Health data breaches: The need for information assurance strategy.

Emmanuel U Amadi
University of Phoenix

ABSTRACT

The implementation of electronic health records system has experienced an increase in the United States of America as a result of the Health Information Technology for Economic and Clinical Health Act (HITECH). With the increase in electronic health records system implementation, comes the risk of health care data breaches that put patients at the risks of identity thefts, insurance frauds and other risks emanating from data breaches. Effective information assurance strategy has become very imperative for health care facilities to institute and implement to safeguard against data breaches and their devastating effects on patients.

Keywords: Data breach, Health data breaches, Electronic health records, Information assurance, Medicaid and Medicare fraud, Insurance fraud.

INTRODUCTION

The buzz in the health care industry is electronic health records system (EHR) and all of its associated benefits (Amadi, 2015, Aarts and Koppel, 2009; Bates, 2002; Bates, Leape, Cullen, et. al, 1998). Despite some of the barriers to the implementations of electronic health records system such as prohibitive cost of many EHR systems, limited access to capital and infrastructure, suitability of EHR products for rural health care settings, difficulty in connecting to or obtaining broadband service, limited health information technology (IT) workforce, difficulty in obtaining stakeholders' buy-in (Shields, Peter, Shin et al 2007; DesRoches. Campbell, Rao SR et al, 2008; Healthit.gov, 2015; Jha, DesRoches, Campbell, et. al., 2009), EHR implementations have increased (Charles, Gabriel and Searcy 2015; DesRoches, Campbell, Rao SR et al, 2008; Jamoon, Batty, Bercovitz et al, 2011).

"Electronic health record system is a computer information system used in health care settings. Electronic health record contains all the medical information/records (tests, results, prescriptions, etc.) of an individual from all of the individual's health care providers. This information is accessible by authorized care providers as well as by health and life insurance companies, government agencies as well as by researchers within the limits of the law" (Amadi, 2015, p.2).

Electronic health records system is integrated with various hospital information systems (HIS), financial information systems (FIS), clinical information systems (CIS), pharmacy information systems (PIS), nursing information systems (NIS), laboratory information systems (LIS), radiology information systems (RIS), and picture archiving and communications systems (PACS) through various interfaces to provide comprehensive, accurate and up-to-date patients' medical information and records that are easily accessible by authorized health care providers. Electronic health records system therefore prevents "in the dark" practice of patient care and management due to incomplete patient medical history or information (Litvin, 2007), since all available patient health information and tests are readily available for the health care providers. No health care facility should be without an electronic health records system.

IMPLEMENTATION RATES OF EMR SYSTEMS

Electronic health records system implementation in the United States has increased over the years according to studies. A study by Jamoon, Batty, Bercovitz et al (2011) showed 54% of physicians in office base practice, 100% of all physicians in health maintenance organizations, about three-quarters of physicians in community health centers (73%), and about 70% of physicians in academic health centers have adopted EHR system (Jamoon, Batty, Bercovitz et al, 2011). According to Jamoon, Batty, Bercovitz et al. (2011) about 58% of primary care, 54% medical care specialists and 48% of surgical specialists have adopted an EHR system and about three-quarters of physicians who have adopted an EHR system reported that their systems meet the "meaningful use" criteria. The implementation rate has also increased in ambulatory settings, 4% of physicians have an extensive and fully functional electronic health records system, and 13% have basic systems (DesRoches, Campbell, Rao SR et al, 2008)

A study by the Office of the National Coordinator for Health Information Technology (ONC) of non-federal acute care hospitals found that 76% of the hospitals have adopted at least a basic EHR system, an increase of 27% from 2013 and eight-fold increase since 2008 and 97% of reported hospitals have certified EHR technology, an increase of 35% since 2011 (Charles,

Gabriel and Searcy 2015). Charles, Gabriel and Searcy (2015) also found that the adoption of comprehensive EHR systems by hospitals have increased by 34.4% in 2014, an eleven-fold increase in the last five years (Charles, Gabriel and Searcy 2015).

