HIPAA Compliance and Cloud Computing

Parshant Tyagi, Navdeep Aggarwal, Bhanu P. Dubey and Emmanuel S. Pilli
Department of Computer Science & Engineering
Graphic Era University, Dehradun, India

ABSTRACT

The Health Insurance Portability and Accountability Act (HIPAA) privacy and security regulations are two crucial provisions in the protection of healthcare data. Governance, compliance and auditing are becoming as important pedagogical subjects as long established financial auditing and financial control. Designing sound IT governance, compliance, and auditing is a challenging task. This paper elaborates the concept of HIPAA compliance in cloud computing by taking a look at the history and dynamics. Cloud computing changes the astir of certain parts of HIPAA Security requirements. We briefly describe the cyber warfare as a premise to enforce the reasons for complying with government regulations for information systems. We discuss the compliance issues of HIPAA with specific reference to cloud computing.

General Terms

HIPAA, cloud computing, cyber warfare

Keywords

Compliance, Security, policy, cyber attacks

1. INTRODUCTION

The Healthcare Insurance Portability and Accountability Act [1,2] is US federal law, enacted by united congress and passed by Bill Clinton that aim to safeguard protected health information (PHI) by regulating healthcare providers. HIPAA came in 1996 but has never been taken seriously before the new act called HITECH (The Health Information Technology for Economic and Clinical Health act) was enacted in 2010. HIPAA indicate that patient's privacy should be emphasized and applied to the whole health industry [3].

Healthcare data generated by the numerous type system that can be collected in to the various type of formats-custom application LOGS, XML, SYSLOG, HL7 and MYRIAD and other formats [4]. It's no surprise that most of the healthcare application do not conform the single data format, the breath of this data is one of the challenging facet for the healthcare organization. Obama administration executes order signed in 2009 that provide bounty on healthcare fraud have begun to change this $ 2.5trillion industry. This order execute challenge the healthcare sector on three fronts, improving patient's outcome, reducing fraud, and supporting regulations [5].

Cloud computing is a hot item in the sequence of high performance computing. Many organizations including government agencies have invested in cloud based services to handle the day-to-day operation of the organization [6]. Cloud computing provide the many benefits to an organization due to the rapid increase of online services and application. The healthcare data rely on the cloud for most of their day-to-day task, and personally identifiable information (PII) will also be stored and proceed on the cloud [7]. The main advantage of this cloud setup, we can access this data anywhere within the world with the internet connectivity, and protect our data on the high configurable cloud data centre.

The major concern with cloud computing is the uncertainty of the security same as the other technology is used by the organization including government agencies. Healthcare and other type of patient data are permanently or temporarily stored in the back-end database beyond the patient control, in this configuration, data confidentiality one of the major concern for patient of the cloud hosted services, when taking in to account the data breaches and recent security incidents. [8,9,10] patient lack of confidence is actually affected the patient's [11] in the lack of alternative option, most patients eventually share their data on with cloud services, rely on the legal agreement and trust the efforts of services providers in securely handling and protecting their data. In order to place the measure are place in to the secure system, cloud computing must adhere to government regulations, this paper will focus on cloud computing and the issues that affect it with HIPAA compliance.

Compliance is one of the greatest challenges faced by organizations today. To help healthcare organization comply with HIPAA, security standard have been created to help organizations protect personally identifiable information. Sensitive enterprise data is always at a risk of being compromised; therefore it has become a mandate to secure sensitive information by establishing network security processes and meeting the guidelines of regulatory bodies. Regulatory compliance standards such as PCI DSS [12], FISMA [13], GLBA [14], SOX [15] and HIPAA require organizations to monitor their network in real-time, ensure high levels of security for their confidential enterprise assets and provide network compliance audit reports to auditors when demanded. It is critical for organizations to observe the regulatory compliance audit guidelines since being non-compliant to the regulatory standards can result in severe penalties [16].

To meet all compliance requirements, organizations are required to take proactive measures to establish network security processes for detecting network anomalies, attacks and other vulnerabilities that can cause harm to the sensitive information of the enterprise. Organizations must fulfill the requirements of the compliance auditor by producing compliance reports such as PCI DSS, FISMA, GLBA, SOX, HIPAA, etc. also demonstrate the security measures taken to curb their network from being compromised. Regulatory bodies also require organizations to retain log data, of their network devices and applications, for long periods, thereby allowing the auditors to authenticate security incidents by checking the audit trails from the log data.

2. BACKGROUND

2.1 HIPAA

HIPAA is an acronym for the Health Information Portability and Accountability Act. To improve the efficiency and effectiveness of the health care system, the Health Insurance Portability and Accountability Act of 1996 (HIPAA), included Administrative Simplification (AM), administrative simplification privilege the security and privacy of health data, the standard are mean to improve the security, efficiency, and effectiveness of the nation health care system.

