Cyber Security's Significance in Health Information Technology (HIT)

*Dr. Pushpender Kumar
Adjunct Professor School of Management,
Alliant International University, USA

** Prof. Rachna Kumar
Professor, Information Systems and Technology
School of Management Alliant International University

Abstract

This paper explores the growing cyber security issues in the healthcare industry in USA. The consequences of cyber attacks are also explored. Finally the paper explains the Health Insurance Portability and Accountability Act (HIPAA) to discuss the federal privacy standards to protect patients' medical records and other health information.

I. Introduction:

The HIPAA Security Standards for the Protection of Electronic Protected Health Information is known as the Security Rule. It establishes a national set of security standards for protecting health information that is held or transmitted in electronic form by a "covered entity" or its contractors. The Security Rule applies to any health care provider who stores or transmits health information in electronic form. The Security Rule specifies the technical and non-technical safeguards that "covered entities" must put in place to secure electronic protected health information (ePHI). The HIPAA Privacy Rule sets national standards for protecting health information. It addresses the use and disclosure of health information. The HIPAA Privacy Rule includes protections for protected health information, Individual privacy rights to control how health information is used, responsibilities of covered entities standards for exchanging health data and penalties for breach of health data. The HIPAA Security Rule is contained within the Privacy Rule.

"As the health-care industry rushed onto the Internet in search of efficiencies and improved care in recent years, it has exposed a wide array of vulnerable hospital computers and medical devices to hacking. Security researchers warn that intruders could exploit known gaps to steal patients' records for use in identity theft schemes and even launch disruptive attacks that could shut down critical hospital systems. A year-long examination of cyber security by The Washington Post has found that health care is among the most vulnerable industries in the country, in part because it lags behind in addressing known problems[1].

"Cyber-security is an ongoing concern for health care organizations. The Health Information Trust Alliance (HITRUST) has engaged in a written debate with lawmakers on how to proceed with cyber-security strategies. There is a sense of urgency in this discussion because medical equipment poses a serious threat to not only hospital networks but patients' privacy and lives. Even the common problem of data breaches can be costly for health care organizations. When protected health information (PHI) is compromised in a hospital network, violations of the Health Insurance Portability and Accountability Act (HIPAA) can occur, leaving health providers liable for up to $1.5 million in fines from the federal government[2]." "Typically, consumers have faced an uphill battle establishing damages following a data breach. However, in the recent case Claridge v. RockYou, Inc., the United States District Court for the Northern District of California acknowledged that claims arising out of the unauthorized disclosure of personal information are relatively new and given the lack of existing authority, declined to find as a matter of law that a plaintiff could not allege damages as a result of a data breach[3]. 'The range of threats facing computer users and critical infrastructure is

complex and continuously evolving. Attacks vary based on the target and skill level of the actor, ranging from publicly accessible malware that can be purchased on the open market. Attackers also have varied motivations, including monetary gain to political ideologies. Though technical explorations provide insight into how to defend against these crimes, there is still a great deal that is unknown about the social world of hackers[4].“Cyber-security no longer means only protecting your computer from ne'er-do-wells. Hackers are cracking codes on all sorts of devices and getting sneaky about breaking into everything from cell phones to car systems. "Security threats are escalating every year," says Adam Wosotowsky, a senior anti-spam analyst with McAfee Labs. In years past, hackers often engaged in what could be considered mischievous fun -- finding vulnerabilities in software and then pointing out problems that needed to be fixed. But over the past decade, Wosotowsky says, security threats have become more malicious, with criminals entering the scene stealing financial and personal information, and even worldwide governments engaging in cyber warfare[5].”