These increases could be attributed to the Health Information Technology for Economic and Clinical Health Act (HITECH), a part of the American Recovery and Reinvestment Act (ARRA) signed into law on February 17, 2009 by President Barack Obama. The Health Information Technology for Economic and Clinical Health Act (HITECH) provided billions of dollars for the expansion of Health Information Technology as well as incentives to hospitals and clinics to adopt and meet the meaningful use of electronic health records system (Health IT.gov). HITECH also established the Health Information Technology Extension Program, a program that funds more than 60 regional extension centers (RECs) that provide technical help and information for physicians as well as critical care access and rural hospitals in the United States on the adoption of EHR system (Health IT.gov). These figures are likely to increase as hospitals are forming rural health alliances, and the implementation of EHR system in a health care faculty has also become one of the recruiting tools for physicians (Amadi, 2015).

INCIDENCE OF EMR DATA BREACHES

One of the benefits of information technology advancement in modern health care environment is the development of electronic health records system for patient care and management (Amadi, 2015). The attributes of electronic health records system over its predecessors lie in the centralization of patient's medical information and its integrations with other patient care information systems. These attributes and features while they allow for portability and mobility of patients' health records throughout the continuum of care spectrum; they also place patients' health data at risks of data breaches.

The incidence of data breaches has increased in recent years that President Obama has proposed an increase in cybersecurity budget to $14 billion. According to a 2015 data breach study, there were about 79,790 security incidents and 2,122 confirmed breaches in 61countries in 2014 (Verizon, 2015). The data beaches resulted in about 700 million records been compromised and a financial loss of about $400 million (Verizon, 2015).

Patients' health data are not spared by these onslaughts of data breaches. According to the Verizon 2015 data breach study, health care industry is one of the most affected industries of data breaches. Some of the health care facilities affected by data breaches in USA were Community Health systems that affected 4.5 million individuals in 2014, Anthem data breach that affected 80 million individuals in February 2015, Primera Blue Cross data that affected 1.1 million individuals breach in March 2015 and UCLA Health data breach that affected 4.5 million in June 2015.

A patient's health record contains vast amount of personal administrative, demographics and medical information such as prescription history, social security number, home address and phone numbers, date of birth, credit card information as well as insurance information. Some of this information could be used in identification and security questions for various purposes. A breach of a patient's health records could result in identity theft, medical fraud with a resultant inaccurate medical history, misdiagnosis, treatment and also possible denial of payment by health insurance companies. Such breaches could result in Medicaid and Medicare fraud, insurance fraud as well as prescription fraud.

Part of implementing a strategic information technology system in business operations and utilizing information technology in health care facilities for strategic business operations is ensuring the confidentiality, integrity, accessibility, privacy and security of patient health records. To help ensure the proper safeguards of patient health records, the Health Insurance Portability and Accountability Act (HIPAA) was enacted in 1997. HIPAA brought in a much needed national security and privacy standards and requirements to the health care industry that were nonexistent prior to the enactment of the Act (HHS.gov).

Despite these provisions and requirements, data breaches still occur in the health care industry as mentioned earlier and also as evident by the number of health care breaches reported to the U.S. department of Health and Human Services office for Civil Rights by health care providers, a requirement of the HIPAA Act.

SOURCES OF HEALTH CARE DATA BREACHES

As required by section 13402(e)(4) of the Health Information Technology for Economic and Clinical Health (HITECH) Act (HSS.gov), data collected by the U.S. health and human services for health care breaches that affected 500 or more individuals between 2009 and 2015, showed that health care data breaches occurred in all the 50 states, a total of 1,252 health care entities where affected and 1,382 patients data were affected during this period (HHS.gov.). Analysis of the data is summarized in the tables below.

