International Journal of Business and Social Research
Volume 05, Issue 02, 2015

Cybersecurity Challenges and Compliance Issues within the U.S. Healthcare Sector

Derek Mohammed[1] Ronda Mariani[2], Shereeza Mohammed[3]

ABSTRACT

Increasingly there are security breaches in U.S. Healthcare organizations that result in billions of dollars of damage to the healthcare system and a high personal cost to individuals whose identifiable and private information is unprotected. The Privacy Act of 1974, Health Insurance Portability and Accountability Act (HIPAA), and Health Information Technology for Economic and Clinical Health Act (HITECH) are three prominent Acts by the federal government that regulate and protect the confidentiality of personal information in the Healthcare system against breaches. This is a case study examining three organizations in the Healthcare Sector using document analysis to ascertain the problems that resulted in information breaches and the consequences of such breaches. It indicates the failures that occur with the inadequate compliance to the above federal Acts and provides recommendations to control future breaches from occurring. The organizations examined are: The Veterans Administration which lacked basic security controls, the Utah Department of Technology Service that failed to control their personally identifiable information, and private healthcare organizations which revealed shortcomings in HIPAA compliance after data breach disclosures or random audits. Each case results from a lack of proper protection on systems and equipment containing sensitive data. The study recommendations include the need for organizations to lead by example as well as the establishment of tighter regulations and enforcement measures relating to civil fines, and audits to review organizational compliance with federal laws.

Keywords: Cybersecurity policy, healthcare sector, HIPAA, HITECH, regulatory compliance.
JEL Classification: M1, M2, M4.
Available Online: 20th Feb, 2015.
MIR Centre for Socio-Economic Research, USA.

1.0 INTRODUCTION

Technological progress and global interconnectivity has increased at a rapid pace in the last few decades. While there are numerous benefits to be derived from this proliferation of information technology, there are disastrous consequences in terms of "advanced persistent threats, DDoS (Distributed Denial of

[1] Saint Leo University, USA. Email: derekmohammed@yahoo.com
[2] Saint Leo University, USA. Email: ronda.mariani@saintleo.edu
[3] Grand Canyon University, USA. Email: shereezam@yahoo.com

Service) attacks, malware infections, cyber espionage, and data and intellectual property theft" (Filkins, 2014). According to Filkins' *SANS Health Care Cyberthreat Report* to diminish such threats requires billions annually. Additionally, the healthcare industry is particularly vulnerable to the damages that occur with the illegal use of personal and confidential information. The invasion of personal privacy occurs on a systematic basis by hackers who then sell the stolen identities on the black-market. In fact, about 90 percent of health institutions experienced a cyber-attack between since 2012 according to the Ponemon Institute (2015). These attacks were directed on medical records, billing and insurance data repositories and this trend will only increase as more health records are digitized.

As with banks and other businesses virtually all modern services in healthcare require individuals to surrender personal information in order to receive services. By surrendering personal information to outside entities, individuals lose control over the confidentiality of their data, and must rely on the organization to ensure its security. Such reliance creates significant potential for personal data breaches, if the trusted organization does not impose adequate security measures adequate to protect customer data. This problem led to the creation of federal regulations that work to protect the privacy of individuals by mandating security restrictions for organizations that hold personal information.

To examine the problem and consequences resulting from such breaches this study examines three organizations in the Healthcare Sector using document analysis. The question driving this study was to investigate the system inadequacies that caused information data breaches and to propose future preventative steps. The findings of this study indicates the failures that occur with the inadequate compliance to the federal Acts and provides recommendations to control future breaches from occurring. The organizations examined are: The Veterans Administration which lacked basic security controls, the Utah Department of Technology Service that failed to control their personally identifiable information, and private healthcare organizations which revealed shortcomings in HIPAA compliance after data breach disclosures or random audits. Each case is as a result of improper protection on systems and equipment containing sensitive data. The problems faced during each of these incidents were exasperated by the slow actions of the organizations that failed to resolve the errors in a timely manner. The delays caused damages resulting in millions of monetary losses.

The policy implications the arise out of this study include the tightening of regulations and enforcement measures relating to civil fines, and audits to review organizational compliance with federal laws. The study begins by addressing the regulatory and compliance environment, a comparative discussion of the three cases and their compliance environments and concludes with recommendations and best practices.

2.0 HEALTHCARE SECTOR REGULATORY COMPLIANCE ENVIRONMENT

The Privacy Act of 1974 was the first major U.S. legislation to address how personal information is handled by third party organizations. Intended to place restrictions on how the federal government could use personal information and give citizens more control, the Privacy Act established personal information handling standards for the federal government and granted citizens the power to petition, view or amend their government stored data. The act also created criminal penalties for those who willfully disclose personal information (Judy, David, Hayes, Ritter, & Rotenberg, 2009). The healthcare sector is an excellent example of a third party organization, which by necessity must hold the personal information of others. As the providers of a vital service in the form of medical care, healthcare organizations need to have patients' personal information on hand and readily accessible in order to provide optimal and effective medical attention. Since this situation creates significant potential for a patients' personal information to become exposed, healthcare organizations must take steps to keep data secure in order to protect the privacy of their patients.

