International Journal of Information Technology and Management

Vol. V, Issue No. I, August-2013, ISSN 2249-4510

AN ASSESSMENT ON VARIOUS INFORMATION SECURITY AND PRIVACY IN HEALTHCARE INFORMATION SYSTEM

AN INTERNATIONALLY INDEXED PEER REVIEWED & REFEREED JOURNAL

www.ignited.in

International Journal of Information Technology and Management
Vol. V, Issue No. I, August-2013, ISSN 2249-4510

An Assessment on Various Information Security and Privacy in Healthcare Information System

Rajesh Sonkar

Research Scholar, CMJ University, Shillong, Meghalaya

Abstract – Information security and privacy in the healthcare sector is an issue of growing importance. The adoption of digital patient records, increased regulation, provider consolidation, and the increasing need for information between patients, providers, and payers, all point towards the need for better information security. We critically survey the research literature on information security and privacy in healthcare, published in both information systems, non-information systems disciplines including health informatics, public health, law, medicine, and popular trade publications and reports. In this paper, we provide a holistic view of the recent research and suggest new areas of interest to the information systems community.

With the recent developments in information and communication technology, healthcare is constantly undergoing changes with new medical technologies, business models and research findings. It has evolved as a new data-centric, more precise, productive, accurate and timely system which can make the difference of life and death in acute situations known as Electronic Health Records (EHRs). The requirements for security and privacy are also very critical and very difficult to satisfy in case of EHRs data as compared to any other data. This is due to the conflicting needs of clinicians (who demand open and easy access to EHRs) and the patients (who prefer closed and private access to EHRs).

Patient Health Record (PHR) systems offer great promise but raise significant philosophical, cultural, legal, and technical challenges. In hopes of furthering debate on key issues, we explain some central questions about the role, purpose, and policies associated with these systems. We also propose a framework for addressing policy questions and candidate technology that we believe may sharpen policy discussion and allow PHR systems to adhere to policies they adopt.

----------♦----------

INTRODUCTION

As the health care delivery system adopts information technology, vast quantities of health care data become available to mine for valuable knowledge. Health care organizations generally adopt information technology to reduce costs as well as improve efficiency and quality. Medical researchers hope to exploit clinical data to discover knowledge lying implicitly in individual patient health records. These new uses of clinical data potentially affect healthcare because the patient-physician relationship depends on very high levels of trust. To operate effectively physicians need complete and accurate information about the patient.

However, if patients do not trust the physician or the organization to protect the confidentiality of their health care information, they will likely withhold or ask the physician not to record sensitive information (California HealthCare Foundation, 1999). This puts the patient at risk for receiving less than optimum care, the organization at risk of having incomplete information for clinical outcome and operational efficiency analysis, and may deprive researchers of important data. Numerous examples exist of inappropriate disclosure of individually identifiable data that has resulted in harm to the individual (Health Privacy Project, 2003). Concerns about such harm have resulted in laws and regulations such as the privacy rules of the Health Insurance Portability and Accountability Act (HIPAA) of 1996 directly governing the use of such information by most health care providers, health plans, payors, clearinghouses, and researchers. These laws and regulations may also indirectly govern the use of this data by the business partners of these entities. None of these laws forbid research or using technologies such as data mining. All require medical investigators, whether conducting biomedical research or quality assurance reviews, to take sound precautions to respect and protect the privacy and security of information about the subjects in their studies.

Researchers, mainly in information systems, have adapted several reference disciplines such as psychology and sociology to analyze the role of individuals and employees in information security risk management (Dhillon and Backhouse 2001; Straub and Collins 1990; Straub and Welke 1998; Vaast 2007; Baker et al. (2007)) and economics to characterize investment decisions and information governance (Cauvsoglu et al. 2004; 2005; Gordon

and Loeb 2002; Khansa and Liginlal 2007; Kumar et 2007; Zhao and Johnson (2008)) Despite this growing stream of research on information security, very limited research has focused on studying information security risks in healthcare sector, which is heavily regulated and calls upon business models quite different from other industries.