“Our electronic devices are such a big part of our lives today that it’s hard to imagine what we once did without them. But our constant use of technology to keep in touch, pay bills, stay on top of the news, shop and research things has a downside: Our data can be exposed to criminals who commit crimes such as identity theft and credit card fraud – unless we take the proper precautions. Our growing reliance on electronic devices is part of the reason why careers in cyber security are growing at a faster pace. Jobs in information security, web development and computer network architecture – three fields at the forefront of cyber security – are expected to grow 22% between 2010 and 2020[6]. The US healthcare delivery system has evolved over the past century from a patient-physician dyadic relationship into a complex network linking patients to multiple stakeholders IT advances and their adoption in healthcare are more likely to improve care provision quality, reduce costs, and advance medical science. However, this evolution has increased the potential for information security risks and privacy violations[7]. Everyday news report cyber attacks especially on your email, credit card and on information which is crucial and having financial impact. We believe if the organizations are small and low profile then they can escape from the attackers but everyday there are attacks on small and low profile organizations like hospitals and health care centers. Criminals are very successful to attack on these small to medium health care and hospitals.

It is pivotal to protect health information in Electronic Health Records (EHRs). The aftermaths of the cyber attacks could be serious, including breach of patient trust, violations of Health Insurance Portability and Accountability Act (HIPAA) or even loss of life. Adoption of EHRs is leading to more and more chances of criminal attacks on health care practices. Many new hospitals and health care centers will have new EHRs which will increase the level of attacks. Even though cyber attacks from hackers and other criminals grab a lot of headlines, research indicate that often times, well-meaning computer users can be their own worst enemies. Why? Because they fail to follow basic safety principles. This might be due to lack of training, time pressure or any of range of reasons[8].

As per the VERIZON – Threat landscape healthcare research report – 94% of hospitals had at least one breach in the last two years and most criminals are actually more interested in accessing a patient’s personal details and applying for credit cards in their name than getting hold of their medical histories. 87% of attacks were by external actors in all industries but in healthcare attacks insider played a role – accounting for nearly a fifth of cases and Point of Sale (POS) systems and desk tops were the most commonly breached devices in healthcare organizations. 84% of healthcare data breaches were first spotted by law enforcement, not by the organization affected and hacking and malware are common practices in healthcare. Health care has a culture in which physicians, nurses and other health-care workers sidestep basic security measures, such as passwords, in favor of convenience. Medical devices at Veterans Affairs facilities were infected by malicious viruses at least 181 times from 2009 to 2011[9].

To protect the privacy and security of health information, the U.S department of Health and

Human Services (HHS) under HIPAA has developed privacy rule and security rule.

01. The privacy rule or standards for privacy of individually identifiable health Information established national standards for the protection of certain health.
02. The security rule or standards for the protection of electronic protected health information establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. A major goal of the security rule is to protect the privacy of individual's health information while allowing covered entities to adopt new technologies to improve the quality and efficiency of patient care.

II. Relation between security rule and privacy rule:

The security rule operationalizes the protection contained in the privacy rule by addressing the technical and non-technical safeguards that organizations called "covered entities" to secure individual's electronic protected health information (PHI). Within the HHS, the office for civil rights (OCR) has responsibility for enforcing the privacy and security rules with voluntary compliance activities and civil money penalties.

Who is covered by the security rule:-

(i) Health Plans; an individual or group plan that provides or pays cost of medical care services or supplies related to health of individuals.
(ii) Health care clearinghouses.
(iii) Health care provider who transmits health information in electronic form in connection with a transaction.

What information is protected:-

Electronic protected health information: The HIPAA privacy rule protects the privacy of individually identifiable health information called protected health information.

Security standards:-

To maintain reasonable and appropriate administrative, technical and physical safeguard for protecting PHI following rules need to be followed[10]:

(i) Ensure the confidentiality, integrity, and availability of all e-PHI that create, receive, maintain or transmit. Confidentiality means, the property that data or information is not made available or disclosed to unauthorized persons or processes. Integrity means the property that data or information have not been altered or destroyed in an unauthorized manner.
(ii) Identify and protect against reasonably anticipated threats to the security or integrity of the information.
(iii) Protect against reasonably anticipated, impermissible uses or disclosures.
(iv) Ensure compliance by their workforce.