Many healthcare institutions are not proactive when it comes to implementing precautionary security measures, and putting effective privacy safeguards in place. This has been an ongoing and costly

challenge running into the billions of dollars in damages. Proactivity involves cybersecurity strategies to keep pace with cybercriminal attempts to infect systems with malware, steal data such as protected health information and intellectual property as well as conduct espionage. The federal government has addressed these issues in the form of the Health Insurance Portability and Accountability Act (HIPAA), and subsequently the Health Information Technology for Economic and Clinical Health Act (HITECH) (Anderson, 2012).

2.01 BACKGROUND ON HIPAA, HITECH, AND THE PRIVACY ACT OF 1974

HIPAA was the first piece of U.S. legislation to address patient privacy within healthcare sector organizations, creating a number of requirements engineered to prevent willful or accidental disclosure of Personal Health Information (PHI). The requirements created by the law affected select healthcare organizations, which it deemed "covered entities," that held or transmitted PHI. Notably, HIPAA forces covered entities to disclose to their patients how they store and use PHI, and create extensive restrictions for how they handle PHI in digital formats also known as electronic protected health information (ePHI) (Judy et al., 2009).

The HIPAA provisions affecting ePHI mandate that covered entities limit access, both physical and electronic, to PHI in order to maintain the confidentiality, integrity, and accessibility of the data. Additionally, the provisions require healthcare organizations to implement risk analysis and management programs, audit trails for data access, integrity controls, and secure transmission technologies for systems handling PHI. Covered entities are also required under HIPAA to address any security breaches or violations within their organization that threaten the security of PHI. Non-compliance with any of these requirements can render an organization to civil and or criminal penalties which are enforced by the Office of Civil Rights within the department of Health and Human Services (HHS OCR) (Brady, 2011).

While the objective behind the creation of HIPAA was admirable, a number of issues with the law prevented it from being an effective solution the problem of PHI insecurity. Perhaps most importantly, the description of covered entities under HIPAA only included select types of healthcare organizations, entirely omitting some healthcare related businesses that interact with PHI from the security requirements. HIPAA also failed to define several important concepts, such as a "breach", making it much easier for violators to evade penalties in court. Additionally, the penalties imposed on violators by HIPAA were both relatively weak compared to the amount of damage that could be caused by a breach, and poorly enforced by the HHS OCR (Anderson, 2012). These issues eventually resulted in an amendment to HIPAA in the form of the Health Information Technology for Economic and Clinical Health (HITECH) Act.

The HITECH Act was passed as title XIII of the American Recovery and Reinvestment Act (ARRA), modifying HIPAA requirements to increase criminal and civil penalties for violators, and promoting more effective enforcement (Civic Impulse, 2009). Under HITECH, the privacy and security requirements of HIPAA now apply to any organizations handling PHI, greatly expanding on the definition of covered entities under HIPAA. The new disclosure requirements outlined by the HITECH Act are probably the most revolutionary provision. Covered entities are now required to disclose any PHI breaches to affected individuals within 60 days of the event. They must also disclose the breach details to local news organizations if the number of affected individuals exceeds 500. HITECH also requires covered entities to submit a report of all security breach events involving PHI to the Department of Health and Human Services annually (Civic Impulse, 2009). Additionally, HITECH dramatically increased the value of criminal and civil penalties for violations of HIPAA, and added the missing definitions that weakened enforcement of the original law (Anderson, 2012).

3.0 COMPARATIVE CASE STUDIES

3.01 CASE STUDY #1: U.S. VETERANS ADMINISTRATION

The United States has one of the most comprehensive systems in the world for providing benefits to its veterans. First officially authorized by the Federal government in 1811, the Veterans Administration includes medical care and pensions for veterans, their widows and dependents. The current Veterans Administration (VA) was established in 1930 by an act of Congress and it has grown to provide medical care, pensions, home loan guarantees, and educational benefits among others. As a medical provider, the VA has to follow HIPAA rules of privacy and computer security but there is a long record by the VA of not adhering to those rules. The VA operates and manages the largest integrated healthcare system in the United States. The administration encompasses more than 1700 hospitals, clinics, community living centers, domiciliary facilities (assisted care), readjustment counseling centers, and facilities. These facilities are located in all 50 states, and U.S. territories. Support for all facilities and millions of users require adequate amounts of organization and resources (U.S. Department of Veterans Affairs, 2014). Those resources involve the use of computers for management of services and tracking of veterans' status and care. Due to its size and complexity, the VA has a history of accusations of substandard care and computer system breaches.