Healthcare Info Security conducted the Healthcare Information Security Today survey to provide an in-depth assessment of the effectiveness of these data protection efforts, including breach prevention measures, and to pinpoint the areas where more work needs to be done. The survey was developed by the editorial staff of Information Security Media Group, with the assistance of members of the *Healthcare Info Security* board of advisers, which includes leading healthcare information security and IT experts. RSA, the Security Division of EMC, supported the survey as sponsor.

The online survey was conducted in the fall of 2012. Respondents included nearly 200 chief information security officers, CIOs, directors of IT and other senior leaders. These executives work at hospitals, integrated delivery systems, physician group practices, insurers and other healthcare organizations.

The emergence of patient-centric health information systems, including Personal Health Record (PHR)1 sites such as Google Health and Microsoft HealthVault , holds great promise for empowering patients and ensuring more effective delivery of health care. At the same time, these systems raise significant patient privacy challenges because organizations running successful PHRs will have access to sizable databases of personal health information. This aggregate health information has economic value to insurance companies, pharmaceuticals, and others, creating economic incentives for flows of personal health information that may not align with patients' interests. While health care providers, such as hospitals and clinics, are regulated by HIPAA, there is no comparable comprehensive regulation that meaningfully constrains transmission and use of personal health information by PHRs or related patient-centric health information systems.

HEALTH INFORMATION PRIVACY AND SECURITY

Often voluminous, heterogeneous, unstructured, lacking standardized or canonical form, and incomplete, as well as surrounded by ethical considerations and legal constraints, the characteristics of patient health care records make them "messy." Because they originate primarily as a consequence of direct patient care with the presumption of benefit for the patient, their use for research or administrative purposes must happen with care to ensure no harm to the patient. Inappropriate disclosure, loss of data integrity, or unavailability may each cause harm (Cios and Moore, 2002).

Recent laws and regulations such as HIPAA provide patients with legal

rights regarding their personally identifiable healthcare information and establish obligations for healthcare organizations to protect and restrict its use or disclosure. Data miners should have a basic understanding of healthcare information privacy and security in order to reduce risk of harm to individuals, their organization or themselves.

Privacy and Healthcare Information : The term "privacy" bears many meanings depending on the context of use. Common meanings include being able to control release of information about one's self to others and being free from intrusion or disturbance in one's personal life. To receive healthcare one must reveal information that is very personal and often sensitive. We control the privacy of our healthcare information by what we reveal to our physicians and others in the healthcare delivery system. Once we share personal information with our caregivers, we no longer have control over its privacy. In this sense, the term "privacy" overlaps with "confidentiality" or the requirement to protect information received from patients from unauthorized access and disclosure.

For example, the HIPAA Privacy Standard (Department of Health and Human Services, 2002) requires healthcare providers, health plans and health plan clearinghouses to establish appropriate administrative, technical, and physical safeguards to protect the use and disclosure of individually identifiable health information. HIPAA draws on ethical standards long developed in the health care disciplines that identify protecting the confidentiality of patient information as a core component of the doctor patient relationship and central to protecting patient autonomy. Thus, ethics, laws and regulations provide patients with certain rights and impose obligations on the healthcare industry that should keep patient health information from being disclosed to those who are not authorized to see it.

Security and Healthcare Information : Use of the Internet has resulted in recognition that information technology security is of major importance to our society. This concern seems relatively new in healthcare, but information technology security is a well established domain. A large body of knowledge exists that can be applied to protect healthcare information. A general understanding of security can be obtained by understanding:

1. Security Components

2. Security Principles

3. Threats, Vulnerabilities, Control Measures and Information Assurance

4. Achieving Information Security: Administrative, Physical, Technical Safeguards.

PRIVACY POSITION

A Personal Health Record is generally a health record that is initiated and maintained by an individual. Google Health, for example, claims to store information "securely and privately" and let patients "always control how it's used". Microsoft HealthVault similarly proposes to allow individuals to "take charge" and "make more informed health decisions" . Both sites promise to help individuals gather and organize medical records. Patients may naturally expect that this collected information will help them understand their health issues more clearly, and also allow them to provide information about past diagnosis and treatment with medical professionals; Google explicitly highlights sharing information with "doctors or caregivers".