Table 1: Business associate involvement

No	1100	79.59%
Yes	282	20.41%

Table 2: Top 13 reported locations of breached information

Location of Breached Information	Number of occurrences	% of occurrences
Paper/Films	315	23.30%
Laptop	249	18.42%
Network Server	165	12.20%
Other	146	10.80%
Desktop Computer	119	8.80%
Email	96	7.10%
Other Portable Electronic Device	79	5.84%
Other, Other Portable Electronic Device	44	3.25%
Electronic Medical Record	42	3.11%
Laptop, Other Portable Electronic Device	13	0.96%
Desktop Computer, Laptop	11	0.81%
Desktop Computer, Network Server	9	0.67%
Other, Paper/Films	8	0.59%

Table 3: Summary of types of breaches

Types of Breach	Number of Occurrences	% of occurrence
Theft	642	46.45%
Unauthorized Access/Disclosure	271	19.61%
Hacking/IT Incident	130	9.41%
Loss	100	7.24%
Other	89	6.44%
Improper Disposal	44	3.18%
Theft, Unauthorized Access/Disclosure	24	1.74%
Loss, Theft	15	1.09%
Unknown	19	1.37%
Hacking/IT Incident, Unauthorized Access/Disclosure	10	0.72%
Other, Unauthorized Access/Disclosure	7	0.51%
Loss, Unauthorized Access/Disclosure	5	0.36%
Other, Theft	5	0.36%
Hacking/IT Incident, Theft, Unauthorized Access/Disclosure	3	0.22%
Improper Disposal, Loss	3	0.22%
Improper Disposal, Loss, Theft	3	0.22%
Hacking/IT Incident, Other	2	0.14%
Improper Disposal, Unauthorized Access/Disclosure	2	0.14%
Loss, Other	2	0.14%
Loss, Unknown	2	0.14%
Other, Theft, Unauthorized Access/Disclosure	2	0.14%
Other, Unknown	2	0.14%

Table 4: Summary of number of beaches

Year	Number of breaches	% of breaches
2009	18	1.30%
2010	197	14.25%
2011	192	13.89%
2012	192	13.89%
2013	249	18.02%
2014	278	20.12%
2015	256	18.52%

Analysis of the data showed increased incidence of health data breaches occurred in-house (79.59%). Majority of the data breaches were due to theft (46.45%), followed by unauthorized access/disclosure (19.61%) and Hacking/IT incident (9.41%). Analysis of the locations of the breaches showed almost all aspects of information storage locations were affected. Considering the importance of patients' health data security and privacy, the effect of such breaches to patients, the reputation of the health care facility, and the penalties associated with health data breaches, effective information assurance strategy is a must for health care facilities.

IMPLEMENTING A GOOD IT ASSURANCE STRATEGY

The modern health care environment while technologically wired and well integrated still remains a patient centric environment. The technologically dependent health business and operational environments face new frontier in data security like other industries that are dependent on information technology. Studies have shown that about 51% of US companies lack comprehensive information assurance and security policies (Anonymous, 2007; Gordon & Loeb, 2002). In an environment where business operations depend on the use of information technology, a well-articulated and implemented information assurance strategy should be an important part of the organizational information technology (IT) governance.

Information Assurance (IA) is defined by Department of Defense Instruction (DoD) 8500.01E as the "measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation." Information assurance strategy provides reliable management decision-making process, enhances customer trust, ensures business continuity and good governance and should be viewed as an enabler for business strategic missions and critical operations rather than as a constraint to business operations (Cummings, 2002; Colwill, Todd, Fielder et al. 2001; Colwill and Gray, 2007; Ezingeard, McFadzean and Birchall, 2005; Hung and Wong, 2009; Kovacich, 2001; McEvilley, 2002).

Technological revolution, information usage and the need for real time or anywhere access to data requires the establishment of appropriate process based information assurance strategy as part of an organizational IT governance that aligns with and based on organizational strategic business and operational processes. While most health care organizations have invested resources in the implementation of EHR system, the same should be invested in implementing an appropriate, comprehensive and effective information assurance strategy. Information assurance strategy provides operational, tactical, strategic and organizational benefits.

A good information assurance strategy consists of administrative, physical and technical measures. Identification of the most critical information assets, their locations, IT dependent processes and identifications of the threats posed to IT infrastructures and organization's strategic goals are core elements for any successful information assurance strategy.