A notable breach of the VA occurred when a VA employee's Maryland home was burglarized and a laptop containing the information of over 26.5 million veterans and their families was stolen. This incident was a wakeup call to the VA that they had a computer security problem. This prompted hearings in Congress since it was the largest government security breach in history (Goldfarb & Lee, 2006). The incident occurred on May 3, 2006 yet individuals were not notified by the agency of the compromised data until May 22, 2006 (Keizer, 2006). Questions revolved around the authorization of the employee to remove the laptop and its data from the VA's compound and take it home. The laptop was recovered intact and it was later determined that no data was accessed. Congress was mandated to pay more than $160 million to provide free credit monitoring for military personnel and veterans. The VA allocated $25 million to create and staff a hotline for those affected and to mail out notices about the theft (Goldfarb & Lee, 2006).

According to the U.S. Government Accounting Office (GAO) in 2013, for the twelfth consecutive year, the VA's independent auditor again reported that insufficient system controls still existed within certain financial systems, representing a major vulnerability. In addition, in 2013, the VA Office of the Inspector General concluded that the implementation of an effective information security program and system security controls continued to pose a significant challenge for the VA's leadership. While the VA made some progress on improving certain cybersecurity issues, it continued to experience repeated deficiencies in the same areas of access controls, contingency planning, and configuration controls (GAO, 2014). According to Healthcare IT News, the VA is still seen as one of the largest non-complying offenders of HIPAA regulations concerning privacy and computer security breaches (McCann, 2014).

VA's failure to introduce security control standards for its servers and network devices resulted in significant vulnerabilities manifesting in its configuration and access management controls. The VA has not effectively implemented procedures to identify and remediate system security vulnerabilities on network devices, database and server platforms, and Web applications. Approximately 6,000 outstanding system security risks have yet to be remediated in the VA's plans of action and milestones. In the consolidated financial statement audit for Fiscal Year 2013, Clifton Larson Allen LLP concluded that a material weakness had still not been eradicated from VA's information security program (Micro, 2013).

3.02 CASE STUDY #2: UTAH DEPARTMENT OF TECHNOLOGY SERVICES

On March 10, 2012, hackers believed to have been operating out of Eastern Europe successfully bypassed the login and password authentication security of one of Utah Department of Technology Services (UDTS) online servers (Schultz, 2012). The breach was due in part to a technician failing to change the factory-set default password. On March 30th, after having gained access to the computer server storing Medicaid and Children's Health Insurance Plans (CHIP) claims data for 20 days, the cyber criminals began

removing unencrypted PII. UTDS detected the breach 3 days later on April 2nd and immediately shut down the server (Vijayan, 2012).

A contractor that supplied software lacking encryption safeguards was later fired. Approximately 780,000 individuals may have been affected, with roughly 280,000 of those individuals having their Social Security numbers (SSNs) and other Personally Identifiable Information (PII) potentially stolen (Booz Allen Hamilton, 2013). Out of the top ten largest data breaches reported to the Department of Health and Human Services since 2009, this breach ranked ninth, however, it is the only breach directly attributed to external hackers (Schultz, 2012).

The specific types of information compromised included: SSNs, names, dates of birth, addresses, diagnosis codes, medical billing codes, national provider identification numbers, and provider taxpayer identification numbers. Types of information not compromised and not stored on this server consisted of personal financial information like bank account numbers and credit card numbers. Affected individuals or supposedly affected individuals were advised to call the appointed Ombudsman for the state of Utah's Data Security, Sheila Walsh-McDonald. This Ombudsman's position, office phone number, and e-mail address were created exclusively to serve those affected by this cyber incident (Vijayan, 2012).

Among the UDTS responses that were taken, letters were sent to all known customers informing them of the incident, and what to do to begin a one free year of credit monitoring with Experian. Due to an oversight, many people that had received this first letter later received a second letter stating that their SSN had not been stolen (Vijayan, 2012). This was a mistake blamed on SSNs being stored in two unique locations on the same breached server. This created additional confusion for many involved. Free credit monitoring was eventually extended for a second year by the state of Utah.

The Utah's Department of Health announced, approximately four months after the breach was noticed, that it would be holding workshop-style outreach meetings in late July 2012. The Governor of Utah called for the resignation of the Director of the Department of Technology Services, Stephen Fletcher. Internal reviews of data security policies and analysis of all state servers were conducted to mitigate further breaches. The independent consulting firm, Deloitte, conducted forensic analysis of this breach and performed a security control and technical vulnerability assessment of all 22 cabinet level agencies. This assessment used an 18-point framework following the NIST 800 standards for security assessments. Hogan Lovells analyzed the state's initial response to affected individuals, as well as later communications and the outreach initiatives for HIPAA compliance (Webb, 2013).