HIPAA requires that consent be obtained before protected health information—medical information that identifies a particular person—can be shared in certain circumstances. Once health information is de-identified, the information is no longer subject to the Privacy Rule's restrictions and can be shared without consent. Organizations required to comply with HIPAA regulations are termed "covered entities". [17] Common examples of covered entities include, Health insurers, Healthcare clearing houses, Hospitals, Home healthcare agencies, Nursing homes, Pharmacies, Laboratories, Physicians, physiotherapists and general practitioner's offices.

2.2 HIPAA TITLES

HIPAA provide a range of requirements for organizations handing healthcare insurance and PHI. This paper is primarily concerned with HIPAA requirements governing data security and privacy. There are five titles:

2.2.1 TITLE 1: Healthcare Access

Title I of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) protects health insurance coverage for workers and their families when they change or lose their jobs [18]. Title I works with group and individual health insurance plans to ensure availability to you.

2.2.2 TITLE 2: Fraud, Privacy, Security and Administration

Title II lists health care system rules and penalties but is most well known for its "Administrative Simplification" rules. The Administrative Simplification provisions of the Health Insurance Portability and Accountability Act of 1996 (HIPAA, Title II) require the Department of Health and Human Services to establish national standards for electronic health care transactions and national identifiers for providers, health plans, and employers. Also addresses the security and privacy of health data.

Adopting these standards will improve the efficiency and effectiveness of the nation's health care system by encouraging the widespread use of electronic data interchange in health care. The U.S. Department of Health and Human Services (DHHS) develops and publishes the rules pertaining to the implementation of HIPAA and standards to be used. All health care organizations impacted by HIPAA are required to comply with the standards within two years of their adoption. [19]

2.2.3 TITLE 3: Tax Related Health Provisions

Established medical savings accounts and increased the deduction for health insurance costs of self- employed individuals and makes other changes to health insurance law.

2.2.4 TITLE 4: Application and Enforcement of Group Health Plan Requirements

Title IV specifies conditions for group health plans portability, access and renewability for those with pre-existing conditions, and modifies continuation of coverage requirements. It also clarifies continuation coverage requirements and includes COBRA clarification. This amends COBRA's 1985 Act to include language for group health plans.

2.2.5 TITLE 5: Revenue Offsets

Title V Includes provisions related to company -based life insurance plans and it includes tax-deduction mandates for company-owned life insurance premiums. It also explains federal code changes that generate more revenue to offset the additional costs caused by HIPAA implementation.

2.3 HITECH Act

The HITECH Act stands for Health Information Technology for Economic and Clinical Health, enacted as part of the American Recovery and Reinvestment Act of 2009. This act establishes notification requirements on what DHHS defines as covered entities (insurance carriers, providers and employees and contractors, and clearinghouses, etc.), vendors, and business associates. If Protected Health Information is compromised, the HITECH Act establishes the requirements of those who are responsible for the information.

HITECH extends the data privacy and security requirements of HIPAA to business associates of covered entities and stipulates that these requirements be included in agreements and contracts between covered entities and business associates [20]. This Act also inflict additional requirements relating to protected health information security breaches and extends these to not only covered entities, but business associates and vendors of personal health records. Finally, the Act also implements changes in the rules governing disclosures of PHI when an organization uses an electronic health record.

2.4 Cyber Warfare

A definition of cyber warfare is not easy to understand. In fact the cyber and warfare are both under debate we touches the cyber warfare in the movies started with war games in 1983 where a small kid who loves to play games, breaks into a military network and accidently almost starts World War III to Sneakers in 1992 where all data encryption is compromised to Swordfish where intelligence agencies use hacking to support their activities to the epic Die Hard 4: Live Free or Die Hard in 2007 when criminals pose as terrorists and take down the Internet and all the critical infrastructure it supports[21].

Some experts limit cyber warfare only to military operations that are held in cyberspace, other experts describe cyber warfare as hostile action taken on by an aggressor to attack the computer networks of an adversary, still others say cyber warfare can be used to describe various aspects of defending and attacking information and computer networks in cyberspace my extensive research is that cyber warfare is a new form of nonconventional warfare that exploits the

vulnerabilities in computer networks to gather sensitive information from an enemy and or using cyber attacks to cripple or destroy the critical infrastructures of other nation states or independent organizations.

Cyber laws is a growing field that define the policies and rules for how the activities in the cyber world take place Cyber policy is an issue that is discussed readily in the United States and in the international community especially with the increased use of cyber attacks as a form of nonconventional warfare. The hop topic issues include but are not limited to determining the jurisdiction of cyberspace, how plaintiffs and defendants should respond in cyber incidences whether those actors are nation states or independent groups.