Technical safeguards:

(i) Access control: -Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software program that have been granted access rights.
(ii) Unique use identification: - Assign a unique name and / or number for identifying and tracking user identity.
(iii) Emergency access procedure: - Establish (implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.
(iv) Automatic Log off: - Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.
(v) Encryption and decryption: - Implement a mechanism to encrypt and decrypt electronic protected health information.

Privacy rule:-

The main objective of the privacy rule, a federal regulation under HIPAA of 1996, is to protect certain health information that identifies individuals who are living or deceased. The privacy rule covers following activities[11]:

01. The privacy rule balances an individual's interest in keeping his or her health information confidential with other social benefits. The department of health and human services (HHS) issued the privacy rules; HHS's OCR has been given the authority to implement and enforce it.
02. Research organizations that handle individually identifiable health information will not have to comply with the privacy rule because they will not be covered entities.
03. Covered entities, which must comply with the rule, are health plans, health care clearinghouses and certain health care providers.
04. The privacy rule establishes conditions under which covered entities can provide researchers access to and use of PHI when necessary to conduct research.
05. The rule also confers certain rights on individuals including rights to access and amend certain health information and to obtain a record of when and how their PHI has been shared with other for certain purposes.
06. Covered entities that fail to comply with the privacy rule may be subject to civil monetary penalties, criminal penalties or imprisonment.
07. Hybrid entities; any single legal entity may elect to be a hybrid entity if it perform both covered and non covered functions as part of its business operations. A covered function is any function the performance of which makes the performer a health plan, a health care provider, or a health care clearing house: to become a hybrid entity the covered entity must designate the health care components within its organization. A health care component may also include any component that conducts non covered health care provider or business associate.
08. Following information covers under privacy rule:
    (1) Name,
    (2) Address,
    (3) Date of Birth
    (4) Telephone
    (5) Facsimile no
    (6) Email
    (7) SS number
    (8) Medical record no.
    (9) Health plan beneficiary no.
    (10) Account no.
    (11) Certificate/license no.
    (12) Vehicle identifiers and serial no.
    (13) Web universal resource locators (URLs)
    (14) Internet protocol (IP) address no.
    (15) Biometric identifiers, fingerprints.
    (16) Full face photo
    (17) Any other unique identity no.

- As per the 2013 survey on medical identity theft report of Ponemon Institute, in 2012 an estimated 1.84 million Americans became victims of medical identity theft. This is an increase of 19% or 313,000 over the 2011 estimate of 1.52 million individuals. Medical identity theft can put victims' lives at risk. 50% of victims were not aware that medical identity theft can create inaccuracies in their permanent medical records. The objective of the medical identity theft is to obtain healthcare services or treatments, prescription pharmaceuticals, medical equipment or government benefits. Most medical identity theft victims lose trust and confidence in their healthcare provider following the loss of their medical credentials. In a Ponemon Survey on Medical Identity Theft, over a third of the victims of medical theft faced burdensome financial costs in a number of different areas. In a Ponemon Survey, a third of the victims spent an average $18,660 to restore their medical identity. The largest amount was spent on identity protection, legal counsel and credit reporting for an average of $8,369. In a nine country survey conducted by Ponemon, the health care sector in general faced the greatest costs following a data breach at $233 per person[12].

Ten best cyber security practices[13]:-

- Use Strong Passwords and Change Them Regularly:

  Passwords are the first line of defense in preventing unauthorized access to any computer. Strong passwords, combined with effective access controls, help to prevent casual misuse. Use a password that does not have characteristics that could make it vulnerable. Strong

passwords should not include personal information. Strong passwords should include at least eight characters in length using upper case and lower case letters, numbers and special characters, such as a punctuation mark. Passwords should be changed on a regular basis, to reduce some of the risk that a system will be broken into with a stolen password.

