Security challenges for health information systems

Curtis Anderson

Health Care Information Systems faces challenges of many organizations protecting their information systems from potential threats, such as viruses, accidental fires, untested software, and employee theft of data. Falling into three categories: Human threats (intentional or unintentional human tampering), Natural and environmental (floods, fires, and power outages), and Technology functions (failure of drives, and no backup), viruses are the most common and virulent forms of computer tampering. Another common security issues has to do with internal breaches, usually caused by installation or use of unauthorized software, illegal and illicit communication surfing sites, and e-mail harassment, and using an organizations computer for personal gain. Hardware, like software, used in health care information systems must be protected from loss caused by theft, thereby exposing confidential patient information(Wager, Lee, & Glaser, 2013, p. 352-356).

The Department of Health and Human Services Security Rules published in the Federal Register on February 20, 2003 (68 Fed. Reg. 34, 8333-8381), and was updated by the HITECH legislation, which is governed by HIPAA Security Rule protects ePHI health information that is maintained or transmitted in electronically, is closely related to HIPAA Privacy Rule, which governs all protected health information (PHI)(Wager et al., 2013, p. 356).

With the advancement of mobile technology and the development of applications found in many portable devices, health intervention is beneficial in the delivery of health care data. A conducted systematic review and meta-analysis shows the effectiveness of mobile-health technology, through a

controlled trial of mobile technology interventions that is used to improve the delivery process of health care information. The conducted independent study of data allocation concealment, allocation sequence, measured the effects by calculating estimates, and random effects meta-analysis(Free et al., 2013). The study showed a low risk of bias, where the health care trials supported outcomes for the appropriate management of disease, and showed significant benefits to the improvement in nurse/surgeon communication use of mobile phones for reducing diagnoses with the use of mobile technology. The conclusion of these trials showed health care providers supporting the process of intervention beneficial, but a more quality trial outcome is needed to be certain of the results.

Security Challenges

The responsibility of the healthcare organization should be to protect health information at all times; a critical process of security practices and regulatory compliance in the healthcare industry(Kwon & Johnson, 2013). Using the Ward's cluster analysis, a minimum variance that is based on the adoption security practice between organizations, measured the dichotomous data to indicate the presence or the absence of security practices. When identifying the relationship of clusters and regulatory compliance, the results of the Healthcare Information and Management Systems Society conducted a telephone-based survey, which found the United States healthcare organizations adoption of security practices, breach incident, and perceived compliance levels related to Health Inform Technology for Economic and Clinical Health, and the Health Insurance Portability and Accountability Act, that state laws governing patient

information security, identified three clusters: Leaders, Follower, and Laggers, producing a difference of non-technical practices, with the highest level compliance being associate with the organization who employed the use of a balance approach using the technical and non-technical practice(Kwon & Johnson, 2013).

Security Strategies

Security incidents have been closely related to the use of laptops, other portable and/or mobile devices and external hardware storage that contain or used to access Electronic Protected Health Information (EPHI), falls under the responsibility of HIPAA Security Rule, which requires reviewing and modifying security policies and procedures on a regular basis(“ HIPAA Security Guidance,” 2006). The reinforcing of ways to protect EPHI when accessed or used outside of and organization’s purview, using strategies can be reasonable and appropriate to conduct business activities using a portable medial/device (such as USB flash drives) to store EPHI, and the ability to access or transport EPHI using laptops, person digital assistants (PDAs) , home computers and non-corporate equipment, delegated by the Centers for Medicare and Medicaid Services (CMS), enforce HIPAA Security Standards, to determine actions covered by the organizations is reasonable and appropriate to safeguard the confidentially, integrity and availability of EPHI(“ HIPAA Security Guidance,” 2006).

The organization should establish risk analysis and risk management drive policies to reduce vulnerabilities that can be associated with remote access, and offsite use of EPHI. Establishing training policies in the workplace to address any vulnerability that may be associates with remote access to EPHI,

by changing and safeguarding passwords, protecting remote device/media by creating polices that prohibits these devise unattended, and the transmitting of EPHE on open networks or downloading EPHI on open networks or downloading EPHI on a remote computer(“ HIPAA Security Guidance,” 2006). It is important that a security incident and non-compliance issue be address in order to manage any harmful effects of the loss of the device, by securing and securing evidence, managing harmful effects, and notifying the affected party. Allowing for or the requiring of offsite use of, or access to EPHI should have and established strategy plan developed and implemented for the authorization and access of EPHI in accordance with HIPAA Security Rule §164. 308(a)(4) and the HIPAA Privacy Rule §164. 508(“ HIPAA Security Guidance,” 2006).