In the 18 months following the breach, Stephen Fletcher successor, Mark VanOrden identified breakdowns in procedures, human error, and the storage of unencrypted data. VanOrden described the threat landscape as sophisticated and asserted, "We block, on average, 50 million potentially malicious attacks a day through our firewalls in our data center" (Webb, 2013). He reorganized the entire IT security group, requested additional funding for cyber security from the State Legislature, and implemented 24/7 continuous network monitoring. A formalized change-management process was put in place to ensure better configuration compliance with any software and hardware alterations. Risk assessments for all agencies were completed and vulnerabilities were then categorized as high, medium, or low, with swift action taken for the most significant risks. According to a study conducted by the firm Javelin Strategy & Research, the total cost of this particular cyber security incident was estimated to be as high as $406 million. Out of this the Utah taxpayers would likely fund just 25% of the total. The remainder is expected to become the burden of banks and retailers (Stewart, 2013).

The statistical trend for the ratio of data breaches that correspond to or result in fraud is approximately one case of fraud for every four breach victims. Based on this benchmark, it can be assumed that nearly 122,000 people will become victims of identity theft-based fraud. Such victims will spend almost 20 hours and $800 to clear their name or to resolve the identity based conflicts that will occur (Study: Utah health breach, 2013). According to Robert Gregg, CEO of cyber security firm ID Experts, "a financial identity can

be worth $5 to $10 if you have all the info. However, a medical identity can be five to ten times that amount because it is easy to monetize that information" (Paganini, 2014).

3.03 CASE STUDY #3: EPHI SECURITY BREACH AT PRIVATE HEALTHCARE ORGANIZATIONS

Compulsory compliance to prescriptive security frameworks such as FISMA facilitates the rigorous and exhaustive implementation of HIPAA Security Rules at government hospitals. Case in point, except for "data privacy provisions", FISMA addresses all of HIPAA's security requirements (Gikas, 2010). Although adoption of a security framework will not necessarily preclude ePHI breaches, it ensures that the organization has sound and vetted security measures in place. On the other hand, implementation of Security Rule standards is left entirely at the discretion of private sector hospitals. With the "due care" stipulation of the Security Rule, hospitals are responsible for assessing their security risks and enforcing the appropriate policies and measures. Mechanisms to validate that every hospital enforces adequate cyber security controls to meet the Security Rule have yet to be established.

Currently, HIPAA compliance deficiencies at private sector hospitals only seem to be publicly exposed on two occasions, after data breach disclosures and during HHS' random audits. Investigations conducted in the aftermath of data breaches inevitably reveal shortcomings in HIPAA compliance. As a result, the HHS intends to expand its random audit program to uncover more security deficiencies in the healthcare industry. The following two cases, Community and Advocate health systems, demonstrate how inadequacies in security controls at private hospitals are revealed only after ePHI has been compromised.

Experts have pointed out that numerous factors have contributed to the current largest data breach in the private healthcare sector that comprised of 4.5 million records that were accessed at the Community Health Systems (CHS). However, many agree that the breach could be largely attributed to CHS' failure to address the known vulnerability of the Heartbleed bug to mitigate attacks that the bug exploited (Peters, 2014). According to Mandiant, the cyber-forensic company tasked to investigate the breach, the attack at CHS likely took place between April and June of 2014 (Ragan, 2014). This account implies that the attack likely occurred after the Heartbleed bug was already officially announced. Although the Security Rule does not explicitly require a patch management policy, the rule specifies that systems must be protected from malicious software designed to exploit vulnerabilities. The security event underscores the need for policies that improve a healthcare organization's agility to address threats as they are disclosed or discovered.

With all the sophisticated exploit schemes attackers have at their disposal, data breaches in healthcare sector are still mostly accomplished with the most simplistic method, physical theft of devices that contain ePHI. The Verizon Data Breach Report shows that physical theft of portable devices account for 46% of all security incidents in healthcare (Verizon, 2014). One of the largest ePHI compromises involved the theft of four laptops at Advocate Health System. The stolen laptops contained unencrypted ePHI and Social Security numbers of more than 4 million patients (McCann, 2014). The company had already suffered a similar breach in 2009 when a company laptop that contained 812 records was stolen. The breaches demonstrate the HHS's inability to ensure that non-compliant organizations take or continue to enforce corrective measures to remediate a security incident. The Advocate Health System case also highlights the importance of ePHI encryption. Although encryption is considered as an addressable HIPAA Security Rule requirement, it is critical to ensure the confidentiality and integrity of ePHI. A 2012 HIMSS survey shows that 64% of hospitals and private practices claim to utilize encryption (Conn, 2013). However, the use of encryption has been argued to be very cumbersome for most users to adequately apply to their systems. For instance, encryption may degrade system performance and impact user's productivity. Such concerns often prevent encryption from being actively implemented within an organization.

On October 1, 2014, Texas Health Resources, the organization that operates Texas Presbyterian Hospital, blamed an electronic health record (EHR) flaw for the initial misdiagnosis of Thomas Eric Duncan, the first

person diagnosed with Ebola in the US. Texas Health Resources maintained that their EHR failed to display Duncan's travel history on the "physician's standard workflow" (McCann, 2014). Two days later, Texas Health Resources retracted its original statement, saying that the EHR was not flawed and that the travel history was available to everyone involved in Duncan's care. Whether the fiasco was brought on by faulty EHR design or user oversight, the fact remains that the EHR failed to draw attention to a critical piece of information. Incomplete health information constitutes a compromise to the integrity of a person's health data. The compromised integrity of health information can "endanger patient safety or decrease the quality of care" (Bowman, 2013).