- Install and Maintain Anti-Virus Software
  The primary way that attackers compromise computers in the small office is through viruses and similar code that exploits vulnerabilities on the machine. Computers can become infected by seemingly innocent outside sources such as CD-ROMs, email, flash drives, and web downloads. Use Anti-virus software that provides continuously updated protection against these exploits. How can users recognize a computer virus infection? System will not start normally (e.g., "blue screen of death"). System repeatedly crashes for no obvious reason. Internet browser goes to unwanted web pages. The user cannot control the mouse/pointer.
- Use a Firewall:
  Unless a small practice uses an EHR system that is totally disconnected from the Internet, it should have a firewall to protect against intrusions and threats from outside sources. A firewall's job is to prevent intruders from entering in the first place.
  The anti-virus can be thought of as infection control while the firewall has the role of disease prevention. A firewall can take the form of a software product or a hardware device. The firewall inspects all messages coming into the system from the outside and determines whether the message should be allowed on the network. Large practices that use a local area network (LAN) should consider a hardware firewall.
- Control Access to Protected Health Information:

The password is only one half of what makes up a computer user's credentials. The other half is the user's identity, or user name. The user name and password are part of an access control system in which users are assigned certain rights to access the data within. An EHR implementation needs to be configured to grant access to PHI only to people who need to know it. EHR systems should be configured carefully to allow limitation of access in all but the smallest practices. Access controls can be configured for role-based access control, so a staff member's role within the practice determines what information may be accessed.

- Control Physical Access:

  Just as files with health care information must be secured, the devices themselves that make up an EHR system must also be safe from unauthorized access. The single most common way that PHI is compromised is through the loss of devices themselves. More than half of all data loss cases consist of missing devices: flash drives, CDs laptops, handhelds, desktop computers, and even hard drives ripped out of machines. It is vital to limit the chances that a device may be tampered with, lost, or stolen. Physically secure devices and information physically: Secure machines in locked rooms. Manage physical access to computer equipment. Restrict ability to remove devices from a secure area.

- Limit Network Access

  Tools that outsiders to gain access to a health care practice's network must be used with extreme caution. In a wireless network, the router must be secured to keep its signal from being picked up by unauthorized persons. Protected Health Information in the wireless network must be encrypted to maintain its protection. Devices brought into the practice by visitors should not be

permitted access to the network. In configuring a wireless network, each legitimate device must be identified to the router and only those devices permitted access to the network. Check to make sure that peer-to- peer applications have not been installed without explicit review and approval.

- Plan for the Unexpected

  Important health care records and other vital assets must be protected against loss from fire, flood, hurricane, earthquake and other natural or man-made disasters. From the first day a new EHR is functioning in a practice, the data must be backed up regularly and reliably. Backup media must be tested regularly for their ability to restore properly. One option for backup storage is cloud computing, but is must be stored according to HIPAA regulations. Storage of backup media must be protected with access controls. Recovery planning must be done so that when an emergency occurs there is a clear procedure in place.

- Maintain Good Computer Habits:

  EHR systems must be properly maintained so that they will continue to function properly. Uninstall any software application that is not essential to running the practice or is no longer needed. Do not simply accept defaults or "standard" configurations when installing software. "Back door" connectivity for updates must be well-secured at the firewall monitored closely for intruders. Disable remote file sharing and remote printing within the operating system configuration. Disable user accounts for former employees. Computers, faxes and photocopiers with data stored on them must be "sanitized" before disposal.

- Protect Mobile Devices

  Mobile devices present threats to information security and privacy. Some of these threats overlap those of the desktop world, but others are unique to mobile devices. Because of their mobility, mobile devices vulnerable to theft, so they should have strong password protection. Laptop computers and other mobile devices must have all wireless communications encrypted and protected. Mobile devices that cannot support encryption should not be used. Transporting data with mobile devices is inherently risky, so should be avoided without strong security controls. If it is absolutely necessary to take a laptop out of a secure area when the laptop contains patient data, the laptop's hard drive should be encrypted.

- Establish a Security Culture

  The weakest link in any computer system is the user. No security policy is effective unless the health care practice is willing and able to implement policies. Enforce policies that require safeguards to be used. Effectively train all users so that they are sensitized to the importance of data security. Health care practices must instill and support a security-minded organizational culture. Security practices must be built in not bolted on.