Social Networks

Underlying factors have concluded that a lack of information regarding the benefits, and limitations of social media health communication amongst the general public, and health professionals, use a systematic approach to identify, these benefits, and/or limitations of social media to communicate health data by a methodological quality of study that is assessed. There were seven main issues of social media, which includes focusing on increased interactions with others, to facilitate, share, and obtaining health messages, as the new dimension to health care medium use by the public, patients, and health professionals who communicate health issues for improving health outcomes. The study shows that social media can be used as a powerful tool, which offers collaboration between users, and social

interaction for a range of individualsto share data electronically (Moorhead et al., 2013).

Securing Data on Social Networks

There is a remarkable surge surrounding personal health record (PHR) systems for the patient and consumer, however biomedical studies do not show a potentially adequate capability and utility of PHR system(Tang, Ash, Bates, Overhage, & Sands, 2006), hinders toe widespread deployment of PHR adoption. Since health care records are more than just a static repository for patient data, it combines data, knowledge, and software tools, to help patients become active participants in their own care. However, the challenges of, technical, social, organizational, legal, and financial requires further study, that requires stakeholder, patients, provider, employers, payers, government, and research institutions to play key roles for developing PHR technology to overcome the barriers to the widespread adoption of PHRs, and develop polices, the cost associate with PHR in medical errors, dollars, and lives, to realize the potential benefits of routine health care and catastrophic disasters(Tang et al., 2006).

Strategies to Safeguard Data

The use of new technology, applications and platforms, such as “ social media,” has created new opportunities in healthcare but raises privacy and security challenges, The need to adapt old police and procedures, privacy and security protocols to cover communication channels and date sharing needs to be used effectively to protect a healthcare organization from the risk of a disclosing the privacy of a patient’s data(“ Social Media in Healthcare: Privacy and Security Considerations,” n. d.). This process of

using online tools and platform for sharing content and information for the purpose of: Delivering pre-development content – sending e-mail or posting on a website, engaging a population in discussion – to facilitate brand awareness/customer satisfaction, and manage communication – that offers individuals and organization a convenient organized way to consolidate their communication.

The challenges healthcare organizations face is: Ethical challenges – an acceptable standard of regulatory and legal requirements that is mandated by Title II of HIPAA, and Sarbanes-Oxley Act (SOX), the National Center for Ethics in Healthcare (NCHEC), and the World Health Organization Ethics and Health Initiative(“ Social Media in Healthcare: Privacy and Security Considerations,” n. d.), to avoid any misconduct or unethical behavior becoming a serious issue with regard to the use of social media.

The U. S Supreme Court decision on Sorrell v. IMS Health, Inc. addressed the issue of aggregated databases and the sale of prescriber data for marketing prescription drugs, where the ability to distribute, exchange, and use date from multiple sources is integral to clinical informatics, research, public health, quality improvement, and other healthcare operations. A pharmacy filling a prescription collects detailed information which includes patient and provider names, drugs, and the dosage and prescribed quantities, and the date of the prescription being filled, allows a pharmacy to sell prescription information to data-mining companies of a patient’s information once it has been de-identified by meeting the HIPAA standards. However, legislation sought to restrict the sale of prescription date for marketing purpose using the prescription confidentiality law of 2006, where a data-mining company

must obtain permission from the provider before selling prescription records(Petersen, DeMuro, Goodman, & Kaplan, 2013).

Hackers, cyberattacks and data breaches are the major attacks from outsiders, the motive and type of hackers is complex to chief information security officers (CISOs) and their staff in order to take action to protect and defend their data system. Causing grate consequences to the organizations, along with bad press, impact on reputation, and drop in share prices, requires legal action if a breach involves personal data theft. Identified as a data breach, the loss of control compromises unauthorized disclosure, unauthorized acquisition, and unauthorized access to data physically or electronically(Hayden, 2015). The protection of all date is impossible, as the proliferation of portable media, smartphones, USB drives and laptops increase the opportunity for the loss or theft of these devices along with their data requires that steps be taken to enable the encryption of mobile devise, and to immediately inform security management of a device being stolen, lost, data being compromised.

Trends in enterprise mobility has made mobile device security imperative, and the sales of smartphones is surpassing PC sales, the completive edge and benefits of mobility can be lost if the smartphone and tablet PC are not protected against mobile security threats: Mobile malware – Smartphones and table are susceptible to worms, viruses, Trojans and spyware. Eavesdropping – wireless networks use of link-level security lack end-to-end upper-layer security, allowing for unencrypted data to be eavesdropped upon. Unauthorized access – the storing of login information to applications on mobile devise can be easily access to allow intruders access to email

accounts and applications, and social media networks. Theft and loss – storing significant amounts of sensitive data on a mobile device can be critical if you are in a hurry and leave you iPhone in a taxicab, restaurant, and data loss can occur. Unlicensed and unmanaged applications – this can cost a company in legal cost(“ Learning guide: Mobile device protection,” 2015).