4.0 SIMILARITIES AND DIFFERENCES OF CASE STUDY COMPLIANCE ENVIRONMENTS

In each of the incidents described above, an organization in the healthcare sector lost control of or allowed unauthorized access to PHI to take place. The security breaches in these events, which can be considered a representative sample of breaches within the healthcare sector, are caused either by lost or stolen equipment containing unencrypted data, or systems with inadequate protections being penetrated by hackers. The first described incident at the VA and the breach at Advocate Health Systems were both caused by the theft of laptop containing unencrypted PHI from the organization in question. In these and similar cases, the breach events could have been prevented by more thorough physical security, and the damage mitigated or completely avoided if the stored PHI had been encrypted. Both the incident at the Utah Department of Technology Services and the breach at Community Health Systems were caused by poor security configuration of central systems which allowed hackers to gain access to unencrypted PHI. While these incidents are not identical, both should have been easily preventable had the staff responsible for managing those systems taken basic efforts to implement and maintain security measures.

Additionally, in all of these incidents, the organization in question took far too long to identify the problem and act to remedy the error. The UDTS case is a particularly glaring example of this, since the hackers had access to the system for more than 3 weeks before the breach was noticed. This extreme delay suggests that these organizations are unprepared to deal with breach events, perhaps lacking an incident response plan. Perhaps the most important similarity between these various security breaches is that they all resulted in several hundred million dollars in damages to the offending organizations, highlighting how seriously these organizations should have focused on information security and regulatory compliance.

The most significant difference between these organizations is that, while they are all involved in healthcare, they originate from both the public and private sectors. It is very interesting that nearly identical problems plague organizations in both the public and the private sectors, with both the VA and AHS suffering from lax physical security and the UDTS and CHS suffering from poor security management. One might expect that the public sector organizations should be more resilient to some forms of breach, since they are affected by more regulatory restrictions (i.e. FISMA) than the public sector. Likewise, private sector organizations could be expected to perform differently, since they should have more freedom with which to implement security measures and assume different motivations for conducting business. Yet despite these differences, the same basic problems recur all across the healthcare sector namely: poor physical security, poor security management, lack of encryption of sensitive data, and slow incident response.

From a regulatory standpoint, it is also important to note that the health care organizations in the public and the private sectors are interconnected and rely on each other for some services. For example, public organizations frequently hire contractors to perform some tasks (as in the UDTS case), and private organizations can rely on the government for funding, important information, and guidance. This makes regulation and compliance in the healthcare sector more complicated, even though the HITECH Act appears to have leveled the playing field by forcing compliance upon all organizations interacting with PHI. Common security failings across the public and private healthcare sectors raise some interesting questions about the effectiveness of the regulatory mechanisms currently in place on these

organizations. This commonality could indicate that the requirements under HIPAA and HITECH are not doing enough to promote PHI security, or that regulatory compliance is a poor mechanism for promoting information security.

4.01 VALUES AND ISSUES ASSOCIATED WITH INCREASING COMPLIANCE REQUIREMENTS

While regulatory laws like HIPAA and HITECH are passed with the intention of increasing consumer privacy and safety, regulations are not always effective and can be difficult for affected organizations to accommodate. Healthcare sector organizations already struggling financially, especially in the poor economic climate, and new compliance requirements are resource demanding in both money and manpower. The difficulties for regulated organizations are compounded since restrictions can negatively affect organizational productivity.

Regulatory compliance does not always translate into improved security within affected organizations. In many cases, regulated organizations work to achieve compliance in the most efficient way possible, or the fastest and cheapest way possible without focusing efforts on improving organizational security. Studies have shown that organizations that take a strategic approach toward improving their security tend to have more effective defenses, when compared to organizations simply working for regulatory compliance (Kwon & Johnson, 2013).

All things considered, the criteria and security measures required by HIPAA and HITECH are necessary to be ensure that healthcare sector organizations take action to protect consumer data. Civil penalties resulting from breaches alone has not proven to be a strong enough motivator for promoting security in the healthcare sector, and inevitably some organizations would choose lax security to save costs. While regulatory effectiveness and necessity is arguable, it is better to have protections in place to safeguard consumers than to be vulnerable to cyber-attacks which inevitably run into law suits and expensive legal issues and court costs.