Health care facilities responsibilities go beyond patient care and management and include ethical responsibilities as well as mandatory requirements to safeguard patients' health information. A good understanding of these responsibilities and the communication of the business value of information assurance to all the organizational levels in clear business terms with defined risks and ownerships are the keys to designing and implementing an effective information assurance strategy.

ADMINISTRATIVE MEASURES

Administrative measures based on risk assessments and risk management should be incorporated in all aspects of organizational structure and culture as part of the information assurance strategy. Security awareness and employees' education and training on cyber as well as non-cyber aspects of security are crucial as these will promote responsible use of the IT infrastructure and help reduce accidental or negligent breaches (Korotka, Yin and Basu, 2005; Loghry and Veach, 2009; McCrohan, 2003; Moulton, 2003; Peterson, 2004; Schou and Trimmer, 2004). Organizational policies and strategies should ensure privacy and privilege requirements are based on job and task responsibilities, on the principle of least privilege and job descriptions

are properly defined with roles and responsibilities of each employee in ensuring the information assurance strategy of the organization (Korotka, Yin and Basu, 2005; Loghry and Veach, 2009; McCrohan, 2003; Moulton, 2003; NASA; Peterson, 2004; Schou and Trimmer, 2004).

Proactive measures with established contingency plans and measures including notification and escalation tree, with all vital information outlying triggers, specific actions in response to such triggers, and off-hours contact information of key IT and non IT personnel are crucial part of an IA strategy (Dawes, Cresswell and Pardo, 2009). Policies should be instituted against the portability of patient health information on a flash drive or on a laptop and if necessary, the media should be encrypted. Availability of skilled professionals enhance the success of IT project, candidate sections for IA infrastructure should be based on appropriate skill sets (Amadi, 2015; Amadi and Born, 2013; Lu, Tsang and Peng, 2008; Sveen, Rich, and Jager, 2007).

Incident response capability should be enhanced by the development of various possible scenarios and documentations of procedures to these scenarios. Regular exercises and drills enhance better responses when a real event occurs. In a world of business partnership and information sharing, a trusted model of data sharing and connectivity should be implemented to ensure security compliance. Business associate agreements should address the processes of data breach notifications and responses. Information assurance strategy should be built into all business partnership processes, and maintained and controlled in-house.

PHYSICAL MEASURES

Well implemented physical security control is a crucial aspect of an information assurance strategy since weaker physical control could be exploited with ease. Traceable access control to datacenters or server rooms and to areas with information systems that contain patient health records should be implemented. Non-in-house IT staff should be accompanied by IT or security personnel when accessing these areas and accesses to these areas should be audited regularly to ensure compliance.

Hard copies of patient data should be placed in secured waste container and properly destructed and disposed of.

TECHNICAL MEASURES

The most talked about portion of an information assurance strategy is the use of technical measures in defending an organization's information technology infrastructure and ensuring that the organization's information enclave is secured. Analysis of the network topology is an important aspect in implementing appropriate technical measures against any data breach (May, Baker, Gabbard, et al, 2004).

Firewall either hardware or software based is a crucial part of the technical measures and should be implemented. Implementation of the four primary types of Intrusion detection and prevention systems (IDPS): network-based, wireless, network behavior analyst (NBA) and host-based IDPS should be considered as they are synergistic in actions (May, Baker, Gabbard, et al, 2004; NIST, 2012).

Virtual Private Network (VPN) is an important technical measure with the increase in business partnerships, and the sharing of sensitive and privileged information over the internet. The use of Virtual Private Network should be encouraged for employees that need remote access to information and placement of patient data on the laptop or mobile storage devices should be

discouraged. Other technical measures include virus protection, certificate server, and directory services vulnerability scanners, matching hardware resources to software requirements, data encryption, correct configuration servers, tracking vulnerabilities and applying periodic software updates and application patches (Badawy. 2007; Ezingeard, McFadzean and Birchall, 2005; May, Baker, Gabbard, et al, 2004).