3. COMPLIANCE ISSUES:

Compliance is a Conformance with an established standard, specification, regulation, or law. Various types of privacy regulations and laws exist within different countries at the local and global levels, making compliance a potentially complicated issue for cloud computing. The HIPAA in the US is just compliance issues affecting cloud computing, based on the type of data and application for which the cloud is being used. Maintaining and proving compliance when using cloud computing. Issues dealing with evaluating how cloud computing affects compliance with internal security policies, as well as various compliance requirements (legislative, regulatory, and otherwise) are discussed here. This domain includes some direction on proving compliance during a cyber attack, data disclosure, audit, and business continuity.

3.1 Cyber Attacks

As the estimate of cloud computing market are set to reach more than 150 billion dollars this year, it is attracting more cybercriminals to perform malicious activities with financial implication. The methods that used to carry out cyber attacks include: denial of service attacks, logic bomb, malicious programs, digital manipulation, and IP spoofing. DoS attacks are when a Hacker floods a system with so much traffic that the system cannot process all the information. This is the main source of cyber attacks because someone wanting to carry these attacks out can do so on limited resources. Logic bombs are the equivalent to time bombs for a computer. They set off attacks, such as a DoS attack, at a predetermined time or if specific events take place on a system. Malware is used to disrupt the normal operations of a computer system or to give someone access to a computer system. Types of malware include Trojan horses, worms, and viruses. Digital Manipulation is when hackers use computer programs to edit videos and photographic images. IP Spoofing is when hackers redirect traffic from a trusted host to the address of their choosing. If users interact with the content on the page they were redirected to they leave their system vulnerable to attack by the hacker [22].

3.2 Data Disclosure

Another major concern with cloud computing deals the HIPAA's privacy and security regulations are abstract, wide, and often not fully known by the staff of hospitals and clinics, almost all healthcare organizations are unable to completely comply with the regulations protecting the data in the cloud is more difficult task because the data in the cloud is potentially spread out of servers over various locations. The issue here is that the information can be mishandled by the user and disclosed to a insecure source. The issue is here that the information mishandled by the various users and disclosed in to an insecure connection. The cloud provider may have multiple employees dealing with the data the risk for human error increases with cloud computing.

3.3 System Auditing

Audit is well positioned through its role as an assurance function to help management and the board identifies and considers the key risks of leveraging cloud computing technology. Audit also can help the business determine whether those risks are being appropriately mitigated. Internal audit's role and level of effort to support and/or assess cloud computing processes likely will be related to the organization's maturity and experience in this area (i.e., every organization is unique and internal audit departments must adapt accordingly[23].

Auditing is the process of tracing and logging significant events that could take place during a system run-time. It can be used for analysis, verification and validation of security measures to achieve overall security objectives in a system. Since advantages of cloud computing are obvious, but the security risks associated with each cloud service model hinder its widespread adoption According to a survey in 2009, cloud security was revealed as the top most challenge/ issue of cloud computing among others like availability of services, performance, lack of interoperability standards and so on[24].

3.4 Business Continuity

Business continuity and disaster recovery plans become even more important in a cloud-computing environment. The disaster recovery plan is a required implementation specification defined within the HIPAA Contingency Plan standard in the Administrative Safeguards section of the HIPAA Security Rule ***164.308(a)(7)(ii)(B) (7).*** The service provider must have redundancies in place for not only data backups but for the everyday use of the services. if the cloud goes down then organizations will have unacceptable downtown that their IT departments cannot control causing a stop to the critical services that the organization uses to conduct its daily operations.

4. THE PLAN:

4.1 Steps to Compliance

Cloud computing is a mixture of different technologies such as virtualization utility/grid computing, and SOA/web service HIPAA gives guide for each type of cloud service

Fig 1: Different Type of cloud computing services

The NIST Computer Security Division has proposed the following six-step process for increasing the security [25].

1. Categorize Information Systems
2. Select Security Controls
3. Implement Security Controls

4. Assess Security Controls
5. Authorize Information System
6. Monitor Security State

4.2 Current Methods

One of the major issues of the HIPAA Security measures fail and patient data is breached but all physicians and healthcare facilities highly value the security of their patients financial and health information, which called "protected health information" (PHI). Since the risks of reputational harm are high in the security breach, providers are required to notify the all affected patients for action and decrease the chances of being victims of identity theft. The other method is a potential investigation by the office for civil rights of the department of health and human services (OCR). OCR enforces the HIPAA security and privacy rules and also notifies the covered entity of the investigation and request relevant information.