Indeed, the consequences for non-compliance with HIPAA requirements can include criminal and civil penalties, as well as more abstract sanctions such as loss of reputation or stock market valuations. Before the passage of HITECH, criminal penalties for HIPAA violations were $100 per violation, stacking up to a maximum penalty of $25,000 for identical violations within a year. Under the revised HITECH rules, HIPAA penalties are tiered with increasing penalties depending on the degree of culpability the court determines the violating organization assumed. The minimum monetary penalty is still $100 per violation if the vulnerability is determined to have been unknown to the organization while the maximum penalty can reach $50,000 per violation if the breach is determined to be the result of willful neglect. The annual cap on monetary criminal penalties for identical violations, regardless of tier, is now $1,500,000, clearly a stark difference compared to the pre-HITECH HIPAA period. The civil penalties for HIPAA violations range wildly depending on the details of the breach and the court decisions. Some penalties reach as high as $1,700,000 (McGrory-Dixon, 2013). In addition to criminal and civil penalties, violating organizations may also incur losses due to the results of bad press following a breach. Additional costs may also be incurred to address the security problems that allowed the initial breach to occur.

5.0 RECOMMENDATIONS AND BEST PRACTICES

Many of the problems that the VA needs to address were identified in the ten findings of the 2013 FISMA audit. Some of these findings included issues with the VA's risk management program, its identity management and access controls, contingency planning, incident response, and security management training. The FISMA audit identified that although the VA had established a risk management framework, the risks were not being communicated to users of the enterprise (Micro, 2013). Additionally, there needed to be more frequent and consistent monitoring of the security controls.

Moreover, the security assessments were not being done on a regular basis as required by FISMA. The audit cited these and other issues as considerable deficiencies in the deployment of identity management and access controls. For example, it was noted that there was a use of weak passwords that allowed malicious users to easily gain unauthorized access to mission-critical systems. Furthermore, many VA systems and facilities had no audit policy.

Executives in charge of information and technology need to devise a mechanism for enforcing stronger passwords to overcome the current password inadequacies. Passwords should be created by avoiding common words, using upper and lower case letters, and combining letters in conjunction with numbers and special characters, etc. User passwords should also be changed on a regular basis. Depending on the sensitivity of the data, the passwords should be changed every month or quarterly. Similarly, findings point to a need for periodic reviews of system access and to instituting the use of a two-factor authentication criteria for remote access.

The audit further found that the VA was unable to monitor all the system connections for unauthorized access attempts or malicious traffic. FISMA stipulates that each organization should create and implement a cybersecurity program comprised of specific procedures for detecting, reporting, and responding to cybersecurity incidents. However, the findings indicated very sloppy incident handling as well as systems full of malware that in many cases took too long to be mitigated. Recommendations to the VA were for them to complete a systems audit to implement a continuous state of system surveillance for all connected devices on the organization's network.

Prior to the data breach discussed in our second case study, UDTS took a compliance approach to regulatory requirements, and was stuck in a defensive or reactionary posture (DeZabala, Saif, & Westerman, 2011). Following the establishment of major federal laws that regulate health care organizations: The Privacy Act of 1974, the False Claims Act, HIPAA and HITECH, the Electronic Signature Act of 2000, and FISMA comes implementation, monitoring and enforcement. Among these one of the largest weaknesses is the lack of enforcement by the U.S. Department of Health and Human Services, or the Office of Civil Rights. Added to this is the imposition of civil fines that are too small to effectively work as deterrent penalties for non-compliance to the law. Hence, even if imposed on violators, they are not high enough to encourage greater compliance.

As all of these examples have demonstrated, the healthcare industry has the "longest average [security] event duration for all industries" (Moore, 2014). When reflecting upon the circumstances experienced in our third case study by Advocate Health System, Texas health Resources, and Community Health Systems, it becomes clear that the time investment for gathering resources could be better used to mitigate the damages.

Hospitals need to look at cybersecurity beyond the context of compliance. Given that these organizations already face overwhelming challenges in following HIPAA to the letter, going beyond mere compliance seems like a tall order. However, a holistic approach to security not only helps ensure satisfaction of all regulatory requirements; it helps ensure that security measures and policies actually address a hospital's "particular circumstances and security priorities" (Doherty & Fulford, 2006). Also, hospitals must align their cybersecurity efforts with their organizational goals and objectives. For instance, since quality patient care is at the core of every hospital's mission, security controls must never interfere or hamper the administration of care. Also, hospitals should not approach security from a purely technical vantage. They must consider the socio-technical dimension of security. Organizations must recognize the critical role of "human factors" such as employee awareness, perceptions and values in security management. Adopting a security framework, especially one designed for healthcare, will help hospitals achieve a comprehensive and adequate security posture. For instance, the HITRUST Common Security Framework, which adapts the ISO 27001 for the healthcare industry, not only identifies appropriate security controls to meet all compliance requirements. The HITRUST framework also presents a tailored approach to security. For example, the framework considers the complexity of the hospital's information systems, the "maturity of the current security processes and controls" and its particular resource constraints

(HITRUST Alliance, 2014). Furthermore, to help improve the entire industry's incident response capabilities, private sector hospitals should consider participating in security information sharing initiatives such as the HITRUST C^3 program.