Protecting home network system should also be considered as an information assurance strategy, since most employees access corporate networks from homes. Best practices for keeping home network system secured should be the norm such as migrating to new operating system and platform, installing a comprehensive security suite, using web browsers and PDF reader with sandboxing capabilities and updating application software (NASA). Organizations need to educate employees on how to and the need to protect home networks, avoid the exchange of work related information using home network systems and use different usernames and passwords for home and work e-email accounts (NASA).

CONCLUSION

Organizations should be aware of their responsibilities to their customers and stakeholders in safeguarding data; a good understanding of these is the key to designing and implementing an effective information assurance strategy. In an age of increasing data breaches, security of data should not be left unaddressed and to luck. "That won't happen to me" attitude is no longer acceptable. Information assurance should be part of the IT governance of an organization.

Appropriate policies that guide and control users actions should be in place to mitigate these risks and also properly enforced. While there might be negotiable tradeoffs in implementing and managing information assurance strategy, top management involvement and support are essential in the determination of tolerable threats based on the organization's missions, goals and strategic objectives.

Health care operations involves many business associates, a good information assurance strategy should include some service level agreements that include service availability, priority and access control to ensure not just availability of information, but also data security and privacy.

REFERENCES

Aarts, J., & Koppel, R. (2009). Implementation Of Computerized Physician Order Entry In Seven Countries, *Health Affairs*, 28(2), 404-414.

Amadi, E. U. (2015). The Electronic health records implementation success: lessons learned and best practice. *Journal of Technology Research, 6*, 1-12

Amadi, E. U., & Born, A. (2013). Information systems program and business needs: Case study of a Midwestern University. *Research In Business & Economics Journal*, 7, 136-156.

Anonymous (2007). Security threats. *International Journal of Micrographics and Optical Technology, 25*(5), 4-6

Bates, D, Leape, L., Cullen, D., Laird, N., Petersen, L., Teich, J., Burdick, E., Hickey, M., Kleefield, S., Shea, B., Vliet, V., & Seger, D. (1998). Effect of Computerized Physician Order Entry and a team intervention on prevention of serious medication errors. *JAMA,* 1311-16.

Bates D. (2000). Using information technology to reduce rates of medication errors in hospitals. *BMJ Journal*, 320,788-791.

Charles, D., Gabriel, M., and Searcy T. (April 2015). Adoption of Electronic health records Systems among U.S. Non-Federal Acute Care Hospitals: 2008-2014. ONC Data Brief, no.23. Office of the National Coordinator for Health Information Technology: Washington DC. https://healthit.gov/sites/default/files/data-brief/2014HospitalAdoptionDataBrief.pdf

Coles, R. S., & Moulton, R. (2003). Operationalizing IT risk management, Computers & Security 22(6), 487-492.

Colwill, C.J., & Gray, A. (2007). Creating an effective security risk model for outsourcing decisions. *BT Technology, 25*(1), 79-87.

Colwill, C. J., Todd, M.C., Fielder, G. P., & Natanson, C. (2001). Information Assurance. *BT Technology Journal, 19*(3), 107-114.

Cummings, R. (2002). The evolution of Information Assurance. *Computer*, *35*(12), 65-72

Dawes, S.S., Cresswel, A., M., & Pardo, T. (2009). From "Need to Know" to "Need to share": Tangled problems, information boundaries. *Public Administration Review*, *69*(3), 392-402.

DesRoches, C.M., Campbell, E. G., Rao, S. R., Donelan, K., Ferris, T. G., Jha, A., Kaushal, R., Levy, D.,E., Rosenbaun,S., Shields, A., Blumenthal, D. (2008). Electronic Health Records in Ambulatory Care. A National Survey of Physicians. *The New England Journal of Medicine 359 (1),* 50-60.

DOD: http://www.prim.osd.mil/cap/cio-ia.html?p=1.1.1.1

Ezingeard, J., McFadzean, E., & Birchall, D. (2005). A model of Information Assurance benefits. *Information Systems Management*, *22*(2), 20-29.

Gordon, L. A., & Loeb, M. P. (2002). The economics of information security investment. *ACM Transactions on Information and System Security*, *5*(4), 438–457.