III. Conclusion:

The Washington post has found that health care is among the most vulnerable industries in the country, in part because its lags behind in addressing the known problems though tens of thousands of doctors and hospitals are using the systems to digitize and share millions of patients' records.

The electronic processing of health information provides considerable benefits to patients and health care providers at the same time that it creates serious risks to the confidentiality, integrity and availability of the data. The internet provides opportunity to hackers to obtain private health information, with reaching consequences to the unsuspecting victims. In order to address such threats to electronic private health

information, the U.S. Department of Health and Human services enacted the HIPAA security rule which thus far has received little attention in the legal literature[14].

IV. References:

01. Robert (2012). Health-care sector vulnerable to hackers, researchers say Retrieved from http://www.washingtonpost.com/investigations/health-care-sector-vulnerable-to-hackers-researchers-say/2012/12/25/72933598-3e50-11e2-ae43-cf491b837f7b_story.html?hpid=z1
02. Department of Homeland Security (2013) Combat Cyber Crime. Retrieved from http://www.dhs.gov/combat-cyber-crime on February 26, 2013. By Brian T. Horowitz, Brian, T. (2012). Cyber-Security in Health Care: 10 Ways to Fight the Threats. Retrieved from http://www.eweek.com/enterprise-apps/slideshows/cyber-security-in-health-care-10-ways-to-fight-the-threats/
03. Timm, Kari (2011). Unauthorized Disclosure of Personal Information May Cause Injury In Fact. Retrieved from http://www.cyberprivacynews.com/2011/05/california-federal-court-acknowledges-that-an-unauthorized-disclosure-of-personal-information-may-cause-injury-in-fact/
04. Holt, Thomas, J. (2012) Examining Attacker Behavior On and Off-Line Using Social Science Research – Video Published on Apr 3, 2012. Retrieved from http://www.youtube.com/watch?v=3tOEgVgPtCs on February 23, 2013
05. Kawamoto, Dawn (2012). The Top 10 Looming Computer Security Threats of 2012. Retrieved from http://www.dailyfinance.com/2012/01/03/the-top-10-looming-computer-security-threats-of-2012/ on February 23, 2013.
06. DeVry University (2013). The Top 5 Cyber Security Threats That Could Affect Your Life. Retrieved from http://www.devry.edu/know-how/top-5-cyber-security-threats-that-could-affect-your-life/ on February 6, 2013.
07. Appari Ajit, Johnson M.Eric, Information security and privacy in healthcare current state of research, International journal of Internet and enterprise management Vol 6. No. 4, 2010, wwwclearwatercompliance.com
08. Cyber security the Protection of data and systems in networks that connect to the internet. 10 best practices for the small healthcare environment V.10 November 2010.
09. Verizon – threat landscape healthcare research report, 2013 data breach investigation report verizonenterprise.com/dbir/2013.
10. Summary of the HIPAA security rule, Health information privacy, US department of health and human services.
11. Protecting personal health information in research understanding the HIPAA privacy rule, www.hhs.gov/ocr/hipaa.
12. 2013 Cost of Data Breach Study: Global Analysis,Benchmark research sponsored by Symantec Independently Conducted by Ponemon Institute LLC, May 2013 Ponemon Institute© Research Report, https://www4.symantec.com/mktginfo/whitepaper/053013_GL_NA_WP_Ponemon-2013-Cost-of-a-Data-Breach-Report_daiNA_cta72382.pdf
13. CYBERSECURITY, The protection of data and systems in networks that connect to the Internet , 10 Best Practices For The Small Healthcare Environment, http://www.healthit.gov/sites/default/files/basic-security-for-the-small-healthcare-practice-checklists.pdf

14. Hoffman Sharona and Podgurski Andy, In sickness,Health and Cyberspace: Protecting the Security of Electronic Private Health Information, Boston College Law Review Vol.48, No. 2, March 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=931069