Government and Quasi-government

Benefitting from health surveillance, has pioneered, informatics analysis, and solutions in the field of informatics to serve other facets of public health, to include emergency response, environmental health, nursing, and administration. As the systematic application of information and computer science and technology, public health practice, research, and learning professions apply mathematic, engineering, information science, and social science to public health problems and processes that are important to biomedical or health informatics(Savel & Foldy, 2012). With seven ongoing elements of any public health surveillance system: Planning and system design – to identify information and sources that addresses the surveillance goal. Data Collection – The use of different collection methods, to identify the appropriate use of a structured data system that supports easier, faster, and higher-quality data entry fields compared to free test, useful vocabulary, and data standards. Date management and collation – are used to share data across different computing/technology platforms to link data with data from a legacy system. Analysis – is used for the statistical and visualization application, to generate algorithms that alert users of aberrations in health event. Interpretation – this is useful to compare information from one

surveillance program with other data sets. Application to public health programs – this utility assesses surveillance data directly flowing into an information system that support public health interventions and information elements(Savel & Foldy, 2012). The challenges of surveillance informatics includes an efficient and effective way to combine sources of complex data and information into an actionable knowledgeable to meet the challenges to arise at a faster, better, and lower cost surveillance and interpretation of health events and trends, the leveraging of technology standards ability to not only talk and listen, but understand each other. Adopting such a system is insufficient since both semantic and syntactic standard must be implemented and tested to ensure system validity.

In conclusion, healthcare security is vital to the securing and protecting a patient’s privacy and healthcare information from being breached, lost, stolen, while protecting the healthcare system from viruses, worms, malware and spyware, that can affect the integrity of an organization, a drop in stock prices, and legal issues. Protecting any system that stores vital organization and personal information should be a priority.

References

Free, C., Phillips, G., Watson, L., Galli, L., Felix, L., Edwards, P., Haines, A. (2013). The effectiveness of mobile-health technologies to improve health care service delivery processes: a systematic review and meta-analysis. Retrieved May 20, 2015, fromhttp://www. ncbi. nlm. nih. gov/pubmed/23458994

HIPAA Security Guidance. (2006). Retrieved May 20, 2015, fromhttp://www. hhs. gov/ocr/privacy/hipaa/administrative/securityrule/remoteuse. pdf

Hayden, E. (2015). Data breach protection requires new barriers. Retrieved May 20, 2015, fromhttp://searchsecurity. techtarget. com/feature/Data-breach-protection-requires-new-barriers

Kwon, J., & Johnson, E. M. (2013). Security practices and regulatory compliance in the healthcare industry. Retrieved May 20, 2015, fromhttp://connection. ebscohost. com/c/articles/84758015/security-practices-regulatory-compliance-healthcare-industry

Learning guide: Mobile device protection. (2015). Retrieved May 20, 2015, fromhttp://searchmobilecomputing. techtarget. com/guides/Mobile-device-protection-and-security-threat-measures

Moorhead, PhD, MSc, S. A., Hazlett, PhD, MSc, D. E., Harrison, MSc, L., Carroll, MD, MPH, J. K., Irwin, PhD, A., & Hoving, PhD, C. (2013). A New Dimension of Health Care: Systematic Review of the Uses, Benefits, and Limitations of Social Media for Health Communication. Retrieved May 20, 2015, fromhttp://www. ncbi. nlm. nih. gov/pmc/articles/PMC3636326/

Petersen, C., DeMuro, P., Goodman, K. W., & Kaplan, B. (2013). Sorrell v. IMS Health: issues and opportunities for informaticians. Retrieved May 20, 2015, fromhttp://www. ncbi. nlm. nih. gov/pubmed/23104048

Savel, MD, T. G., & Foldy, MD, S. (2012). The Role of Public Health Informatics in Enhancing Public Health Surveillance. Retrieved May 20, 2015,

fromhttp://www. cdc. gov/mmwr/preview/mmwrhtml/su6103a5. htm? s_cid= su6103a5_x

Social Media in Healthcare: Privacy and Security Considerations. (n. d.). Retrieved May 20, 2015, fromhttp://himss. files. cms-plus. com/HIMSSorg/Content/files/Social_Media_Healthcare_WP_F

Tang, MD, MS, P. C., Ash, PhD, J. S., Bates, MD, D. W., Overhage, MD, PhD, J. M., & Sands, MD, MPH, D. Z. (2006). Personal Health Records: Definitions, Benefits, and Strategies for Overcoming Barriers to Adoption. Retrieved May 20, 2015, fromhttp://www. ncbi. nlm. nih. gov/pmc/articles/PMC1447551/

Wager, K. A., Lee, F. W., & Glaser, J. P. (2013). *Health Care Information Systems* (3rd ed.). San Francisco, CA: Jossey-Bass.