Organizations within the healthcare sector must also consider incorporating security into its organizational culture. This entails development of a "system of collective moral concepts, mindsets and behavior patterns" (Brady, 2011). Thus, integrating a security philosophy will be a gradual and ongoing process. It is essential that management sets the tone for the rest of the organization. Employees must immediately recognize that management considers "security as a core part of the business" (Johnson & Goetz, 2007). To nurture a security mindset, hospitals must continuously ensure that employees are aware of security issues and of their particular roles in mitigating and minimizing risks.

In the following years, the UDTS leadership team has steered the organization towards a more proactive approach in adopting more industry best practices (Webb, 2013). One recommendation would be to include adaptive authentication which is a new type of access management that flags suspicious requests. Adaptive authentication poses additional challenges to the user making the request and puts a hold on the account or denies the request if the user fails these tests. Suggestions from legal experts include doing everything possible to demonstrate due diligence to stem the loss of good will and decrease chances of success for class-action lawsuits. If basic security measures and protocols were ignored, the company may be found to be negligent (McDavid, 2014). With the next round of approximately 350 random HIPAA compliance audits coming in 2015, policy and procedural compliance should be getting a thorough review.

6.0 CONCLUSION

The Privacy Act, HIPAA, and HITECH are effective regulations when properly implemented, and when used to protect an organization's confidential or sensitive personal information of individuals. The failure to ensure such compliance poses a continuous problem for the integrity and reliability of healthcare systems. This study indicates that a variety of measures and policy implications can be used to mitigate the number and seriousness of cyber-attacks. Such implications extend beyond the letter of the law and evolve into comprehensive compliance in a customized manner that is relevant to the organization, its mission and goals. This results in an institutionalization of an organizational culture of security that is conscientiously and continually practiced by all employees. Such an approach will ensure that cyber security policy implementation becomes part of the job function of all employees and that its essential nature is appreciated. Extending beyond the institution and participating in security information sharing initiatives such as the HITRUST C^3 program will also enhance the way the organization works to protect information in its environmental context.

More study recommendations include monitoring the cyber policy implementation where more frequent and consistent monitoring of security controls is needed. Further, security assessments must be done on a regular basis as required by FISMA. This must be followed by complete systems audits to implement a continuous state of system surveillance for all connected devices on an organization's network.

Finally policy implications also extend to enforcement measures. Static approaches to security are the most effective strategy in regulating compliance combined with civil or criminal penalties to safeguard personal information. The continuation of random audits with added fines for negligence will force organizations to become proactive in passing tests to prevent lawsuits. Organizations will continue to be held responsible for their actions or lack thereof when confronted by breaches in security. Reorganization of priorities is necessary to prevent a repeat of these case studies and their slow reaction in resolving the errors created from failing to comply with regulations. True change and progress in cybersecurity will only become achievable when mere reactionary measures are enhanced with proactive analysis of developing threat vectors on the horizon.

REFERENCES

Anderson, H. (2012, April 9). Utah health breach affects 780,000. *Data Breach Today*. Retrieved from http://www.databreachtoday.com/utah-health-breach-affects-780000-a-4667

Booz Allen Hamilton. (2013). Stemming the rising tide of health privacy breaches revisited. *Booz Allen Hamilton Inc.* Retrieved from http://www.boozallen.com/content/dam/boozallen/media/file/stemming-rising-tide-health-care-breaches-vp.pdf

Bowman, S. (2013, October 1). Impact of electronic health record systems on information integrity: Quality and safety implications. *National Center for Biotechnology Information (NCBI).* Retrieved from http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3797550/

Brady, J. W. (2011). Securing health care: Assessing factors that affect HIPAA security compliance in academic medical centers. *Proceedings of the 44th Hawaii International Conference on System Sciences* (pp. 1-10). Kauai: IEEE.

Civic Impulse. (2009). H.R. 1 — 111th Congress: American Recovery and Reinvestment Act of 2009. Retrieved from https://www.govtrack.us/congress/bills/111/hr1

Conn, J. (2013, August 13). Advocate data breach highlights lack of encryption, a widespread issue. *Modern Healthcare*. Retrieved from http://www.modernhealthcare.com/article/20130830/NEWS/308309953

DeZabala, T., Saif, I., & Westerman, G. (2011, July 1). Evolve or fail. *Deliotte University Press.* Retrieved from http://dupress.com/articles/evolve-or-fail-how-security-can-keep-pace-with-strategy/

Doherty, N., & Fulford, H. (2006). Aligning the information security policy with the strategic information systems plan. *Computers & Security, 25*, 55-63.

Filkins, B. (2014). *SANS health care cyberthreat report: widespread compromises detected, compliance nightmare on horizon.* Retrieved from http://www.sans.org/reading-room/whitepapers/analyst/health-care-cyberthreat-report-widespread-compromises-detected-compliance-nightmare-horizon-34735

Gikas, C. (2010). A general comparison of FISMA, HIPPA, ISO 27000 and PCI-DSS standards. *Information Security Journal: A Global Perspective,* 19(3), 132-141.