One basic issue is the degree to which an individual may restrict visibility into information they store in their PHR. In the commonly held view of privacy as a right to control information about oneself, adopted by privacy advocates including Deborah Peel of Patients Privacy Rights, patient control would seem to effectively address privacy concerns. However, it is not clear how complete control could be achieved, it is not clear that current sites promise it, and it is debatable whether complete control is actually in the best interests of individuals or the public good.

Certainly no individual wishes to be asked directly whenever someone wishes to access their health record. Further, when aggregate statistics are calculated, there is room for debate as to whether release of those statistics constitute use of personal health data. With regard to individual control over their health information, Google's privacy policy allows use in other Google Products; although data will not be used to customize ads, there are apparently no further explicit restriction on the cross-product use of data. Finally, epidemics and spread of certain diseases are currently tracked my government health agencies, and it is likely that laws requiring notification or tracking of certain diseases will be applied to PHRs, in the interest of the public good. We therefore question the simple view that equates privacy with individual control. Instead, we propose evaluation and debate regarding a broader view of privacy based on the theory of contextual integrity.

STATE OF INFORMATION SECURITY RESEARCH IN HEALTHCARE

In this sections, we present a comprehensive review of information security literature in healthcare sector. For this survey of information security literature, we conducted a multidisciplinary search in a diverse set of publications from a range of fields including information systems, health informatics, public health, medicine, and law. Furthermore, we searched for articles in popular trade publications and reports as well. For example, a significant body of research examines the impact of IT investments on quality improvement, in particular the reduction of medical errors. This body of research has a noteworthy overlap with information security research since medical errors arising from erroneous data entry or unwarranted data manipulation/ obfuscation may lead to future potential risks. Another stream of research focuses on introduction of personal health record (PHR) technology which offers patients direct control over their health records. Scholars focusing on privacy and information security aspects of PHR are examining important privacy concerns such as information disclosure in the online PHR systems.

Privacy Concern among Healthcare Consumers : A significant body research has examined the perception of privacy concern from viewpoint of a special class of patients, including mental health patients, seekers of HIV testing, and adolescents. In a recent survey of past research on healthcare confidentiality, Sankar et al. (2003) make four overarching conclusions. First, patients strongly believe that their information should be shared only with people involved in their care. Second, patients do identify with the need of information sharing among physicians, though HIV patients are less likely to approve sharing of their health information. Third, many patients who agree to information sharing among physicians reject the notion of releasing information to third parties including employers and family members. Lastly, the majority of patients who have undergone genetic testing believe that patients should bear the responsibility of revealing test results to at-risk family members.

INFORMATION ACCESS CONTROL

Modern healthcare systems are large networked systems managing patient data with a multitude of users accessing health data for diverse contextual purposes within and across organizational boundaries. Role Based Access Control (RBAC), originally developed to manage access to resources in a large computer network (Ferraiolo and Kuhn 1992; Sandhu et al. 1996), is generally presented as an effective tool to manage data access in healthcare industry because of its ability to implement and manage a wide range of access control policies based on complex role hierarchies commonly found in healthcare organizations (Gallaher et al. 2002). This stream of research primarily focuses on developing algorithms and frameworks to facilitate role based information access (e.g. Li and Tripunitara 2006; Motta and Furuie 2003), and contextual access control (Covington et al. 2000; Motta and Furuie