4.3 Recommendation

We would like to build tools that effectively handle the operations of internal activities. Auditing is the best method to control. Audit controls refer to the capability to record and analyze system activity. The entire process helps to control provides a standard means to assess activities regarding the electronic protected health information (EPHI) in an entity's care. Audit control generates the system audit logs, these logs will help to System Activity Review that is required under the Security Rule. An automated audit analysis tool to manage the audit systems as well as the audit logs or records that are generated by the audit system can determine significant events. The audit analysis tool can also provide the log report in the human-readable format that will help the internal system activity review of audit logs. We would like to emphasize the importance of enforcement of HIPAA compliance.

5. CONCLUSION AND FUTURE WORK

There are a number of security issues associated with cloud computing and facing by organization that utilize cloud computing. In most cases, organization must ensure that their client's data protected while customer must ensure that the organization has taken the proper security measures to protect their data. Organization must make sure they are protecting its infrastructure and its users. HIPAA compliance is a step in that direction.

6. REFERENCES

[1] Health Insurance Portability and Accountability Act of 1996 HIPAA.

[2] "Health Insurance Portability Accountability Act of 1996 (HIPAA)," Centers for Medicare and Medicaid Services (1996) [Online]. Available: http://www.cms.hhs.gov/ hipaageninfo. (retrieved: 05/15/2006).wman,

[3] L. Wei-Bin and L. Chien-Ding, 2008 "A Cryptographic Key Management Solution for HIPAA Privacy/Security Regulations," Information Technology in Biomedicine, IEEE Transactions on, vol. 12, no. 1, pp. 34-41.

[4] TBGSECURITY, "Compliance Management," Available: http://tbgsecurity.com/tbg-basic/compliance-management.

[5] Splunk, "Using Healthcare Machine Data for Operational Intelligence " 2013

[6] Zavou, 2010, "An autopsy of data flows in cloud,"

[7] D. T. Le Garen, 2011 "FISMA compliance and cloud computing," in Proceedings of the 2011 Information Security Curriculum Development Conference Kennesaw, Georgia: ACM.

[8] Berghel, H., 2012, Identity theft and financial fraud: Some strangeness in the proportions. Computer 45(1), 86.

[9] Sophos: Groupon subsidiary leaks 300k logins, Fixes fail, fails again (2011 Jun), http://nakedsecurity.sophos.com/2011/06/30/groupon-subsidary-leaks-300k-logins-fixes-fails-fails-again/.

[10] The Wall Street Journal: Google Discloses Privacy Glitch (2009), http:// blogs.wsj.com/digits/2009/03/08/1214/

[11] Gens, F, October 2008, IT Cloud Services User Survey, pt.2: Top Bene ts & Challenges. IDC, http://blogs.idc.com/ie/?p=210

[12] Payment Card Industry Data Security Standard, https://www.pcisecuritystandards.org/security_standards/ pc i_dss.shtml

[13] FISMA:http://csrc.nist.gov/drivers/documents/FISMAfinal.Pdf

[14] Gramm-Leach-Bliley Act (GLBA, the Financial Services Modernization Act), http://www.gpo.gov/fdsys/pkg /PLAW106publ102/contentdetail.html.

[15] Sarbanes-Oxley Act 2002, U.S. Securities and Exchange Commission (effective July 30, 2002), http://www.sec.gov/about/laws/soa2002.pdf

[16] T. D. Breaux, A. I. Anton, C. Karat, and J. Karat, "Enforceability vs. accountability in electronic policies," in Seventh IEEE International Workshop on Policies for Distributed Systems and Networks. pp. 4 pp.-230.

[17] HHS.gov, (2013), "Health Information Privacy," Available: http://www.hhs.gov/ocr/privacy/

[18] ISHERIFF, "HIPAA: Data Security and Privacy Compliance."

[19] C. D. o. H. C. Services, "HIPAA Standards Compliance Calendar,"Available:http://www.dhcs.ca.gov/formsandpubs/laws/hipaa/Pages/1.10HIPAATitleInformatio

[20] NETFORENSICS, "HIPAA, HITECH and the "Meaningful Use" of Log Management & SIEM:," 2010.

[21] S. W. Jason Andress, Cyber Warfare: ELSEVIER, 2011.

[22] A. Jason and W. Steve, Cyber warfare: techniques, tactics and tools for security practitioners: Syngress, 2011.

[23] I. Gul, A. ur Rehman, and M. H. Islam, 2011, "Cloud computing security auditing," The 2nd International Conference on Next Generation Information Technology (ICNIT) , pp. 143-148.

[24] D. Brand, 2012, "Internal Audit's Role in Cloud Computing," EDPACS, vol. 46, no. 2, pp. 1-10.

[25] D. T. Le Garen, 2011, "FISMA compliance and cloud computing," in the 2011 Information Security Curriculum Development Conference Kennesaw, Georgia.