Goldfarb, Z. & Lee, C. (2006, June 30). Stolen VA laptop and hard drive recovered. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2006/06/29/AR2006062900352.html

HITRUST Alliance. (2014, July). Cyber threat intelligence and incident coordination center: Protecting the healthcare industry form cyber-attacks. *Health Information Trust Alliance (HITRUST).* Retrieved from http://hitrustalliance.net/content/uploads/2014/07/ HiTrustC3Datasheet.pdf

Johnson, M. E., & Goetz, E. (2007). Embedding information security into the organization. *IEEE Security & Privacy*, 16-24

Judy, H.L., David, S.L., Hayes, B.S., Ritter, J.B., & Rotenberg, M. (2009). Privacy in cyberspace: U.S. and European perspectives. In S. Bosworth, M. E. Kabay, & E. Whyne (Eds.), *Computer security handbook* (5th ed). New York, NY: John Wiley & Sons.

Keizer, G. (2006). *FBI Recovers Stolen Veterans Affairs Laptop*. Retrieved from http://www.informationweek.com/fbi-recovers-stolen-veterans-affairs-laptop/d/d-id/1044759?

Kwon, J. & Johnson, M. E. (2013). Security practices and regulatory compliance in the healthcare industry. *Journal of the American Medical Informatics Association*, 20(1), 44-47.

McCann, E. (2014, October 6). Missed Ebola diagnosis leads to debate. *Healthcare IT News.* Retrieved from http://www.healthcareitnews.com/news/epic-pushes-back-against-ebola-ehr-blame-shifting

McDavid, S. (2014, March). A primer on cybersecurity litigation for the not-so-tech-savvy attorney. *American Bar Association,* 3(8), 17-19. Retrieved from http://www.americanbar.org/publications/gpsolo_ereport/2014/march_2014/primer_cybersecurity_litigation_for_not-so-tech-savvy_attorney.html

McGrory-Dixon, A. (2013). HHS toughens HIPAA violation penalties. *BenefitsPro*. Retrieved from http://www.benefitspro.com/2013/04/09/hhs-toughens-hipaa-violation-penalties

Micro, T. (2013). VA records breach shows difficulty of balancing cyber security, physical security. Retrieved from http://blog.trendmicro.com/va-records-breach-shows-difficulty-balancing-cyber-security-physical-security/

Moore, J. (2014, July 24). Health care providers look to improve security incident response. *iHealthBeat*. Retrieved from http://www.ihealthbeat.org/insight/2014/health-care-providers-look-to-improve-security-incident-response

Paganini, P. (2014, September 16). Risks and cyber threats to the healthcare industry. *Infosec Institute.* Retrieved from http://resources.infosecinstitute.com/risks-cyber-threats-healthcare-industry/

Peters, S. (2014, August 20). Heartbleed not only reason for health systems breach. *Information Week Dark Reading*. Retrieved from http://www.darkreading.com/heartbleed-not-only-reason-for-health-systems-breach/d/d-id/1298157

Ragan, S. (2014, August 14). Community health systems blames China for recent data breach. *CSO.* Retrived form http://www.csoonline.com/article/2466084/data-protection/community-health-systems-blames-china-for-recent-data-breach.html

Schultz, D. (2012). As patients' records go digital, theft and hacking problems grow. *Kaiser Health News.* Retrieved from http://www.kaiserhealthnews.org/Stories/2012/ June/04/electronic-health-records-theft-hacking.aspx

Stewart, K. (2013, April 29). Report: Utah's health data breach was a costly mistake. *The Salt Lake Tribune.* Retrieved from http://www.sltrib.com/sltrib/news/56210404-78/security-breach-health-data.html.csp

Study: Utah health breach could approach $406M. (2013, May 1). *Insurance Journal.* Retrieved from http://www.insurancejournal.com/news/west/2013/05/01/290357.htm

The Ponemon Institute (2014). *Fourth annual benchmark study on patient privacy & data security*. Retrieved from http://www.ponemon.org/library/fourth-annual-benchmark-study-on-patient-privacy-data-security

U.S. Department of Veterans Affairs. (2014). *History - Department of Veterans Affairs*. Retrieved from http://www.va.gov/about_va/vahistory.asp

U.S. Government Accountability Office. (2014). *Information Security VA Needs to Address Identified Vulnerabilities*. Retrieved from http://www.gao.gov/assets/670/666900.pdf

Verizon. (2014). 2014 Data breach investigations report. *Verizon.* Retrieved from http://www.verizonenterprise.com/DBIR/2014/

Vijayan, J. (2012, May 16). Utah CTO takes fall for data breach. *Computerworld.* Retrieved from http://www.computerworld.com/article/2504542/security0/utah-cto-takes-fall-for-data-breach.html

Webb, G. (2013, August 9). What's changed since hackers breached a state Medicaid server? *Utah Business*. Retrieved from http://utahbusiness.com/articles/view/ the_state_of_security