2003). Schwartmann (2004) extends this stream of research by proposing an enhanced RBAC system that incorporates attributable roles and permissions. This enhanced system implementation is theorized to reduce the burden of managing access privileges by lowering extremely high number of permissions and roles to a manageable size and hence reducing administrative cost. In addition progress is being made in several fronts, including use of autonomous agents to create privacy-aware healthcare applications (Tentori et al. 2006), authorization policy framework for peer-to-peer technology based distributed healthcare system (Al-nayadi and Abawajy 2007), encrypted bar code technology framework for electronic transfer of prescription (Ball et al. 2003), pseudonymous linkage (Reidl et al. 2007), and electronic consent models that allows patients to define which component of a medical record could be shared to whom (O'Keefe et al. 2005; Nepal et al. 2006).

DATA INTEROPERABILITY AND INFORMATION SECURITY

Healthcare information systems currently adopted by some provider organizations store health information in different proprietary formats. This diversity of data formats creates a major hurdle in sharing patient data among provider organizations as well to medical and health policy research. Walker, et al. (2005), in a recent investigation, empirically argued that investing in EMR interoperability and establishing a health information exchange, could save the industry $77Bper year. Whereas without interoperability, continued adoption of current EMR technologies will promote information silos that already exist in today's paper based medical records leading to proprietary control by information creators (Brailer 2005). Moreover, privacy and security in establishing an interoperable health information exchange remain dominant issues. Recently, nationwide initiatives have been undertaken to address the privacy and security problems under the auspices of AHRQ and the Office of the National Coordinator for Health Information Technology. Currently 33 states and one territory have developed plans to implement privacy and security policy solutions that enable seamless electronic exchange of health information (Dimitropoulos 2007a). Most of these state plans recognize the need and call for development of a universal patient consent form that incorporates common information disclosure situations as well for specially protected information. Furthermore they call for standardized approaches for user authorization and authentication, user access, and audit of patient record access and modification, uniform identification of patients, security of data during transmission and at rest (Dimitropoulos 2007b).

REVIEW OF THE LITERATURE

In the previous sections managing health information privacy and security has been described as required by organizations involved in the industry of delivering healthcare; e.g. healthcare providers, health plans, payors, and clearinghouses. In this section we will explore the additional issues that large scale data mining presents for managing health information privacy and security. Data mining offers many possible benefits to the medical community, including administrators as well as researchers. One example of the value that can be derived from large data collections is demonstrated by Kaiser Permanente's Northern California Region reduction of the risk of their members dying from cardiovascular causes so that it is no longer their number one cause of death. According to the 2002 Annual Report of the National Committee for Quality Assurance (2002, pg. 23), "Since 1996, appropriate cholesterol control (as defined by HEDIS, an LDL level of less than 130) among the CAD population has improved from 22 percent to 81 percent. Among eligible patients discharged after a heart

attack, 97 percent were on beta-blockers. The mortality rate from heart attacks at KPNC hospitals are up to 50 percent lower than at similar hospitals across the state." This was made possible by the development of a clinical data repository to support real-time direct healthcare delivery to its membership (over three million individuals), evidence-based medical knowledge and use of this data to guide their healthcare delivery processes (Levin et al., 2001) (Pheatt et al., (2003). As information technology has become commonly used to support the core processes of healthcare, enormous volumes of data have been produced.

Numerous organizations desire access to this data to apply techniques of knowledge discovery. Privacy concerns exist for information disclosed without illegal intrusion or theft. A person's identity can be derived from what appears to be innocent information by linking it to other available data. Concerns also exist that such information may be used in ways other than promised at the time of collection. Ways to share person specific data while providing anonymity of the individual are needed. Stated another way, controls are needed to manage the inferences about individual identity that can be made from shared person specific data. The Federal Office of Management and Budget (1994) has developed an approach to limit disclosure from government data so that the risk that the information could be used to identify an individual, either by itself or in combination with other information, is very small. This Report on Statistical Disclosure Limitation Methodology, Statistical Policy. The report includes a tutorial, guidelines, and recommendations for good practice; recommendations for further research; and an annotated bibliography. Techniques, rules and procedures (magnitude versus frequency, counts, suppression, random versus controlled rounding, confidentiality editing) and microdata (sampling, removing identifiers, demographic detail, high visibility variables, adding random noise, rank

swapping, blank and imputation for randomly selected records and blurring) are documented.