Healthit.gov (2016). What electronic health records implementation issues are unique to rural settings? http://www.healthit.gov/providers-professionals/faqs/what-electronic-health-record-implementation-issues-are-unique-rural-se

HHS.gov (2016): Breaches affecting 500 or more individuals. Retrieved from https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf

HHS.gov (2016). HIPAA Administrative Simplification Statute and Rules. Retrieved from http://www.hhs.gov/ocr/privacy/hipaa/administrative/enforcementrule/index.html

Hung, H., & Wong, Y.H. (2009). Information transparency and digital privacy protection: Are they mutually exclusive in the provision of e-services? *Journal of Science Marketing, 23*(3), 154-164.

Jamoom, E, Beatty, P, Bercovitz, A, Woodwell, D, Palso, K, Rechtsteiner, E (2011). Physician Adoption of Electronic health records Systems: United States, 2011. Retrieved from http://www.cdc.gov/nchs/data/databriefs/db98.pdf

Jha, A.K, DesRoches, C.M., Campbell, E.G., Donelan, K., Rao, S.R., Ferris, T.G., Shields, A., Rosenbaum, S., & Blumenthal, D. (2009). Use of electronic health records in U.S. Hospitals. *The New England Journal of Medicine*, 360, 1628-1638.

Kovacich, G. L. (2001). The Corporate Information Assurance Officer (CIAO). *Computer & Security,* 20, 302-307.

Korotka, M.S., Yin, L. R., & Basu, S. C. (2005). Information Assurance Technical framework and end user information ownership: A critical analysis. *Journal of Information Privacy & Security*, *1*(1), 10-26.

Litvin, C. (2007, June). In the Dark - The Case for Electronic Health Records. *The New England Journal of Medicine,* 356*(24),*

Lu, Y., Tsang, W.W.K, & Peng, M.W. (2008). Knowledge management and innovation strategy in the Asia Pacific Toward an institutional-based view. *Asia Pacific Journal of Management,* 25, 361-374.

Loghry, J. D., & Veach, C., B. (2009). Enterprise risk assessments: Holistic approach provides companywide perspective. *Professional Safety*, 31-35.

May, C., Baker, M., Gabbard, D., Good, T., Grimes, G., Holmgren, M., Nolan, R., Nowak, R., & Pennline, S. (2004). Advanced Information Assurance Handbook. Retrieved August 1, 2010, from www.cert.org/archive/pdf/aia-handbook.pdf

McEvilley, M. (2002). The essence of information assurance and its implications for the Ada community. *Proceedings of the 2002 annual ACM SIGAda international conference on Ada* (pp.35-39). Houston, Texas, USA.

NASA: Best Practices for Keeping Your Home Network Secure. Retrieved form https://www.nsa.gov/ia/_files/factsheets/I43V_Slick_Sheets/Slicksheet_BestPracticesForKeepingYourHomeNetworkSecure.pdf

NIST (2012): Guide to Intrusion Detection and Prevention Systems (IDPS). *Recommendations of the National Institute of Standards and Technology* http://csrc.nist.gov/publications/drafts/800-94-rev1/draft_sp800-94-rev1.pdf

Schou, C. D., & Trimmer, K. J. (2004). Information Assurance and security. *Journal of Organizational and End User Computing,* 16(3), 1-7.

Shields, A.E, Shin P., Leu, M.G., Levy, D. E., Betancourt, R. M., Hawkins, D. and Proser. M. (2007). Adoption Of Health Information Technology In Community Health Centers: Results Of A National Survey, *Affairs*, 26(5), 1373-1383. Retrieved from http://content.healthaffairs.org/cgi/content/abstract/26/5/1373

Sveen, F. O., Rich, E. & Jager, M. (2007). Overcoming organizational challenges to secure knowledge management. *Inf Syst Front,* 9, 481-492.

Verizon (2015). 2015 Data Breach Investigations Report: Quantify the impact of a data breach with new data from the 2015 dbir. Retrieved 08/22/2015 from http://www.verizonenterprise.com/DBIR/2015/