECH) was established which offers incentives for using EHRs. The law became pivotal in finally considering the negative effects of ambiguous regulations, and took the first major step in specifying situations that warrant increased security and provides details on how to secure those systems and documents. Additionally, HITECH addresses the lax enforcement standards by holding parties accountable for security breaches due to "willful neglect". For a provider who wants to gain the benefit of incentives, and moreover avoid any subsequent penalties, increasing their literacy regarding HIPAA's Privacy and Security Rules and the new provisions of the Act is the best option. After HITECH was created, a private company, the Health Information Trust Alliance (HITRUST) was established and developed a Common Security Framework (CSF) certification process for health sector agencies to utilize. Furthermore, the Health Care Industry Cybersecurity Task Force founded by Congress (authorized by the Cybersecurity Act of 2015) produces an annual report that reveals all vulnerabilities and works with HITRUST to make recommendations for cybersecurity framework and policy changes aimed at improvement.

The largest contention currently about regulation information and technology in the medical field is between the U.S. Food and Drug Administration (FDA) and the U.S. Federal Trade Commission (FTC). With the advent of mobile health devices (mHealth) and wireless technology, not only are peoples' medical information a concern, but the medical devices used for treatment are also subject to cyberattacks. Essentially the challenge is striking a balance between ensuring that medical devices function properly and healthfully while still respecting the privacy of the patient. Medical technology ranges from devices that store a patient's entire medical history to wirelessly keeping vital organs functioning. This double-edged sword of technology is a blessing and a burden. On one hand, the convenience afforded to patients alleviates time spent in hospitals and prolongs life. On the other, however, the surface area of attack has expanded and now reaches the realm of affecting human life. For example, wireless pacemakers allow doctors and patients to monitor heart rate and anomalies via the internet meanwhile making the device's functionalities vulnerable to hacking.

Despite some minor bureaucratic clashes between the FDA and the FTC over who is responsible for this type of technology, both agencies are collaborating on efforts for regulatory awareness. The most recent effort is through an online tool that allows an individual to input information pertaining to the potential new application which in turn provides the corresponding law for that application. In addition to collaboration, it is worth mentioning that the FTC, HIPAA, and HITECH all have stipulations regarding notifying individuals in the event their PHI is compromised as a result of a security breach by the medical facility or office to include EHRs. Therefore, using unsecure mHealth devices will damage the trust between patients and doctors, in addition to having negative economic ramifications.

Essentially, the concept of cybersecurity regulation as a necessity in the health industry is becoming a reality. The main problem with regulating EHRs has been addressing offices and organizations that do not utilize EHRs. To promote use of EHRs U.S. government has attempted to incentivize its implementation through the HITECH Act. While regulations in general could benefit from being more specific, ultimately the burden lies with the medical entities to hire and/or appoint qualified personnel to lead their cybersecurity departments. The divide between IT and medical staff should be dissolved so that everyone understands the current regulations, and internalizes the importance of practicing handling PHI safely and securely. Whether the health organization chooses NIST or the CSF via HITRUST, or another approved framework, the burden falls on the individual organization to ensure compliance in order for the regulation to be truly effective. For example, "while federal regulation calls for designated privacy and information security officers in covered entities, this has been done neither universally nor effectively across the health care industry" (Schulke, 2017). So the enforcement of complying with existing regulations is a worrisome concern for the actors in the health industry.

## 5. Conclusion

The current evolution of technology has been both a boon and a bane to the health care industry. While technology has made the health care industry more efficient, it also has made it more vulnerable to cyberattacks. One of the major issues the healthcare industry faces is the ability to stay in compliance with federal regulations. It is not the intent of sectors in the healthcare industry to avoid compliance but due various factors, noncompliance can be common practice. These factors include: lack of tools and programs to protect sensitive information; different sets of standards on how data is protected in the different health care sectors; and budgetary issues. These are just some of the daily battles that the health care industry must deal with on a continuous basis. Staying in compliance with healthcare regulations will continue to be an uphill battle but the problem may be rooted in the regulations themselves.

Regulations such as HIPPA mandate the safeguarding of PHI, but give minimal instruction on how to properly secure it. However, there has been progress in creating a more standardized environment with the creation of the HITECH act and the HITRUST committee. Both have been used to incentivize and give guidance on the cybersecurity framework and policy produced for the healthcare industry. The federal government is striving to strengthen the cybersecurity stance of the healthcare industry. Increasing or creating regulations may seem like the solution to the problem. However, in order to succeed, a new and experienced generation of IT professionals that understand the importance of cybersecurity and the priorities of the health care industry must be embraced by the health industry.

## References

[1] Andre, T. (2017). Cybersecurity: An Enterprise Risk Issue. Healthcare Financial Management, 71(2), 1-6.

[2] Chaudhary, R., & Hamilton, J. (2016). Internal Audit's Critical Role in Cybersecurity. New Perspectives on Healthcare Risk Management, Control & Governance, 35(2), 20-29.

[3] Cohen, M. F. (2016). Impact of the HITECH financial incentives on EHR adoption in small, physician-owned practices. International Journal of Medical Informatics, 94, 143-154.

[4] Conaty-Buck, S. (2017). Cybersecurity and healthcare records. American Nurse Today, 12(9), 62.

[5] Douglas, P. C. (2015). Cyber Risk Management: Do You Know Your Threat Sources? Add more precision to your security framework. New Perspectives on Healthcare Risk Management, Control & Governance, 34(3), 27-29.

[6] Lanz, J. (2016). Bolster your data defenses. Journal of Accountancy, 222(2), 22-24.

[7] PWC. (2016). Surviving seismic change: Winning a piece of the $5 trillion US health ecosystem. Retrieve from: https://www.pwc.com/us/en/health-industries/health-research-institute/publications/pdf/pwc-hri-health-industry-changes.pdf.

[8] Rechtman, Y., & Rashbaum, K. (2015). HIPAA Security Rule - Demystified. CPA Journal, 85(4), 68-70.

[9] Schulke, D. F. (2013). The regulatory arms race: Mobile-health applications and agency posturing. Boston University Law Review, 93(5), 1699-1752.

[10] Shoffner, M., Owen, P., Mostafa, J., Lamm, B., Wang, X., Schmitt, C. P., & Ahalt, S. C. (2013). The Secure Medical Research Workspace: An IT Infrastructure to Enable Secure Research on Clinical Data. CTS Journal , 6(3), 222-225.

[11] Whitman, M. E., & Mattord, H. J. (2016). Management of Information Security. Boston, MA.