CONCLUSION

Technology is enabling medical health records to be put in the electronic format, EPRs, and making them available to the users via the Internet. In addition, advances in the area of sensor networks are making the idea of remote patient monitoring a reality. In this paper we discussed the privacy and security issues that arise when integrating these new technology into the traditional health care system. We explored some of the existing solutions that can be employed and the open research questions that need to be answered before the widespread use of the new technology is possible with minimal security and privacy risks.

A formal approach to managing the use and disclosure of personal health information is in the best interests of patients, individual researchers, organizations and society. The risks to those who do not adhere to good security and privacy practices are considerable. Future laws and regulations are likely to increase penalties for inappropriate use or disclosure. While much attention has been given to research, organizations should implement the same general processes to support analyses done for the purpose of healthcare operations as for research.

“Researchers have no automatic right to review patient data. Besides developing strategies for minimizing patient risk, as described herein, investigators should take simple steps to characterized their compliance with human subjects requirements” (Berman, pg. 33, 2002). A recent publication recommends:

“First, sensitive raw data like identifiers, names, addresses and the like, should be modified or trimmed out from the original database, in order for the recipient of the data not to be able to compromise another person’s privacy. Second, sensitive knowledge which can be mined from a database by using data mining algorithms, should also be excluded, because such a knowledge can equally well compromise data privacy, as we will indicate.

REFERENCES

- Abrahama, C., Watson, R.T., Boudreau, M.C. (2008) ―Ubiquitous Access: On the Front Lines of Patient Care and Safety,‖ *Communications of the ACM*, vol. 51, no.6, pp 95 – 99,

- Agrawal, R., Evfimievski, A., Srikant, R. (2003) ―Information sharing across private databases,‖ in *Proceedings of ACM SIGMOD*.

- Behlen, F.M., and Johnson, S.B., (1999) ―Multicenter Patient Records Research: Security Policies and Tools,‖ *Journal of the American Medical Informatics Association*, vol. 6, no. 6, pp 435-443

- Computer Science and Telecommunications Board, National Research

- Council, *For the Record: Protecting Electronic Health Information*. Washington, DC: National Academy Pr; 1997.

- Dhillon, G. and Backhouse, J. (2001) ―Current Directions in IS Security Research: Towards Socio-Organizational Perspectives,‖ *Information Systems Journal*, vol. 11, no. 2, pp. 127-153

- Gordon, L.A. and Loeb, M.P. (2002) ―The Economics of Information Security Investment,‖ *ACM Transactions on Information and System Security*, vol. 5, no. 4, pp. 438-457

- Kaiser, J. (2004) "Patient Records: Privacy Rule Creates Bottleneck for U.S. Biomedical Researchers," *Science*, vol.305, no.5681, pp 168-169

- M.N. Huda, S.Yamada, N. Sonehara 2009 "Privacy-aware access to patient-controlled Personal Health Records in emergency situations." In Proceedings of third International Conference on Pervaisve Health, 1-3 April, London, UK.

- Office for Civil Rights, “Summary of the HIPAA privacy rule,” US Department of Health & Human Services, 2003.

- Sweeney L 2002 k-Anonymity: A model for protecting privacy, International Journal on Uncertainty ,Fuzziness and Knowledge based systems, 2002.

- Taipale, K.A. (2003). “Data Mining and Domestic Security: Connecting the Dots to Make Sense of Data,” *The Columbia Science and Technology Law Review*, Vol. V, 5-83.